



Guia do Desenvolvedor

# AWS IoT Wireless



# AWS IoT Wireless: Guia do Desenvolvedor

Copyright © 2026 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 desprestige 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 AWS IoT Wireless? .....	1
Recursos do AWS IoT Wireless .....	1
Integrar dispositivos LoRaWAN e Sidewalk .....	1
Integração com AWS IoT Core .....	2
Para usuários iniciantes no AWS IoT Wireless .....	2
Serviços relacionados .....	3
Acessar o AWS IoT Wireless .....	3
Conceitos básicos .....	5
Configurar o AWS IoT Wireless .....	5
Configurar a Conta da AWS .....	5
Instalar o Python e a AWS CLI .....	8
Descrever os recursos sem fio .....	10
Nomes e descrição dos recursos .....	11
Tags de recursos .....	12
AWS IoT Core for LoRaWAN .....	14
Introdução .....	14
Como acessar o AWS IoT Core for LoRaWAN .....	15
Regiões e endpoints do AWS IoT Core for LoRaWAN .....	15
Definição de preço do AWS IoT Core for LoRaWAN .....	16
O que é o AWS IoT Core for LoRaWAN? .....	16
Recursos do AWS IoT Core for LoRaWAN .....	16
O que é LoRaWAN? .....	17
Como a AWS IoT Core for LoRaWAN funciona .....	19
Como se conectar ao AWS IoT Core for LoRaWAN .....	21
Convenções de nomenclatura para dispositivos, gateways, perfis e destinos .....	21
Mapeamento dos dados do dispositivo para os dados do serviço .....	21
Usar o console para integrar o dispositivo e o gateway ao AWS IoT Core for LoRaWAN .....	22
Gateways LoRaWAN integrados .....	22
Integrar dispositivos LoRaWAN .....	32
Configurar a posição dos recursos LoRaWAN .....	48
Como funciona o posicionamento para dispositivos LoRaWAN .....	49
Visão geral do fluxo de trabalho do posicionamento .....	50
Configuração da posição de um recurso .....	51
Configuração da posição dos gateways LoRaWAN .....	52

Configuração da posição de dispositivos LoRaWAN .....	56
Gerenciar gateways do LoRaWAN .....	62
Requisito de software LoRa Basics Station .....	62
Usar gateways qualificados do AWS Partner Device Catalog .....	62
Usar protocolos CUPS e LNS .....	62
Configure os recursos de beaconing e filtragem dos gateways LoRaWAN .....	63
Atualizar o firmware do gateway utilizando CUPS .....	69
Escolher gateways para receber o tráfego de dados de downlink LoRaWAN .....	85
Gerenciar dispositivos LoRaWAN .....	88
Considerações sobre dispositivos .....	88
Uso de dispositivos com gateways qualificados para o AWS IoT Core for LoRaWAN .....	88
Versão LoRaWAN .....	88
Modos de ativação .....	88
Classes de dispositivos .....	89
Executar a ADR para dispositivos LoRaWAN .....	89
Gerenciar a comunicação dos dispositivos LoRaWAN .....	92
Gerenciar o tráfego LoRaWAN de redes de dispositivos públicas LoRaWAN (Everynet) .....	101
FUOTA para dispositivos LoRaWAN e grupos multicast .....	112
Preparar dispositivos para configuração multicast e FUOTA .....	113
Criar grupos multicast .....	117
FUOTA para dispositivos LoRaWAN .....	130
Monitorar recursos LoRaWAN com o analisador de rede .....	145
Adicionar o perfil do IAM necessário para o analisador de rede .....	147
Criar a configuração do analisador de rede e adicionar recursos .....	149
Transmita mensagens de rastreamento com WebSockets .....	158
Monitorar mensagens de rastreamento em tempo real .....	166
Depure seus grupos multicast e tarefas FUOTA usando o analisador de rede .....	169
Endpoints da VPC do LoRaWAN .....	173
Considerações sobre os endpoints da VPC do AWS IoT Wireless .....	173
Arquitetura de link privado do AWS IoT Core for LoRaWAN .....	173
Endpoints do AWS IoT Core for LoRaWAN .....	174
Integrar o endpoint do ambiente de gerenciamento .....	175
Integrar os endpoints do plano de dados .....	179
AWS IoT Core para Amazon Sidewalk .....	189
Acessar o AWS IoT Core para Amazon Sidewalk .....	189
AWS IoT Core para regiões e endpoints do Amazon Sidewalk .....	189

Preços do AWS IoT Core para Amazon Sidewalk .....	190
O que é o AWS IoT Core para Amazon Sidewalk? .....	190
Recursos do AWS IoT Core para Amazon Sidewalk .....	190
O que é o Amazon Sidewalk? .....	191
Como funciona o AWS IoT Core para Amazon Sidewalk .....	193
Conceitos básicos do AWS IoT Core para Amazon Sidewalk .....	194
Experimente o tutorial de monitoramento de sensores .....	195
Introdução à integração de seus dispositivos do Sidewalk .....	196
Conectar-se ao AWS IoT Core para Amazon Sidewalk .....	200
Pré-requisitos .....	200
Descrição de recursos do Sidewalk .....	201
Adicionar seu dispositivo do Sidewalk .....	201
Adicionar um destino para o dispositivo do Sidewalk .....	211
Conectar seu dispositivo final do Sidewalk .....	219
Provisionamento em massa de dispositivos Sidewalk .....	221
Fluxo de trabalho de provisionamento em massa do Amazon Sidewalk .....	222
Criação de perfis de dispositivos com suporte de fábrica .....	227
Provisionamento de dispositivos do Sidewalk usando tarefas de importação .....	231
Segurança .....	244
Proteção de dados .....	245
Criptografia de dados no AWS IoT Wireless .....	246
Segurança de dados e de transporte do LoRaWAN .....	246
Gerenciamento de identidade e acesso .....	248
Público .....	249
Autenticando com identidades .....	249
Gerenciamento do acesso usando políticas .....	253
Como funciona o AWS IoT Wireless com o IAM .....	255
Exemplos de políticas baseadas em identidade .....	264
Políticas gerenciadas pela AWS .....	268
Solução de problemas .....	274
Validação de compatibilidade .....	277
Resiliência .....	277
Segurança da infraestrutura .....	278
Monitorar recursos sem fio utilizando o CloudWatch .....	279
Ferramentas de monitoramento .....	279
Como monitorar recursos utilizando o Amazon CloudWatch .....	280

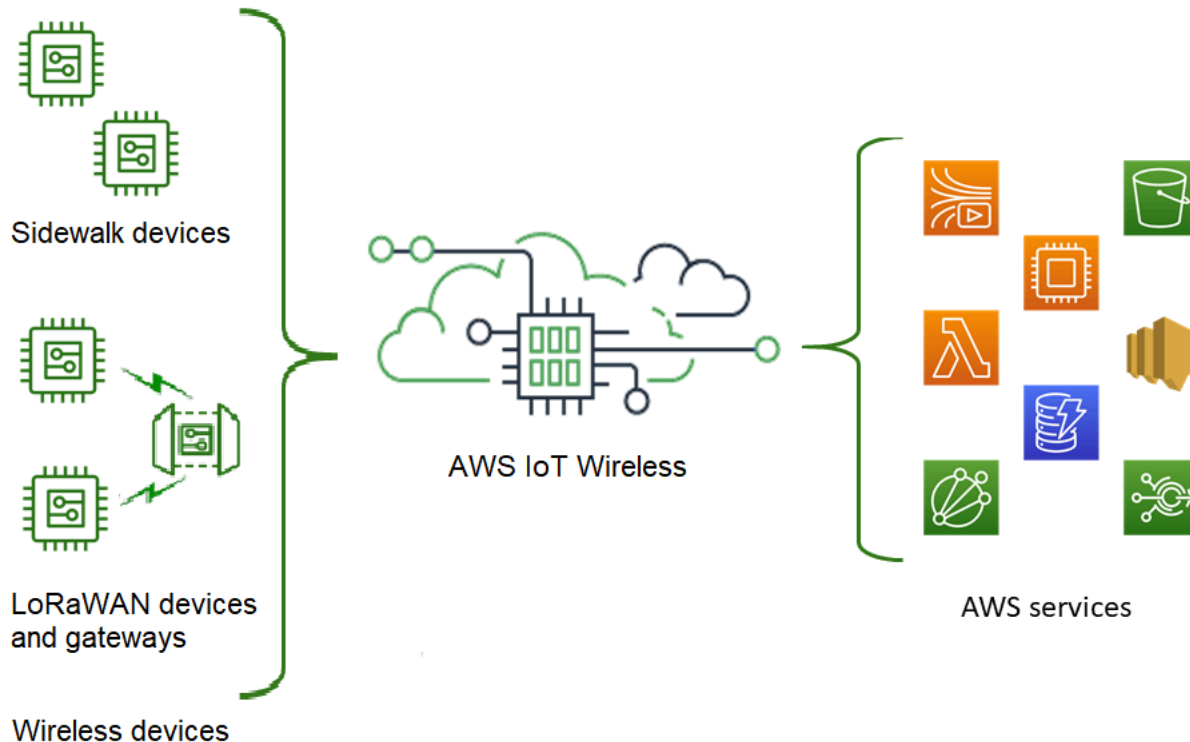
Configurar registro em log da .....	281
Criar um perfil e uma política de log .....	281
Configurar o registro em log para recursos do .....	284
Monitorar com o CloudWatch Logs .....	297
Visualizar as entradas de log .....	298
Utilizar o CloudWatch Insights para filtrar logs .....	306
Notificações de eventos .....	311
Como seus recursos podem ser notificados sobre eventos .....	311
Tipos de eventos e recursos .....	311
Política para receber notificações de eventos sem fio .....	312
Formato dos tópicos do MQTT para eventos sem fio .....	313
Preços para eventos sem fio .....	317
Ativar eventos para recursos sem fio .....	318
Configurações do evento .....	318
Pré-requisitos .....	318
Habilitar notificações usando o Console de gerenciamento da AWS .....	319
Habilitar notificações usando a AWS CLI .....	320
Notificações de eventos para recursos LoRaWAN .....	322
Tipos de eventos para recursos LoRaWAN .....	323
Eventos de ingresso LoRaWAN .....	323
Eventos de status de conexão .....	326
Notificações de eventos para recursos do Sidewalk .....	329
Tipos de eventos para recursos do Sidewalk .....	329
Eventos de estado de registro do dispositivo .....	329
Eventos de proximidade .....	333
Operações da API AWS IoT Wireless .....	336
Operações de API para perfis de dispositivos .....	336
Listar perfis de dispositivos em sua Conta da AWS .....	336
Excluir perfis de dispositivos de sua Conta da AWS .....	337
Operações de API para dispositivos LoRaWAN e Sidewalk .....	338
Associar dispositivos sem fio em sua Conta da AWS a uma coisa de IoT .....	338
Listar os dispositivos sem fio em sua Conta da AWS .....	339
Excluir dispositivos sem fio de sua Conta da AWS .....	340
Operações de API para destinos de dispositivos sem fio .....	340
Obter informações sobre o destino .....	340
Atualizar as propriedades do seu destino .....	341

---

Listar destinos em sua Conta da AWS .....	341
Excluir destinos da sua Conta da AWS .....	342
Operações da API para provisionamento em massa .....	342
Obter informações sobre a tarefa de importação .....	343
Obter o resumo de dispositivo da tarefa de importação .....	344
Adicionar dispositivos a uma tarefa de importação .....	344
Listar as tarefas de importação em sua Conta da AWS .....	345
Excluir tarefas de importação de sua Conta da AWS .....	346
Recursos do AWS CloudFormation .....	348
Modelos do AWS IoT Wireless e do CloudFormation .....	348
Saiba mais sobre a CloudFormation .....	348
Cotas .....	349
Marcação de recursos sem fio .....	350
Conceitos Básicos de Tags .....	350
Criar e gerenciar tags .....	350
Atualizar tags ou listar tags de recursos .....	351
Restrições e limitações de tags .....	351
Utilização de tags com políticas do IAM .....	352
Histórico do documento .....	355

# O que é o AWS IoT Wireless?

O AWS IoT Wireless fornece os serviços de nuvem que conectam os dispositivos sem fio a outros dispositivos e serviços da Nuvem AWS. Ao conectar os dispositivos ao AWS IoT Wireless, é possível integrá-los em soluções baseadas no AWS IoT. Utilizando o AWS IoT Wireless, é possível integrar dispositivos LoRaWAN e Sidewalk ao AWS IoT. Esses dispositivos sem fio utilizam o protocolo de comunicação de rede de longa distância de baixa potência (LPWAN) para comunicação com o AWS IoT.



## Recursos do AWS IoT Wireless

O AWS IoT Wireless fornece os seguintes recursos:

### Integrar dispositivos LoRaWAN e Sidewalk

É possível integrar dispositivos LoRaWAN e Sidewalk ao AWS IoT Wireless.

- AWS IoT Core for LoRaWAN

Para integrar os dispositivos e gateways LoRaWAN ao AWS IoT Wireless, utilize o AWS IoT Core for LoRaWAN. Ele é um Servidor da rede LoRaWAN (LNS) que elimina a necessidade de

configurar e operar um LNS privado. O AWS IoT Core for LoRaWAN fornece gerenciamento de gateway utilizando os recursos Servidor de Configuração e Atualização (CUPS) e atualização de firmware sem fios (FUOTA). Para ter mais informações, consulte [O que é o AWS IoT Core for LoRaWAN?](#).

- AWS IoT Core para Amazon Sidewalk

Para integrar os dispositivos Sidewalk ao AWS IoT Wireless, é possível utilizar os recursos oferecidos pelo AWS IoT Core para Amazon Sidewalk. O [Amazon Sidewalk](#) é uma rede compartilhada que conecta dispositivos, como Amazon Echo, câmeras de segurança Ring, luzes externas, e é compatível com outros dispositivos Sidewalk em sua comunidade. Para ter mais informações, consulte [O que é o AWS IoT Core para Amazon Sidewalk?](#).

## Integração com AWS IoT Core

É possível utilizar os seguintes recursos oferecidos pela integração do AWS IoT Wireless com o AWS IoT Core:

- Associar dispositivos a uma coisa do AWS IoT

É possível associar os dispositivos e gateways sem fio a uma coisa do AWS IoT, o que ajuda a armazenar uma representação do dispositivo na nuvem. É possível utilizar coisas no AWS IoT para pesquisar e gerenciar os dispositivos com maior facilidade e acessar outros recursos do AWS IoT Core. Para obter mais informações, consulte [Managing devices with AWS IoT](#) no Guia do desenvolvedor do AWS IoT Core.

- Utilizar as regras do AWS IoT para rotear mensagens

Você pode utilizar o recurso de regras do AWS IoT para interagir com outro AWS service (Serviço da AWS) e aplicações. As mensagens de uplink enviadas dos dispositivos à nuvem podem ser roteadas para esses serviços e outras aplicações. Para obter mais informações, consulte [AWS IoT rules](#) no Guia do desenvolvedor do AWS IoT Core.

## Para usuários iniciantes no AWS IoT Wireless

Se estiver utilizando o AWS IoT Wireless pela primeira vez, leia as seguintes seções para começar:

- [O que é o AWS IoT Core for LoRaWAN?](#)

Esta seção oferece uma visão geral da tecnologia LoRaWAN e de como o AWS IoT Core for LoRaWAN funciona. Ela também fornece recursos para ajudar você a saber mais.

- [O que é o AWS IoT Core para Amazon Sidewalk?](#)

Esta seção oferece uma visão geral da tecnologia do Amazon Sidewalk e de como o AWS IoT Core para Amazon Sidewalk funciona. Ela também fornece recursos para ajudar você a saber mais.

- [Conceitos básicos do AWS IoT Core para Amazon Sidewalk](#)

Leia esta seção para saber mais sobre como utilizar o AWS IoT Core para Amazon Sidewalk e como integrar seus dispositivos Amazon Sidewalk.

- [Conectar gateways e dispositivos ao AWS IoT Core for LoRaWAN](#)

É possível saber mais sobre como integrar os dispositivos LoRaWAN utilizando o console e a API.

## Serviços relacionados

- [Amazon CloudWatch](#)

Depois de integrar os dispositivos LoRaWAN ou Sidewalk ao AWS IoT Wireless, você pode utilizar o Amazon CloudWatch para registrar em log e monitorar os dispositivos e gateways sem fio em tempo real. Para monitorar os dispositivos e gateways LoRaWAN, você pode utilizar o analisador de rede, que reduz o tempo necessário para configurar uma conexão e começar a receber mensagens de rastreamento.

- [AWS IoT Core](#)

Também é possível utilizar a integração com o AWS IoT Core para conectar-se a um AWS service (Serviço da AWS) que pode ser acessado no mecanismo de regras. Para obter mais informações, consulte [AWS service \(Serviço da AWS\)s used by the rules engine](#).

## Acessar o AWS IoT Wireless

É possível utilizar o console, a API ou a CLI para integrar dispositivos LoRaWAN e Sidewalk.

- Usar o console de AWS IoT

Para integrar dispositivos sem fio, utilize a página [AWS IoT Wireless](#) do Console de gerenciamento da AWS.

- Uso da API AWS IoT Wireless

É possível integrar dispositivos LoRaWAN e Sidewalk utilizando a API do [AWS IoT Wireless](#). A API do AWS IoT Wireless em que o AWS IoT Core se baseia é compatível com o SDK da AWS. Para obter mais informações, consulte [SDKs da AWS e toolkits](#).

- Usando a AWS CLI

É possível utilizar a AWS CLI para executar comandos para integrar e gerenciar dispositivos LoRaWAN e Amazon Sidewalk. Para obter mais informações, consulte [referência de CLI de AWS IoT Wireless](#).

# Conceitos básicos do AWS IoT Wireless

É possível começar a usar o AWS IoT Wireless cadastrando-se em uma Conta da AWS e seguindo as etapas para criar um usuário do IAM. Após o cadastro, é possível utilizar o Console de gerenciamento da AWS, a API do AWS IoT Wireless ou a AWS CLI para integrar os dispositivos e gateways Sidewalk e LoRaWAN. Ao integrar dispositivos, considere uma forma de descrever e marcar os recursos para ajudar a identificá-los mais facilmente.

Os tópicos a seguir mostram como começar a usar o AWS IoT Wireless.

## Tópicos

- [Configurar o AWS IoT Wireless](#)
- [Descrever os recursos do AWS IoT Wireless](#)

# Configurar o AWS IoT Wireless

Ao cadastrar-se na AWS, sua Conta da AWS é automaticamente cadastrada em todos os serviços da AWS, incluindo o AWS IoT Wireless. Você será cobrado apenas pelos serviços que usar.

Para configurar o AWS IoT Wireless, utilize as etapas na próxima seção:

## Tópicos

- [Configurar a Conta da AWS](#)
- [Instalar o Python e a AWS CLI](#)

# Configurar a Conta da AWS

Antes de utilizar o AWS IoT Core for LoRaWAN ou o AWS IoT Core para Amazon Sidewalk pela primeira vez, execute as tarefas a seguir para configurar a sua Conta da AWS.

## Tópicos

- [Cadastrar-se em uma conta da AWS](#)
- [Criar um usuário do IAM](#)
- [Fazer login como usuário do IAM](#)

## Cadastrar-se em uma conta da AWS

Se você ainda não tem uma Conta da AWS, siga as etapas a seguir para criar uma.

Como cadastrar-se para uma Conta da AWS

1. Abra <https://portal.aws.amazon.com/billing/signup>.
2. Siga as instruções on-line.

Parte do procedimento de cadastramento envolve o recebimento de uma chamada telefônica e a inserção de um código de verificação no teclado do telefone.

Quando você se cadastra para uma Conta da AWS, um Usuário raiz da conta da AWS é criado. O usuário raiz tem acesso a todos os Serviços da AWS e atributos na conta. Como prática recomendada de segurança, [atribua acesso administrativo a um usuário administrativo](#) e utilize somente o usuário raiz para executar as [tarefas que exigem acesso do usuário raiz](#).

## Criar um usuário do IAM

Para criar um usuário administrador, selecione uma das opções a seguir.

Selecionar uma forma de gerenciar o administrador	Para	Por	Você também pode
Centro de Identidade do IAM (Recomendado)	Use credenciais de curto prazo para acessar a AWS. Isso está de acordo com as práticas recomendadas de segurança. Para obter	Seguindo as instruções em <a href="#">Conceitos básicos</a> no Centro de Identidade do AWS IAM Guia do usuário.	Para configurar o acesso programático, consulte <a href="#">Configurar a AWS CLI para usar o Centro de Identidade e do AWS IAM</a> no AWS Command Line Interface Guia do usuário.

Selecionar uma forma de gerenciar o administrador	Para	Por	Você também pode
	informações sobre as práticas recomendadas, consulte <a href="#">Práticas recomendadas de segurança no IAM</a> no Guia do usuário do IAM.		
No IAM (Não recomendado)	Use credenciais de curto prazo para acessar a AWS.	Seguindo as instruções em <a href="#">Criar o seu primeiro usuário administrador e um grupo de usuários do IAM</a> no Guia do usuário do IAM.	Para configurar o acesso programático, consulte <a href="#">Gerenciamento de chaves de acesso de usuários do IAM</a> no Guia do usuário do IAM.

## Fazer login como usuário do IAM

Depois de criar um usuário do IAM, você pode fazer login na AWS com seu nome de usuário e senha do IAM.

Antes de fazer login como usuário do IAM, você pode verificar o link de login para usuários do IAM no console do IAM. No painel do IAM, no link de login de usuários do IAM, é possível ver o link de login da sua Conta da AWS. O URL do link de login contém o ID da sua Conta da AWS sem traços (-).

Se você não quiser que o URL do link de login contenha o ID da sua Conta da AWS, crie um alias da conta. Para obter mais informações, consulte [Criação, exclusão e listagem de um alias de Conta da AWS](#) no Manual do usuário do IAM.

## Como fazer login como usuário do IAM

1. Saia do Console de gerenciamento da AWS.
2. Insira o link de login, que inclui seu ID (sem traços) da Conta da AWS ou o alias da Conta da AWS.

```
https://aws_account_id_or_alias.signin.aws.amazon.com/console
```

3. Insira o nome e a senha de usuário do IAM que você acabou de criar.

Quando a conexão é estabelecida, a barra de navegação exibe *your\_user\_name @ your\_aws\_account\_id*.

## Instalar o Python e a AWS CLI

Antes de conectar o dispositivo final LoRaWAN ou Sidewalk, configure a instalação do Python e a AWS CLI.

### Important

Para realizar todo o fluxo de trabalho de integração para provisionar e registrar seu dispositivo final do Sidewalk, você também deve configurar o HDK e o gateway do Sidewalk. Para obter instruções, consulte [Configuração do kit de desenvolvimento de hardware \(HDK\)](#) e [Configuração de um gateway do Sidewalk](#) na documentação do Amazon Sidewalk.

### Tópicos

- [Instale o Python e o Python3-pip](#)
- [Configurar a AWS CLI](#)

## Instale o Python e o Python3-pip

Para usar a AWS CLI e o boto3 conforme descrito na seção a seguir, use o Python versão 3.6 ou posterior. Se você quiser integrar seus dispositivos finais usando o console de AWS IoT, você pode pular esta seção e continuar configurando sua Conta da AWS. Para verificar se você já instalou o Python e o Python3-pip, execute os comandos a seguir. Se a execução desses comandos retornar a versão, o Python e o Python3-pip foram instalados corretamente.

```
python3 -V  
pip3 --version
```

Se esse comando retornar um erro, pode ser porque o Python não está instalado, ou seu sistema operacional chama o executável Python v3.x de Python3. Nesse caso, substitua todas as instâncias de python por python3 ao executar os comandos. Se ainda produzir um erro, baixe e execute o [instalador do Python](#) ou instale o Python, dependendo do seu sistema operacional, conforme descrito abaixo.

## Windows

Em sua máquina Windows, baixe o Python no [site do Python](#) e execute o instalador para instalar o Python em sua máquina.

## Linux

Em sua máquina Ubuntu, execute o seguinte comando sudo para instalar o Python.

```
sudo apt install python3  
sudo apt install python3-pip
```

## macOS

Em sua máquina Mac, use o Homebrew para instalar o Python. O Homebrew também instala o pip, que então aponta para a versão Python3 instalada.

```
$ brew install python
```

## Configurar a AWS CLI

As etapas a seguir mostram como configurar a AWS CLI e o boto3 (AWS SDK para Python). Para seguir estas etapas, você precisa se cadastrar em uma Conta da AWS e criar um usuário administrativo. Para obter instruções, consulte [Configurar o AWS IoT Wireless](#).

### 1. Instalar e configurar a AWS CLI

É possível utilizar a AWS CLI para integrar os dispositivos finais do Sidewalk ao AWS IoT Core para Amazon Sidewalk de forma programática. Se você quiser integrar seus dispositivos finais usando o console de AWS IoT, você pode pular esta seção. Abra o [console do AWS IoT Core](#) e vá para a próxima seção para começar a conectar os dispositivos ao AWS IoT Core para

Amazon Sidewalk. Para obter instruções sobre como configurar o AWS CLI, consulte [Como instalar e configurar a AWS CLI](#).

## 2. Instale o boto3 (SDK da AWS para Python)

Os comandos a seguir mostram como instalar o boto3 (SDK da AWS para Python) e a AWS CLI. Você também instalará o botocore, que é necessário para executar o boto3. Para obter instruções detalhadas, consulte [Como instalar o Boto3](#) no Guia de documentação do Boto3.

### Note

O `awscli` versão 1.26.6 requer a versão PyYAML 3.10 ou posterior, mas não posterior à 5.5.

```
python3 -m pip install botocore-version-py3-none-any.whl
python3 -m pip install boto3-version-py3-none-any.whl
```

## 3. Configure suas credenciais e a região padrão

Configure suas credenciais e a região padrão nos arquivos `~/.aws/credentials` e `~/.aws/config`. A biblioteca boto3 usa essas credenciais para identificar sua Conta da AWS e autorizar chamadas de API. Para obter as instruções de configuração, consulte:

- [Configuração](#) no Guia de documentação do Boto3
- [Configurações e configurações do arquivo de credenciais](#) no Guia de documentação da AWS CLI

## Descrever os recursos do AWS IoT Wireless

Antes de começar a usar a integração de dispositivos LoRaWAN ou Sidewalk, considere a convenção de nomenclatura dos dispositivos, dos gateways e do destino. O AWS IoT Wireless oferece várias opções para identificar os recursos criados. Embora os recursos do AWS IoT Wireless recebam uma ID exclusiva quando são criados, essa ID não é descritiva nem pode ser alterada após a criação do recurso. Para tornar a seleção, a identificação e o gerenciamento dos recursos mais conveniente, atribua um nome, adicione uma descrição e anexe tags e valores de tags à maioria dos recursos do AWS IoT Wireless.

- [Nomes e descrição dos recursos](#)

Para dispositivos, gateways e perfis, o nome do recurso é um campo opcional que você pode alterar após a criação do recurso. O nome aparece nas listas exibidas nas páginas do hub de recursos.

Para destinos, dê um nome exclusivo para a conta da AWS e Região da AWS. Não é possível alterar o nome do destino depois que o recurso de destino é criado.

Embora um nome possa ter até 256 caracteres, o espaço de exibição no hub de recursos é limitado. Certifique-se de que a parte distintiva do nome apareça nos primeiros 20 a 30 caracteres, se possível.

- [Tags de recursos](#)

As tags são pares de chave/valor de metadados que podem ser anexados aos recursos da AWS. Você escolhe as chaves de tag e os valores correspondentes.

Gateways, destinos e perfis podem ter até 50 tags anexadas a eles. Os dispositivos não são compatíveis com tags.

## Nomes e descrição dos recursos

Suporte ao recurso AWS IoT Wireless para nome

Recurso	Suporte ao campo de nome
Destino	O nome é uma ID exclusiva do recurso e não pode ser alterado.
Dispositivo sem fio	O nome é um descritor opcional do recurso e pode ser alterado.
Gateway LoRaWAN	O nome é um descritor opcional do recurso e pode ser alterado.

Recurso	Suporte ao campo de nome
Perfil	O nome é um descritor opcional do recurso e pode ser alterado.

O campo de nome aparece nas listas do hub de recursos; no entanto, o espaço é limitado e, portanto, somente os primeiros 15 a 30 caracteres do nome podem estar visíveis. Ao selecionar nomes para os recursos, considere como você deseja que eles identifiquem os recursos e como serão exibidos no console.

### Descrição

Os recursos de destino, dispositivo e gateway também oferecem suporte a um campo de descrição, que pode aceitar até 2.048 caracteres. O campo de descrição aparece somente na página de detalhes do recurso individual. Embora o campo de descrição possa conter muitas informações, ele aparece somente na página de detalhes do recurso e pode não ser conveniente para digitalização no contexto de vários recursos.

## Tags de recursos

### Suporte de recursos do AWS IoT Wireless para tags da AWS

Recurso	Suporte a tags da AWS
Destino	Você pode adicionar até 50 tags da AWS ao recurso.
Dispositivo sem fio	Esse recurso não é compatível com tags da AWS.
Gateway LoRaWAN	Você pode adicionar até 50 tags da AWS ao recurso.
Perfil	Você pode adicionar até 50 tags da AWS ao recurso.

Tags são palavras ou frases que funcionam como metadados que você pode usar para identificar e organizar os recursos da AWS. Você pode pensar na chave de tag como uma categoria de informações e no valor de tag como um valor específico nessa categoria. Por exemplo, você pode ter um valor de tag de cor e dar a alguns recursos um valor de azul para essa tag e a outros um valor de vermelho. Com isso, você pode usar o [Editor de tag](#) no console da AWS para encontrar os recursos com um valor de tag de cor de azul.

Para obter mais informações sobre marcação no AWS IoT Wireless, consulte [Marcando seus Recursos AWS IoT Wireless](#).

Para ter mais informações sobre tags e estratégias de marcação, consulte [Editor de tags](#).

# AWS IoT Core for LoRaWAN

O AWS IoT Core for LoRaWAN é um Servidor da rede LoRaWAN (LNS) que oferece gerenciamento de gateway utilizando os recursos Servidor de Configuração e Atualização (CUPS) e atualização de firmware sem fios (FUOTA). É possível substituir o LNS privado pelo AWS IoT Core for LoRaWAN e conectar os dispositivos e gateways de rede de longa distância e longo alcance (LoRaWAN) ao AWS IoT Core. Ao fazer isso, você reduzirá a manutenção, os custos operacionais, o tempo de configuração e os custos indiretos.

## Note

O AWS IoT Core for LoRaWAN aceita somente o formato de endereço IPv4. Ele não é compatível com IPv6 ou com a configuração de pilha dupla (IPv4 e IPv6). Para obter mais informações, consulte [AWS service \(Serviço da AWS\)s compatíveis com IPv6](#).

## Introdução

Os dispositivos LoRaWAN são dispositivos de longo alcance, baixo consumo de energia e operados por bateria que usam o protocolo LoRaWAN para operar em um espectro de rádio sem licença. LoRaWAN é um protocolo de comunicação de rede de área ampla de baixa potência (LPWAN) criado em LoRa. LoRa é o protocolo de camada física que permite a comunicação de baixa potência e área ampla entre dispositivos.

Para conectar seus dispositivos LoRaWAN à AWS IoT, você deve usar um gateway LoRaWAN. O gateway atua como uma ponte para conectar o dispositivo ao AWS IoT Core for LoRaWAN e trocar mensagens. O AWS IoT Core for LoRaWAN utiliza o mecanismo de regras do AWS IoT para rotear as mensagens dos dispositivos LoRaWAN para outros serviços do AWS IoT.

Para reduzir o esforço de desenvolvimento e integrar rapidamente os dispositivos ao AWS IoT Core for LoRaWAN, é recomendável utilizar dispositivos finais certificados pela LoRaWAN. Para obter mais informações, consulte a página de [visão geral do produto AWS IoT Core for LoRaWAN](#). Para obter informações sobre como obter a certificação LoRaWAN de seus dispositivos, consulte [Certificação de produtos LoRaWAN](#).

## Como acessar o AWS IoT Core for LoRaWAN

É possível integrar rapidamente os dispositivos e gateways LoRaWAN ao AWS IoT Core for LoRaWAN utilizando o console ou a API do AWS IoT Wireless.

### Usar o console

Para integrar os dispositivos e gateways LoRaWAN utilizando o Console de gerenciamento da AWS, faça login no Console de gerenciamento da AWS e navegue até a página [AWS IoT Core for LoRaWAN](#) no console do AWS IoT. Com isso, é possível utilizar a seção Introdução para adicionar os gateways e os dispositivos ao AWS IoT Core for LoRaWAN. Para ter mais informações, consulte [Usar o console para integrar o dispositivo e o gateway ao AWS IoT Core for LoRaWAN](#).

### Como usar a API ou a CLI

É possível integrar dispositivos LoRaWAN e Sidewalk utilizando a API do [AWS IoT Wireless](#). A API do AWS IoT Wireless em que o AWS IoT Core for LoRaWAN se baseia é compatível com o SDK da AWS. Para obter mais informações, consulte [SDKs e Toolkits da AWS](#).

Você pode usar a AWS CLI para executar comandos para integrar e gerenciar gateways e dispositivos LoRaWAN. Para obter mais informações, consulte [referência de CLI de AWS IoT Wireless](#).

## Regiões e endpoints do AWS IoT Core for LoRaWAN

O AWS IoT Core for LoRaWAN é compatível com os endpoints da API do ambiente de gerenciamento e do plano de dados específicos da Região da AWS. Os endpoints da API do plano de dados são específicos para sua Conta da AWS e Região da AWS. Para obter mais informações sobre os endpoints AWS IoT Core for LoRaWAN, consulte [Endpoints AWS IoT Core for LoRaWAN](#) na Referência geral da AWS.

Para uma comunicação mais segura entre os dispositivos e o AWS IoT, conecte os dispositivos ao AWS IoT Core for LoRaWAN por meio do AWS PrivateLink em sua nuvem privada virtual (VPC) em vez de conectá-los pela internet pública. Para ter mais informações, consulte [AWS IoT Core for LoRaWAN e endpoint da VPC de interface \(AWS PrivateLink\)](#).

O AWS IoT Core for LoRaWAN tem cotas que se aplicam aos dados do dispositivo que são transmitidos entre os dispositivos e o TPS máximo para as operações de API AWS IoT Wireless. Para obter mais informações, consulte [AWS IoT Core for LoRaWAN quotas](#), na Referência geral da AWS.

# Definição de preço do AWS IoT Core for LoRaWAN

Se for um cliente novo, ao fazer login na AWS, você poderá começar a usar o AWS IoT Core for LoRaWAN gratuitamente utilizando o [nível gratuito da AWS](#). Com o AWS IoT Core for LoRaWAN, você só paga pelo que usa. Para obter informações sobre visão geral do produto e definição de preços, consulte [Preços do AWS IoT Core](#).

## O que é o AWS IoT Core for LoRaWAN?

O AWS IoT Core for LoRaWAN substitui um Servidor da rede LoRaWAN (LNS) privado conectando dispositivos e gateways LoRaWAN à AWS. Usando o mecanismo de regras de AWS IoT, você pode rotear mensagens recebidas de dispositivos LoRaWAN, onde elas podem ser formatadas e enviadas para outros serviços AWS IoT. Para proteger as comunicações dos dispositivos com o AWS IoT, o AWS IoT Core for LoRaWAN utiliza certificados X.509.

O AWS IoT Core for LoRaWAN gerencia as políticas de serviços e dispositivos que o AWS IoT Core exige para se comunicar com os gateways e dispositivos LoRaWAN. O AWS IoT Core for LoRaWAN também gerencia os destinos que descrevem as regras do AWS IoT que enviam dados do dispositivo para outros serviços.

## Recursos do AWS IoT Core for LoRaWAN

Com o AWS IoT Core for LoRaWAN, você pode:

- Integrar e conectar dispositivos e gateways LoRaWAN ao AWS IoT sem a necessidade de configurar e gerenciar um LNS privado.
- Conectar dispositivos LoRaWAN que estão em conformidade com as especificações LoRaWAN 1.0.x ou 1.1 padronizadas pela LoRa Alliance. Esses dispositivos podem operar no modo classe A, classe B ou classe C.
- Usar gateways LoRaWAN compatíveis com o LoRa Basics Station versão 2.0.4 ou posterior. Todos os gateways qualificados do AWS IoT Core for LoRaWAN executam uma versão compatível do LoRa Basics Station.
- Conecte os dispositivos LoRaWAN à nuvem utilizando redes LoRaWAN disponíveis ao público, o que reduz o tempo de implantação e elimina a necessidade de gerenciamento de uma rede LoRaWAN privada, economizando tempo e custo.
- Monitore a intensidade do sinal, a largura de banda e o fator de propagação utilizando a taxa de dados adaptativa do AWS IoT Core for LoRaWAN e otimize a taxa de dados, se necessário.

Também é possível utilizar o analisador de rede para monitorar os recursos LoRaWAN em tempo real.

- Atualizar o firmware dos gateways LoRaWAN usando o serviço CUPS e o firmware dos dispositivos LoRaWAN usando o Firmware Updates Over-The-Air (FUOTA).

Os tópicos a seguir fornecem informações adicionais sobre a tecnologia LoRaWAN e o AWS IoT Core for LoRaWAN.

Tópicos

- [O que é LoRaWAN?](#)
- [Como a AWS IoT Core for LoRaWAN funciona](#)

## O que é LoRaWAN?

A [LoRa Alliance](#) descreve o LoRaWAN como “um protocolo de rede de baixa potência e área ampla (LPWA) projetado para conectar sem fio 'objetos' operadas por bateria à Internet em redes regionais, nacionais ou globais e que visa aos principais requisitos da Internet das Coisas (IoT), como comunicação bidirecional, segurança de ponta a ponta, serviços de mobilidade e localização.”.

## LoRa e LoRaWAN

O LoRaWAN é um protocolo de comunicação de rede de área ampla de baixa potência (LPWAN) que funciona em LoRa.

O LoRaWAN foi reconhecido como um padrão internacional para redes de longa distância de baixa potência. Para obter mais informações, consulte [LoRAWAN formally recognized as ITU international standard](#). A especificação LoRaWAN está aberta para que qualquer pessoa possa configurar e operar uma rede LoRa.

LoRa é uma tecnologia de frequência de áudio que opera em um espectro de radiofrequência sem licença. LoRa é um protocolo de camada física que usa modulação de espectro espalhado e oferece suporte à comunicação de longo alcance ao custo de uma largura de banda estreita. Ele usa uma forma de onda de banda estreita com uma frequência central para enviar dados, o que o torna resistente a interferências.

## Características da tecnologia LoRaWAN

- Comunicação de longo alcance de até 10 milhas na linha de visão.

- Bateria de longa duração de até 10 anos. Para aumentar a duração da bateria, você pode operar seus dispositivos no modo classe A ou classe B, o que requer maior latência de downlink.
- Baixo custo para dispositivos e manutenção.
- Espectro de rádio sem licença, mas aplicam-se regulamentos específicos da região.
- Baixo consumo de energia, mas tem um tamanho de carga útil limitado de 51 bytes a 241 bytes, dependendo da taxa de dados. A taxa de dados pode ser de 0,3 Kbit/s a 27 Kbit/s com um tamanho máximo de carga útil de 222.

## Versões do protocolo LoRaWAN

A LoRa Alliance especifica o protocolo LoRaWAN utilizando documentos de especificação LoRaWAN. Para considerar os regulamentos específicos por região, a LoRa Alliance também publica documentos de parâmetros regionais. Para obter mais informações, consulte [LoRaWAN regional parameters and specifications](#).

A versão inicial do LoRaWAN é a 1.0. As versões adicionais são 1.0.1, 1.0.2, 1.0.3, 1.0.4 e 1.1. As versões 1.0.1 a 1.0.4 são comumente chamadas de 1.0.x.

## Saiba mais sobre o LoRaWAN

Os links a seguir contêm informações úteis sobre a tecnologia LoRaWAN e sobre o LoRa Basics Station, que é o software executado nos gateways LoRaWAN para conectar dispositivos finais ao AWS IoT Core for LoRaWAN.

- [LoRaWAN recognized as ITU International Standard](#)

O LoRaWAN foi reconhecido como um padrão internacional para redes de longa distância de baixa potência. O padrão é intitulado Recommendation ITU-T Y.4480: “Low power protocol for wide area wireless networks”.

- [Os fundamentos do LoRaWAN](#)

Os fundamentos do LoRaWAN contêm um vídeo introdutório que aborda os fundamentos do LoRaWAN e uma série de capítulos que ajudarão você a aprender sobre LoRa e LoRaWAN.

- [O que é o LoRaWAN](#)

A LoRa Alliance oferece uma visão geral técnica do LoRa e do LoRaWAN, incluindo um resumo das especificações do LoRaWAN em diferentes regiões.

- [LoRa Basics Station](#)

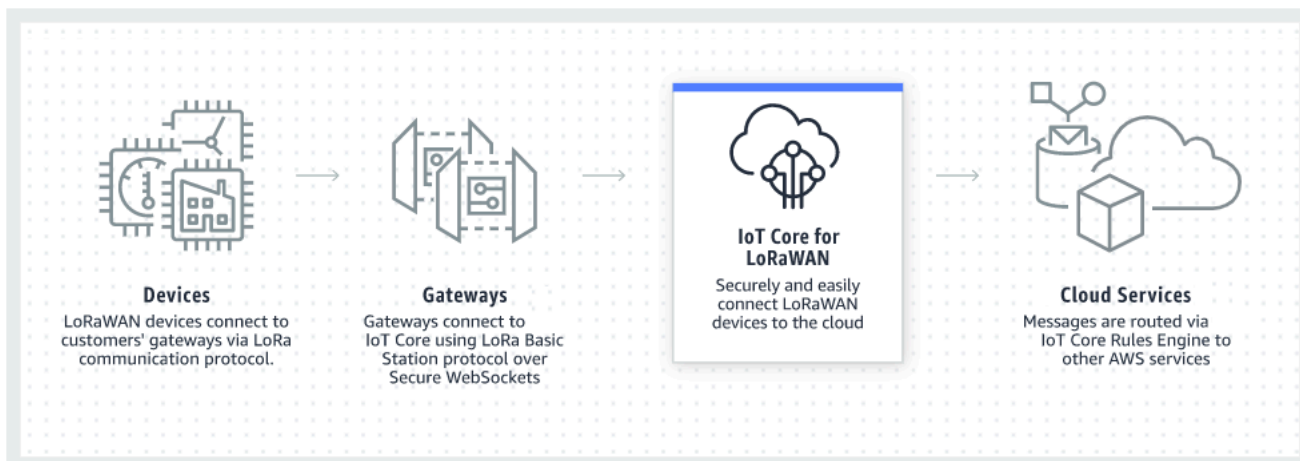
A Semtech Corporation apresenta conceitos úteis sobre os fundamentos do LoRa para gateways e nós finais. O LoRa Basics Station, um software de código aberto executado em seu gateway LoRaWAN, é mantido e distribuído por meio do repositório [GitHub](#) da Semtech Corporation. Você também pode aprender sobre os protocolos LNS e CUPS que descrevem como trocar dados LoRaWAN e realizar atualizações de configuração.

- [Parâmetros e especificações regionais do LoRaWAN](#)

O documento RP002-1.0.2 inclui suporte para todas as versões da especificação LoRaWAN Layer 2. Ele inclui informações sobre as especificações e parâmetros regionais do LoRaWAN e as diferentes versões do LoRaWAN.

## Como a AWS IoT Core for LoRaWAN funciona

A arquitetura de rede LoRaWAN é implantada em uma topologia de estrelas, na qual os gateways retransmitem informações entre os dispositivos finais e o servidor da rede LoRaWAN (LNS). O fluxograma a seguir mostra como um dispositivo LoRaWAN interage com o AWS IoT Core for LoRaWAN. Ele também mostra como o AWS IoT Core for LoRaWAN substitui um LNS e se comunica com outro AWS service (Serviço da AWS) na Nuvem AWS.



Os dispositivos LoRaWAN se comunicam com o AWS IoT Core por meio de gateways LoRaWAN. O AWS IoT Core for LoRaWAN gerencia as políticas de serviços e de dispositivos exigidas pelo AWS IoT Core para gerenciar e se comunicar com gateways e dispositivos LoRaWAN. O AWS IoT Core for LoRaWAN também gerencia os destinos que descrevem as regras do AWS IoT que enviam dados de dispositivos a outros serviços.

## Comece a usar o AWS IoT Core for LoRaWAN

As etapas a seguir mostram uma visão geral de como é possível começar a usar o AWS IoT Core for LoRaWAN.

1. Selecione os dispositivos sem fio e os gateways LoRaWAN de que você precisará.

O [AWS Partner Device Catalog](#) contém gateways e kits de desenvolvedor qualificados para uso com AWS IoT Core for LoRaWAN. Para ter mais informações, consulte [Usar gateways qualificados do AWS Partner Device Catalog](#).

2. Adicione os dispositivos sem fio e os gateways LoRaWAN ao AWS IoT Core for LoRaWAN.

O [Conectar gateways e dispositivos ao AWS IoT Core for LoRaWAN](#) oferece informações sobre como descrever os recursos e adicionar dispositivos sem fio e gateways LoRaWAN ao AWS IoT Core for LoRaWAN. Você também aprenderá a configurar os outros recursos do AWS IoT Core for LoRaWAN necessários para gerenciar esses dispositivos e enviar os dados aos serviços da AWS.

3. Complete a solução do AWS IoT Core for LoRaWAN.

Comece com [nossa solução de exemplo do AWS IoT Core for LoRaWAN](#) e adote-a.

## Recursos do AWS IoT Core for LoRaWAN

Os recursos a seguir ajudarão você a saber mais sobre o AWS IoT Core for LoRaWAN e como começar a usá-lo.

- [Conceitos básicos do AWS IoT Core for LoRaWAN](#)

O vídeo a seguir descreve como o AWS IoT Core for LoRaWAN funciona e fornece orientações sobre o processo de adição de gateways LoRaWAN utilizando o Console de gerenciamento da AWS.

- [AWS IoT Core for LoRaWAN Workshop](#)

O workshop aborda os fundamentos da tecnologia LoRaWAN e sua implementação com o AWS IoT Core for LoRaWAN. Também é possível utilizar o workshop para praticas em laboratórios que mostram como conectar o gateway e o dispositivo ao AWS IoT Core for LoRaWAN para criar um exemplo de solução de IoT.

- [Implementing Low-Power Wide-Area Network \(LPWAN\) Solutions with AWS IoT](#)

Esse artigo fornece uma estrutura de decisão para ajudar você a decidir se a LPWAN é a escolha certa para seu caso de uso de IoT, apresenta uma visão geral das tecnologias de conectividade LPWAN e dos respectivos recursos e oferece diretrizes de implementação.

## Conectar gateways e dispositivos ao AWS IoT Core for LoRaWAN

O AWS IoT Core for LoRaWAN ajuda você a conectar e gerenciar dispositivos sem fio LoRaWAN (rede de longa distância e baixo consumo de energia) e elimina a necessidade de desenvolver e operar um LNS. Dispositivos e gateways WAN de longo alcance (LoRaWAN) podem se conectar ao AWS IoT Core usando o AWS IoT Core for LoRaWAN.

## Convenções de nomenclatura para dispositivos, gateways, perfis e destinos

Antes de iniciar o AWS IoT Core for LoRaWAN e criar os recursos, considere a convenção de nomenclatura dos dispositivos, gateways e destino.

O AWS IoT Core for LoRaWAN atribui IDs exclusivos aos recursos que você cria para dispositivos sem fio, gateways e perfis. No entanto, você também pode dar aos recursos nomes mais descritivos para facilitar a identificação deles. Antes de adicionar dispositivos, gateways, perfis e destinos ao AWS IoT Core for LoRaWAN, considere como você os nomeará para facilitar o gerenciamento.

Você também pode adicionar tags aos recursos criados. Antes de adicionar dispositivos LoRaWAN, considere como você pode usar tags para identificar e gerenciar recursos do AWS IoT Core for LoRaWAN. As tags podem ser modificadas depois de adicionadas.

Para obter mais informações sobre nomenclatura e marcação, consulte [Descrever os recursos do AWS IoT Wireless](#).

## Mapeamento dos dados do dispositivo para os dados do serviço

Os dados dos dispositivos sem fio LoRaWAN geralmente são codificados para otimizar a largura de banda. Essas mensagens codificadas chegam ao AWS IoT Core for LoRaWAN em um formato que pode não ser facilmente usado por outros serviços da AWS. O AWS IoT Core for LoRaWAN usa regras de AWS IoT que podem usar funções AWS Lambda para processar e decodificar as mensagens do dispositivo em um formato que outros serviços da AWS podem usar.

Para transformar os dados do dispositivo e enviá-los a outros serviços da AWS, você precisa saber:

- O formato e o conteúdo dos dados que os dispositivos sem fio enviam.
- O serviço para o qual você deseja enviar os dados.
- O formato exigido pelo serviço.

Usando essas informações, você pode criar a regra de AWS IoT que executa a conversão e envia os dados convertidos para os serviços da AWS que os usarão.

## Usar o console para integrar o dispositivo e o gateway ao AWS IoT Core for LoRaWAN

Você pode usar a interface do console ou a API para adicionar o gateway e os dispositivos LoRaWAN. Se você estiver usando o AWS IoT Core for LoRaWAN pela primeira vez, recomendamos usar o console. A interface do console é mais prática ao gerenciar alguns recursos do AWS IoT Core for LoRaWAN por vez. Ao gerenciar um grande número de recursos do AWS IoT Core for LoRaWAN, considere criar soluções mais automatizadas usando a API AWS IoT Wireless.

Muitos dos dados que você insere ao configurar recursos do AWS IoT Core for LoRaWAN são dados pelos fornecedores dos dispositivos e são específicos para as especificações LoRaWAN compatíveis. Os tópicos a seguir descrevem como você pode descrever os recursos AWS IoT Core para LoRaWAN e usar o console ou a API para adicionar gateways e dispositivos.

### Note

Se estiver utilizando uma rede pública para conectar os dispositivos LoRaWAN à nuvem, você poderá ignorar a integração dos gateways. Para ter mais informações, consulte [Gerenciar o tráfego LoRaWAN de redes de dispositivos públicas LoRaWAN \(Everynet\)](#).

### Tópicos

- [Integre os gateways ao AWS IoT Core for LoRaWAN](#)
- [Integrar os dispositivos ao AWS IoT Core for LoRaWAN](#)

## Integre os gateways ao AWS IoT Core for LoRaWAN

Se estiver usando o AWS IoT Core for LoRaWAN pela primeira vez, você pode adicionar o primeiro gateway e dispositivo LoRaWAN usando o console.

**Note**

Se estiver utilizando uma rede pública para conectar os dispositivos LoRaWAN à nuvem, você poderá ignorar a integração dos gateways. Para ter mais informações, consulte [Gerenciar o tráfego LoRaWAN de redes de dispositivos públicas LoRaWAN \(Everynet\)](#).

## Antes de integrar o gateway

Antes de integrar o gateway ao AWS IoT Core for LoRaWAN, recomendamos que você:

- Use gateways qualificados para uso com o AWS IoT Core for LoRaWAN. Esses gateways se conectam ao AWS IoT Core sem nenhuma configuração adicional e usam a versão 2.0.4 ou posterior do software [LoRa Basics Station](#). Para ter mais informações, consulte [Gerenciar gateways com o AWS IoT Wireless](#).
- Considere a convenção de nomenclatura dos recursos que você cria para poder gerenciá-los com mais facilidade. Para ter mais informações, consulte [Descrever os recursos do AWS IoT Wireless](#).
- Tenha os parâmetros de configuração exclusivos de cada gateway prontos para serem inseridos com antecedência, o que facilita a inserção dos dados no console. Os parâmetros de configuração do gateway sem fio que a AWS IoT exige para se comunicar e gerenciar o gateway incluem o EUI do gateway e a banda de frequência LoRa.

Para integrar os gateways ao AWS IoT Core for LoRaWAN:

- [Considere a seleção da faixa de frequência e adicione o perfil do IAM necessário](#)
- [Adicionar um gateway ao AWS IoT Core for LoRaWAN](#)
- [Conecte o gateway LoRaWAN e verifique o status da conexão](#)

## Considere a seleção da faixa de frequência e adicione o perfil do IAM necessário

Antes de adicionar o gateway ao AWS IoT Core for LoRaWAN, recomendamos que você considere a faixa de frequência na qual o gateway estará operando e adicione o perfil do IAM necessário para conectar o gateway ao AWS IoT Core for LoRaWAN.

**Note**

Se você estiver adicionando o gateway usando o console, clique em Criar função no console para criar o perfil do IAM necessário para que você possa pular essas etapas. Você precisa executar essas etapas somente se estiver usando a CLI para criar o gateway.

Considere a seleção de faixas de frequência LoRa para os gateways e conexão de dispositivos

O AWS IoT Core for LoRaWAN é compatível com as faixas de frequência EU863-870, US902-928, AU915 e AS923-1, que você pode usar para conectar os gateways e dispositivos que estão fisicamente presentes em países que suportam as faixas de frequência e as características dessas faixas. As faixas EU863-870 e US902-928 são muito usadas na Europa e na América do Norte, respectivamente. A faixa AS923-1 é muito usada na Austrália, Nova Zelândia, Japão e Singapura, entre outros países. A AU915 é usada na Austrália e na Argentina, entre outros países. Para obter mais informações sobre qual faixa de frequência usar em sua região ou país, consulte [Parâmetros regionais LoRaWAN®](#).

A LoRa Alliance publica especificações LoRaWAN e documentos de parâmetros regionais que estão disponíveis para download no site da LoRa Alliance. Os parâmetros regionais da LoRa Alliance ajudam as empresas a decidir qual faixa de frequência usar em uma região ou país. A implementação da faixa de frequência do AWS IoT Core for LoRaWAN segue a recomendação no documento de especificação de parâmetros regionais. Esses parâmetros regionais são agrupados em um conjunto de parâmetros de rádio, junto com uma alocação de frequência adaptada à faixa Industrial, Científica e Médica (ISM). Recomendamos que você trabalhe com as equipes de conformidade para garantir o cumprimento de todos os requisitos regulamentares aplicáveis.

Adicione um perfil do IAM para permitir que o Servidor de Configuração e Atualização (CUPS) gerencie as credenciais do gateway

Esse procedimento descreve como adicionar um perfil do IAM para permitir que o Servidor de Configuração e Atualização (CUPS) gerencie as credenciais do gateway. Execute este procedimento antes que um gateway LoRaWAN tente se conectar ao AWS IoT Core for LoRaWAN. No entanto, você precisa fazer isso apenas uma vez.

Adicione o perfil do IAM para permitir que o Servidor de Configuração e Atualização (CUPS) gerencie as credenciais do gateway

1. Abra o [Hub de perfis do console do IAM](#) e escolha Criar perfil.

2. Se você acha que já adicionou o perfil `IoTWirelessGatewayCertManagerRole`, na barra de pesquisa, insira **`IoTWirelessGatewayCertManagerRole`**.

Se você vir um perfil `IoTWirelessGatewayCertManagerRole` nos resultados da pesquisa, você tem o perfil do IAM necessário. Você pode sair do procedimento agora.

Se os resultados da pesquisa estiverem vazios, você não tem o perfil do IAM necessário. Continue o procedimento para adicioná-lo.

3. Em Selecionar tipo de entidade confiável, escolha Outra Conta da AWS.
4. Em ID da conta, insira a ID da Conta da AWS e escolha Próximo: permissões.
5. Na caixa de pesquisa, insira **`AWSIoTWirelessGatewayCertManager`**.
6. Na lista de resultados da pesquisa, selecione a política chamada `AWSIoTWirelessGatewayCertManager`.
7. Escolha Próximo: tags e Próximo: revisar.
8. Em Nome do perfil, insira **`IoTWirelessGatewayCertManagerRole`** e selecione Criar perfil.
9. Para editar o novo perfil, na mensagem de confirmação, escolha `IoTWirelessGatewayCertManagerRole`.
10. Em Resumo, escolha a guia Relações de confiança e escolha Editar relações de confiança.
11. Em Documento de política, altere a propriedade `Principal` para ficar parecida com o exemplo a seguir.

```
"Principal": {
  "Service": "iotwireless.amazonaws.com"
},
```

Depois de alterar a propriedade `Principal`, o documento de política completo deve ser semelhante a este exemplo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "iotwireless.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
```

```
    "Condition": {}  
  }  
]  
}
```

12. Para salvar as alterações e sair, escolha Atualizar política de confiança.

Você criou, agora, o `IoTWirelessGatewayCertManagerRole`. Você não precisará fazer isso de novo.

Se você executou esse procedimento ao adicionar um gateway, poderá fechar essa janela e o console do IAM e retornar ao console de AWS IoT para concluir a adição do gateway.

## Adicionar um gateway ao AWS IoT Core for LoRaWAN

Você pode adicionar o gateway ao AWS IoT Core for LoRaWAN usando o console ou a CLI.

Antes de adicionar o gateway, recomendamos que você considere os fatores mencionados na seção [Antes de integrar o gateway do `Integre os gateways ao AWS IoT Core for LoRaWAN`](#).

Se você estiver adicionando o gateway pela primeira vez, recomendamos usar o console. Se quiser adicionar o gateway usando a CLI, você já deve ter criado o perfil do IAM necessário para que o gateway possa se conectar ao AWS IoT Core for LoRaWAN. Para obter informações sobre como criar o perfil, consulte [Adicione um perfil do IAM para permitir que o Servidor de Configuração e Atualização \(CUPS\) gerencie as credenciais do gateway](#).

### Adicionar um gateway usando o console

Navegue até a página de introdução do [AWS IoT Core for LoRaWAN](#) do console de AWS IoT, escolha Começar e, em seguida, escolha Adicionar gateway. Se você já adicionou um gateway, escolha Exibir gateway para ver o gateway que foi adicionado. Se quiser adicionar mais gateways, escolha Adicionar gateway.


#### 1. Dê detalhes do gateway e informações sobre a faixa de frequência

Use a seção Detalhes do gateway para dar informações sobre os dados de configuração do dispositivo, como o EUI do gateway e a configuração da faixa de frequência.

- EUI do gateway

O EUI (Identificador Único Estendido) do dispositivo de gateway individual. O EUI é um código alfanumérico de 16 dígitos, por exemplo, `c0ee40ffff29df10`, que identifica exclusivamente

um gateway na rede LoRaWAN. Essas informações são específicas do modelo de gateway e você pode encontrá-las no dispositivo de gateway ou no manual do usuário.

 Note

O EUI do gateway é diferente do endereço MAC Wi-Fi que você pode ver impresso no dispositivo de gateway. O EUI segue um padrão EUI-64 que identifica exclusivamente o gateway e, portanto, não pode ser reutilizado em outras Conta da AWSs e regiões.

- Faixa de frequência (RFRegion)

A faixa de frequência do gateway. Você pode escolher entre US915, EU868, AU915 ou AS923-1, dependendo do que o gateway suporta e de qual país ou região o gateway está se conectando fisicamente. Para obter mais informações sobre as faixas, consulte [Considere a seleção de faixas de frequência LoRa para os gateways e conexão de dispositivos](#).

## 2. Especifique os dados de configuração do gateway sem fio (opcional)

Esses campos são opcionais e você pode usá-los para dar informações adicionais sobre o gateway e a configuração dele.

- Nome, descrição e tags para o gateway

As informações nesses campos opcionais vêm de como você organiza e descreve os elementos no sistema sem fio. Você pode atribuir um Nome ao gateway, usar o campo Descrição para dar informações sobre o gateway e usar Tags para adicionar pares de chave-valor de metadados sobre o gateway. Para obter mais informações sobre como nomear e descrever os recursos, consulte [Descrever os recursos do AWS IoT Wireless](#).

- Configuração do LoRaWAN usando sub-bandas e filtros

Se quiser, você também pode especificar dados de configuração do LoRaWAN, como as sub-bandas que você deseja usar e filtros que podem controlar o fluxo de tráfego. Neste tutorial, é possível pular esses campos. Para ter mais informações, consulte [Configurar as sub-bandas do gateway e os recursos de filtragem](#).

## 3. Associar qualquer objeto de AWS IoT ao gateway

Especifique se deseja criar algo de AWS IoT e associá-lo ao gateway. O conteúdo em AWS IoT pode facilitar a pesquisa e o gerenciamento dos dispositivos. Associar algo ao gateway permite que o gateway acesse outros atributos de AWS IoT Core.

## 4. Criar e baixar o certificado de gateway

Para autenticar o gateway para que ele possa se comunicar com segurança com AWS IoT, o gateway LoRaWAN deve apresentar uma chave privada e um certificado para AWS IoT Core for LoRaWAN. Crie um Certificado de gateway para que AWS IoT possa verificar a identidade do o gateway usando o padrão X.509.

Clique no botão Criar certificado e baixe os arquivos do certificado. Você os usará mais tarde para configurar o gateway.

#### 5. Copie os endpoints CUPS e LNS e baixe os certificados

O gateway LoRaWAN deve se conectar a um endpoint CUPS ou LNS ao estabelecer uma conexão com AWS IoT Core for LoRaWAN. Recomendamos usar o endpoint do CUPS, já que ele também oferece gerenciamento de configuração. Para verificar a autenticidade dos endpoints do AWS IoT Core for LoRaWAN, o gateway utilizará um certificado de confiança para cada um dos endpoints CUPS e LNS.

Clique no botão Copiar para copiar os endpoints do CUPS e do LNS. Você precisará dessas informações mais tarde para configurar o gateway. Em seguida, clique no botão Baixar certificados de confiança do servidor para baixar os certificados de confiança para os endpoints do CUPS e do LNS.

#### 6. Criar o perfil do IAM para as permissões do gateway

É necessário adicionar um perfil do IAM para permitir que o Servidor de Configuração e Atualização (CUPS) gerencie as credenciais do gateway.

##### Note

Nesta etapa, crie o perfil `IoTWirelessGatewayCertManager`. Ignore essas etapas se já tiver criado esse perfil. Execute este procedimento antes que um gateway LoRaWAN tente se conectar ao AWS IoT Core for LoRaWAN. No entanto, você precisa fazer isso apenas uma vez.

Para criar o perfil do IAM `IoTWirelessGatewayCertManager` para a conta, clique no botão Criar perfil. Se o perfil já existir, selecione-o na lista suspensa.

Clique em Enviar para concluir a criação do gateway.

## Adicione um gateway usando a API

Se você estiver adicionando um gateway pela primeira vez usando a API ou a CLI, deverá adicionar o perfil do IAM IoTWirelessGatewayCertManager para que o gateway possa se conectar ao AWS IoT Core for LoRaWAN. Para obter informações sobre como criar o perfil, consulte a seção [Adicione um perfil do IAM para permitir que o Servidor de Configuração e Atualização \(CUPS\) gerencie as credenciais do gateway](#) a seguir.

As listas a seguir descrevem as ações de API que executam as tarefas associadas à adição, atualização ou exclusão de um gateway LoRaWAN.

### Ações de API do AWS IoT Wireless para gateways AWS IoT Core for LoRaWAN

- [CreateWirelessGateway](#)
- [GetWirelessGateway](#)
- [ListWirelessGateways](#)
- [UpdateWirelessGateway](#)
- [DeleteWirelessGateway](#)

Para ver a lista completa das ações e dos tipos de dados disponíveis para criar e gerenciar recursos do AWS IoT Core for LoRaWAN, consulte a [Referência da API AWS IoT Wireless](#).

### Como utilizar a AWS CLI para adicionar um gateway

É possível utilizar a AWS CLI para criar um gateway sem fio com o comando [create-wireless-gateway](#). O exemplo a seguir cria um gateway de dispositivo LoRaWAN sem fio. Você também pode apresentar um arquivo `input.json` que contenha detalhes adicionais, como o certificado de gateway e as credenciais de provisionamento.

#### Note

Também é possível executar esse procedimento com a API usando os métodos na API da AWS que correspondam aos comandos da CLI mostrados aqui.

```
aws iotwireless create-wireless-gateway \  
  --lorawan GatewayEui="a1b2c3d4567890ab",RfRegion="US915" \  
  --certificates-path /path/to/certificates/
```

```
--name "myFirstLoRaWANGateway" \  
--description "Using my first LoRaWAN gateway"  
--cli-input-json input.json
```

Para obter informações sobre as CLIs que você pode usar, consulte [Referência da AWS CLI](#)

## Conecte o gateway LoRaWAN e verifique o status da conexão

Antes de verificar o status da conexão do gateway, você já deve ter adicionado o gateway e conectado ele ao AWS IoT Core for LoRaWAN. Para obter informações sobre como adicionar o gateway, consulte [Adicionar um gateway ao AWS IoT Core for LoRaWAN](#).

### Conectar o gateway ao AWS IoT Core for LoRaWAN

Depois de adicionar o gateway, conecte-se à interface de configuração do gateway para inserir as informações de configuração e os certificados de confiança.

Depois de adicionar as informações do gateway ao AWS IoT Core for LoRaWAN, adicione algumas informações do AWS IoT Core for LoRaWAN ao dispositivo do gateway. A documentação apresentada pelo fornecedor do gateway deve descrever o processo de carregamento dos arquivos de certificado no gateway e de configuração do dispositivo de gateway para se comunicar com o AWS IoT Core for LoRaWAN.

### Gateways qualificados para uso com o AWS IoT Core for LoRaWAN

Para obter instruções sobre como configurar o gateway LoRaWAN, consulte a seção [Configurar dispositivo de gateway](#) do workshop do AWS IoT Core for LoRaWAN. Aqui, você encontrará informações sobre instruções para conectar gateways qualificados para uso com o AWS IoT Core for LoRaWAN.

### Gateways compatíveis com o protocolo CUPS

As instruções a seguir mostram como conectar os gateways compatíveis com o protocolo CUPS.

1. Faça upload dos seguintes arquivos que você obteve ao adicionar o gateway.
  - Certificado de dispositivo de gateway e arquivos de chave privada.
  - Arquivo de certificado de confiança para o endpoint do CUPS, `cups.trust`.
2. Especifique o URL do endpoint do CUPS que você obteve antes. O endpoint será do formato `prefix.cups.lorawan.region.amazonaws.com:443`.

Para detalhes sobre como obter essas informações, consulte [Adicionar um gateway ao AWS IoT Core for LoRaWAN](#).

## Gateways compatíveis com o protocolo LNS

As instruções a seguir mostram como conectar os gateways compatíveis com o protocolo LNS.

1. Faça upload dos seguintes arquivos que você obteve ao adicionar o gateway.
  - Certificado de dispositivo de gateway e arquivos de chave privada.
  - Arquivo de certificado de confiança para o endpoint do LNS, `Ins.trust`.
2. Especifique o URL do endpoint do LNS que você obteve antes. O endpoint terá o formato `https://prefix.Ins.lorawan.region.amazonaws.com:443`.

Para detalhes sobre como obter essas informações, consulte [Adicionar um gateway ao AWS IoT Core for LoRaWAN](#).

Depois de conectar o gateway ao AWS IoT Core for LoRaWAN, você pode verificar o status da conexão e obter informações sobre quando o último uplink foi recebido usando o console ou a API.

### Verifique status da conexão do gateway usando o console

Para verificar o status da conexão usando o console, navegue até a página [Gateways](#) do console de AWS IoT e escolha o gateway adicionado. Na seção Detalhes específicos de LoRaWAN da página Detalhes do gateway, você verá o status da conexão e a data e hora em que o último uplink foi recebido.

### Verificar o status da conexão do gateway usando a API

Para verificar o status da conexão usando a API, use a API `GetWirelessGatewayStatistics`. Essa API não tem um corpo de solicitação e contém apenas um corpo de resposta que mostra se o gateway está conectado e quando o último uplink foi recebido.

```
HTTP/1.1 200
Content-type: application/json

{
  "ConnectionStatus": "Connected",
  "LastUplinkReceivedAt": "2021-03-24T23:13:08.476015749Z",
  "WirelessGatewayId": "30cbdcf3-86de-4291-bfab-5bfa2b12bad5"
```

```
}
```

## Integrar os dispositivos ao AWS IoT Core for LoRaWAN

Depois de integrar o gateway ao AWS IoT Core for LoRaWAN e verificar o status da conexão, você pode integrar os dispositivos sem fio. Para obter informações sobre como integrar os gateways, consulte [Integre os gateways ao AWS IoT Core for LoRaWAN](#).

Os dispositivos LoRaWAN usam um protocolo LoRaWAN para trocar dados com aplicativos hospedados na nuvem. O AWS IoT Core for LoRaWAN é compatível com dispositivos que estão em conformidade com as especificações LoRaWAN 1.0.x ou 1.1 padronizadas pela LoRa Alliance.

Um dispositivo LoRaWAN normalmente contém um ou mais sensores e agentes. Os dispositivos enviam dados de telemetria de uplink por meio de gateways LoRaWAN para AWS IoT Core for LoRaWAN. Os aplicativos hospedados na nuvem podem controlar os sensores enviando comandos de downlink para dispositivos LoRaWAN por meio de gateways LoRaWAN.

### Antes de integrar o dispositivo sem fio

Antes de integrar o dispositivo sem fio ao AWS IoT Core for LoRaWAN, você precisa ter as seguintes informações prontas com antecedência:

- Especificação LoRaWAN e configuração do dispositivo sem fio

Tenha os parâmetros de configuração exclusivos de cada dispositivo prontos para serem inseridos com antecedência, o que facilita a inserção dos dados no console. Os parâmetros específicos que você precisa inserir dependem da especificação LoRaWAN que o dispositivo usa. Para obter a lista completa das especificações e dos parâmetros de configuração, consulte a documentação de cada dispositivo.

- Nome e descrição do dispositivo (opcional)

As informações nesses campos opcionais vêm de como você organiza e descreve os elementos no sistema sem fio. Para obter mais informações sobre nomenclatura e descrição dos recursos, consulte [Descrever os recursos do AWS IoT Wireless](#).

- Perfis de dispositivos e serviços

Tenha alguns parâmetros de configuração de dispositivos sem fio prontos que sejam compartilhados por vários dispositivos e possam ser armazenados no AWS IoT Core for LoRaWAN como perfis de dispositivos e serviços. Os parâmetros de configuração são encontrados

na documentação do dispositivo ou no próprio dispositivo. Você deve identificar um perfil de dispositivo que corresponda aos parâmetros de configuração do dispositivo, ou criar um se necessário, antes de adicionar o dispositivo. Para ter mais informações, consulte [Adicionar perfis ao AWS IoT Core for LoRaWAN](#).

- Destino do AWS IoT Core for LoRaWAN

Cada dispositivo deve ser atribuído a um destino que processará as mensagens para enviar para AWS IoT e outros serviços. As regras de AWS IoT que processam e enviam as mensagens do dispositivo são específicas do formato da mensagem do dispositivo. Para processar as mensagens do dispositivo e enviá-las para o serviço correto, identifique o destino que você criará para usar com as mensagens do dispositivo e atribua-o ao dispositivo.

Para integrar o dispositivo sem fio ao AWS IoT Core for LoRaWAN

- [Adicione o dispositivo sem fio ao AWS IoT Core for LoRaWAN](#)
- [Adicionar perfis ao AWS IoT Core for LoRaWAN](#)
- [Adicionar destinos ao AWS IoT Core for LoRaWAN](#)
- [Criar regras para processar mensagens de dispositivo LoRaWAN](#)
- [Conecte o dispositivo LoRaWAN e verifique o status da conexão](#)

## Adicione o dispositivo sem fio ao AWS IoT Core for LoRaWAN

Se você estiver adicionando o dispositivo sem fio pela primeira vez, recomendamos usar o console. Navegue até a página Introdução ao [AWS IoT Core for LoRaWAN](#) do console de AWS IoT, escolha Iniciar e, em seguida, escolha Adicionar dispositivo. Se você já adicionou um dispositivo, escolha Exibir dispositivo para ver o gateway que foi adicionado. Se você quiser adicionar mais dispositivos, escolha Adicionar dispositivo.

Como alternativa, você também pode adicionar dispositivos sem fio da página [Dispositivos](#) do console de AWS IoT.

Adicione a especificação do dispositivo sem fio ao AWS IoT Core for LoRaWAN usando o console

Escolha uma Especificação de dispositivo sem fio com base no método de ativação e na versão LoRaWAN. Depois de selecionados, os dados são criptografados com uma chave que a AWS possui e gerencia para você.

### Modos de ativação OTAA e ABP

Antes que o dispositivo LoRaWAN possa enviar dados de uplink, é preciso concluir um processo chamado ativação ou adesão. Para ativar o dispositivo, você pode usar o OTAA (ativação sem fio) ou o ABP (ativação por personalização).

O ABP não exige adesão e usa chaves estáticas. Quando você usa o OTAA, o dispositivo LoRaWAN envia uma adesão e o servidor de rede pode permitir a solicitação. Recomendamos que você use o OTAA para ativar o dispositivo porque novas chaves de sessão são geradas para cada ativação, o que o torna mais seguro.

## Versão LoRaWAN

Quando você usa o OTAA, o dispositivo LoRaWAN e os aplicativos hospedados em nuvem compartilham as chaves raiz. Essas chaves raiz dependem de você estar ou não usando a versão v1.0.x ou v1.1. A v1.0.x tem apenas uma chave raiz, AppKey (chave de aplicativo), enquanto a v1.1 tem duas chaves raiz, AppKey (chave de aplicativo) e NwkKey (chave de rede). As chaves de sessão são derivadas com base nas chaves raiz de cada ativação. Tanto NwkKey quanto AppKey são valores hexadecimais de 32 dígitos dados pelo fornecedor sem fio.

## EUIs de dispositivos sem fio

Depois de selecionar a Especificação do dispositivo sem fio, você verá os parâmetros EUI (Extended Unique Identifier) do dispositivo sem fio exibidos no console. Você pode encontrar essas informações na documentação do dispositivo ou do fornecedor sem fio.

- DevEUI: valor hexadecimal de 16 dígitos exclusivo do dispositivo e encontrado no rótulo do dispositivo ou na documentação dele.
- AppEUI: valor hexadecimal de 16 dígitos exclusivo do servidor de junção e encontrado na documentação do dispositivo. No LoRaWAN versão v1.1, o AppEUI é chamado de JoinEUI.

Para obter mais informações sobre identificadores exclusivos, chaves de sessão e chaves raiz, consulte a documentação da [LoRa Alliance](#).

Adicione a especificação do dispositivo sem fio ao AWS IoT Core for LoRaWAN usando a API

Se estiver adicionando um dispositivo sem fio usando a API, você deverá criar o perfil de dispositivo e o perfil de serviço antes de criar o dispositivo sem fio. Você usará o perfil do dispositivo e a ID do perfil de serviço ao criar o dispositivo sem fio. Para obter informações sobre como criar esses perfis usando a API, consulte [Adicionar um perfil de dispositivo usando a API](#).

As listas a seguir descrevem as ações de API que realizam as tarefas associadas à adição, atualização ou exclusão de um perfil de serviço.

Ações da API AWS IoT Wireless para perfis de serviço

- [CreateWirelessDevice](#)
- [GetWirelessDevice](#)
- [ListWirelessDevices](#)
- [UpdateWirelessDevice](#)
- [DeleteWirelessDevice](#)

Para ver a lista completa das ações e dos tipos de dados disponíveis para criar e gerenciar recursos do AWS IoT Core for LoRaWAN, consulte a [Referência da API AWS IoT Wireless](#).

Como usar a AWS CLI para criar um dispositivo sem fio

Você pode usar a AWS CLI para criar um dispositivo sem fio usando o comando [create-wireless-device](#). O exemplo a seguir cria um dispositivo sem fio usando um arquivo input.json para inserir os parâmetros.

#### Note

Também é possível executar esse procedimento com a API usando os métodos na API da AWS que correspondam aos comandos da CLI mostrados aqui.

Conteúdo de input.json

```
{
  "Description": "My LoRaWAN wireless device"
  "DestinationName": "IoTWirelessDestination"
  "LoRaWAN": {
    "DeviceProfileId": "ab0c23d3-b001-45ef-6a01-2bc3de4f5333",
    "ServiceProfileId": "fe98dc76-cd12-001e-2d34-5550432da100",
    "OtaaV1_1": {
      "AppKey": "3f4ca100e2fc675ea123f4eb12c4a012",
      "JoinEui": "b4c231a359bc2e3d",
      "NwkKey": "01c3f004a2d6efffe32c4eda14bcd2b4"
    }
  },
}
```

```
    "DevEui": "ac12efc654d23fc2"
  },
  "Name": "SampleIoTWirelessThing"
  "Type": LoRaWAN
}
```

É possível fornecer este arquivo como entrada para o comando `create-wireless-device`.

```
aws iotwireless create-wireless-device \
  --cli-input-json file:///input.json
```

Para obter informações sobre as CLIs que você pode usar, consulte [Referência da AWS CLI](#)

## Adicionar perfis ao AWS IoT Core for LoRaWAN

Perfis de dispositivos e serviços podem ser definidos para descrever configurações comuns de dispositivos. Esses perfis descrevem os parâmetros de configuração que são compartilhados pelos dispositivos para facilitar a adição desses dispositivos. O AWS IoT Core for LoRaWAN é compatível com perfis de dispositivos e perfis de serviços.

Os parâmetros de configuração e os valores a serem inseridos nesses perfis são apresentados pelo fabricante do dispositivo.

### Adicionar perfis de dispositivos

Os perfis de dispositivos definem os recursos do dispositivo e os parâmetros de inicialização que o servidor de rede usa para definir o serviço de acesso por rádio LoRaWAN. Ele inclui a seleção de parâmetros como faixa de frequência LoRa, versão de parâmetros regionais LoRa e versão MAC do dispositivo. Para conhecer as diferentes faixas de frequência, consulte [Considere a seleção de faixas de frequência LoRa para os gateways e conexão de dispositivos](#).

### Adicionar um perfil de dispositivo usando o console

Se você estiver adicionando um dispositivo sem fio usando o console conforme descrito em [Adicione a especificação do dispositivo sem fio ao AWS IoT Core for LoRaWAN usando o console](#), depois de adicionar a especificação do dispositivo sem fio, você poderá adicionar o perfil do dispositivo. Se quiser, você também pode adicionar dispositivos sem fio da página [Perfis](#) do console de AWS IoT na guia LoRaWAN.

Você pode escolher entre os perfis de dispositivo padrão ou criar um novo perfil de dispositivo. Recomendamos que você use os perfis de dispositivo padrão. Se o aplicativo exigir que você crie um

perfil de dispositivo, dê um Nome de perfil de dispositivo, selecione a Faixa de frequência (RfRegion) que você está usando para o dispositivo e o gateway e mantenha as outras configurações nos valores padrão, a menos que especificado de outra forma na documentação do dispositivo.

Adicionar um perfil de dispositivo usando a API

Se estiver adicionando um dispositivo sem fio usando a API, você deverá criar o perfil de dispositivo antes de criar o dispositivo sem fio.

As listas a seguir descrevem as ações de API que realizam as tarefas associadas à adição, atualização ou exclusão de um perfil de serviço.

Ações da API AWS IoT Wireless para perfis de serviço

- [CreateDeviceProfile](#)
- [GetDeviceProfile](#)
- [ListDeviceProfiles](#)
- [UpdateDeviceProfile](#)
- [DeleteDeviceProfile](#)

Para ver a lista completa das ações e dos tipos de dados disponíveis para criar e gerenciar recursos do AWS IoT Core for LoRaWAN, consulte a [Referência da API AWS IoT Wireless](#).

Como usar a AWS CLI para criar um perfil de dispositivo

Você pode usar a AWS CLI para criar um perfil de dispositivo usando o comando [create-device-profile](#). O exemplo a seguir cria um perfil de dispositivo.

```
aws iotwireless create-device-profile
```

A execução desse comando cria automaticamente um perfil de dispositivo com uma ID que você pode usar ao criar o dispositivo sem fio. Agora você pode criar o perfil de serviço usando a seguinte API e, em seguida, criar o dispositivo sem fio usando os perfis de dispositivo e de serviço.

```
{
  "Arn": "arn:aws:iotwireless:us-east-1:123456789012:DeviceProfile/12345678-
a1b2-3c45-67d8-e90fa1b2c34d",
  "Id": "12345678-a1b2-3c45-67d8-e90fa1b2c34d"
}
```

Para obter informações sobre as CLIs que você pode usar, consulte [Referência da AWS CLI](#)

## Adicionar perfis de serviço

Os perfis de serviço descrevem os parâmetros de comunicação de que o dispositivo precisa para se comunicar com o servidor de aplicativos.

### Adicionar um perfil de serviço usando o console

Se estiver adicionando um dispositivo sem fio usando o console conforme descrito em [Adicione a especificação do dispositivo sem fio ao AWS IoT Core for LoRaWAN usando o console](#), depois de adicionar o perfil do dispositivo, você poderá adicionar o perfil de serviço. Se quiser, você também pode adicionar dispositivos sem fio da página [Perfis](#) do console de AWS IoT na guia LoRaWAN.

Recomendamos que você deixe a configuração AddGWMetaData ativada para receber metadados de gateway adicionais para cada carga útil, como RSSI e SNR para a transmissão de dados.

### Adicionar um perfil de serviço usando a API

Se você estiver adicionando um dispositivo sem fio usando a API, primeiro crie o perfil de serviço antes de criar o dispositivo sem fio.

As listas a seguir descrevem as ações de API que realizam as tarefas associadas à adição, atualização ou exclusão de um perfil de serviço.

### Ações da API AWS IoT Wireless para perfis de serviço

- [CreateServiceProfile](#)
- [GetServiceProfile](#)
- [ListServiceProfiles](#)
- [UpdateServiceProfile](#)
- [DeleteServiceProfile](#)

Para ver a lista completa das ações e dos tipos de dados disponíveis para criar e gerenciar recursos do AWS IoT Core for LoRaWAN, consulte a [Referência da API AWS IoT Wireless](#).

### Como usar a AWS CLI para criar um perfil de serviço

Você pode usar a AWS CLI para criar um serviço usando o comando [create-service-profile](#). O exemplo a seguir cria um perfil de serviço.

```
aws iotwireless create-service-profile
```

A execução desse comando cria automaticamente um perfil de serviço com uma ID que você pode usar ao criar o dispositivo sem fio. Agora você pode criar o dispositivo sem fio usando os perfis de dispositivo e de serviço.

```
{
  "Arn": "arn:aws:iotwireless:us-east-1:123456789012:ServiceProfile/12345678-
a1b2-3c45-67d8-e90fa1b2c34d",
  "Id": "12345678-a1b2-3c45-67d8-e90fa1b2c34d"
}
```

## Adicionar destinos ao AWS IoT Core for LoRaWAN

Os destinos do AWS IoT Core para LoRaWAN descrevem a regra de AWS IoT que processa os dados de um dispositivo para uso por serviços da AWS.

Como a maioria dos dispositivos LoRaWAN não envia dados para o AWS IoT Core para LoRaWAN em um formato que possa ser usado por serviços da AWS, uma regra de AWS IoT deve processá-los primeiro. A regra de AWS IoT contém a instrução SQL que interpreta os dados do dispositivo e as ações da regra de tópico que enviam o resultado da instrução SQL aos serviços que a usarão.

Se você estiver adicionando o destino pela primeira vez, recomendamos usar o console.

Adicionar um destino usando o console

Se você estiver adicionando um dispositivo sem fio usando o console conforme descrito em [Adicione a especificação do dispositivo sem fio ao AWS IoT Core for LoRaWAN usando o console](#), depois de já ter adicionado a especificação do dispositivo sem fio e perfis ao AWS IoT Core for LoRaWAN conforme descrito antes, você poderá ir em frente e adicionar um destino.

Se quiser, você também pode adicionar um destino de AWS IoT Core for LoRaWAN a partir da página [Destinos](#) do console de AWS IoT.

Para processar os dados de um dispositivo, especifique os campos a seguir ao criar um destino do AWS IoT Core para LoRaWAN e escolha Adicionar destino.

- Detalhes do destino

Insira um Nome de destino e uma descrição opcional para o destino.

- Nome da regra

A regra de AWS IoT configurada para avaliar as mensagens enviadas pelo seu dispositivo e processar os dados do dispositivo. O nome da regra será mapeado para o seu destino. O destino exige que a regra processe as mensagens recebidas. Você pode escolher que as mensagens sejam processadas invocando uma regra de AWS IoT ou publicando no agente de mensagens de AWS IoT.

- Se você escolher Inserir um nome de regra, digite um nome e escolha Copiar para copiar o nome da regra que você inserirá ao criar a regra de AWS IoT. Você pode escolher Criar regra para criar a regra agora ou navegar até o Hub de [regras](#) do console de AWS IoT e criar uma regra com esse nome.

Você também pode inserir uma regra e usar a configuração Avançada para especificar um nome de tópico. O nome do tópico é passado durante a invocação da regra e é acessado usando a expressão `topic` dentro da regra. Para obter mais informações sobre regras de AWS IoT, consulte <https://docs.aws.amazon.com/iot/latest/developerguide/iot-rules.html>.

- Se você escolher Publicar no agente de mensagens de AWS IoT, insira o nome de um tópico. Em seguida, você pode copiar o nome do tópico de MQTT e vários assinantes podem se inscrever nesse tópico para receber mensagens publicadas nele. Para ter mais informações, consulte <https://docs.aws.amazon.com/iot/latest/developerguide/topics.html>.

Para obter mais informações sobre as regras de AWS IoT para destinos, consulte [Criar regras para processar mensagens de dispositivo LoRaWAN](#).

- Nome do perfil

O perfil do IAM que concede permissões de dados do dispositivo para o acesso à regra, nomeada em Nome da regra. No console, é possível criar um novo perfil de serviço ou selecionar um já existente. Se você estiver criando um novo perfil de serviço, poderá inserir um nome de perfil (por exemplo, **IoTWirelessDestinationRole**) ou deixá-lo em branco para AWS IoT Core for LoRaWAN para gerar um novo nome de perfil. O AWS IoT Core for LoRaWAN, então, criará automaticamente o perfil do IAM com as devidas permissões em seu nome.

Para obter mais informações sobre os perfis do IAM, consulte [Usar perfis do IAM](#).

## Adicionar um destino usando a API

Se quiser adicionar um destino usando a CLI em vez disso, você já deverá ter criado a regra e o perfil do IAM para o destino. Para obter mais informações sobre os detalhes que um destino exige no perfil, consulte [Criar um perfil do IAM para os destinos](#).

A lista a seguir contém as ações da API que realizam as tarefas associadas à adição, atualização ou exclusão de um destino.

Ações de API AWS IoT Wireless para destinos

- [CreateDestination](#)
- [GetDestination](#)
- [ListDestinations](#)
- [UpdateDestination](#)
- [DeleteDestination](#)

Para ver a lista completa das ações e dos tipos de dados disponíveis para criar e gerenciar recursos do AWS IoT Core for LoRaWAN, consulte a [Referência da API AWS IoT Wireless](#).

Como usar a AWS CLI para adicionar um destino

Você pode usar a AWS CLI para adicionar um destino usando o comando [create-destination](#). O exemplo a seguir mostra como criar um destino inserindo um nome de regra usando `RuleName` como o valor para o parâmetro `expression-type`. Se você quiser especificar um nome de tópico para publicar ou assinar o agente de mensagens, altere o valor do parâmetro `expression-type` para `MqttTopicId`.

```
aws iotwireless create-destination \  
  --name IoTWirelessDestination \  
  --expression-type RuleName \  
  --expression IoTWirelessRule \  
  --role-arn arn:aws:iam::123456789012:role/IoTWirelessDestinationRole
```

A execução desse comando cria um destino com o nome de destino, nome da regra e nome do perfil especificados. Para obter informações sobre os nomes de regras e de perfis para destinos, consulte [Criar regras para processar mensagens de dispositivo LoRaWAN](#) e [Criar um perfil do IAM para os destinos](#).

Para obter informações sobre as CLIs que você pode usar, consulte [Referência da AWS CLI](#).

## Criar um perfil do IAM para os destinos

Os destinos do AWS IoT Core for LoRaWAN exigem perfis do IAM que dão ao AWS IoT Core for LoRaWAN as permissões necessárias para enviar dados para a regra de AWS IoT. Se esse perfil ainda não estiver definido, você deverá defini-lo para que ele apareça na lista de perfis.

Quando você usa o console para adicionar um destino, o AWS IoT Core for LoRaWAN cria automaticamente um perfil do IAM para você, conforme descrito antes neste tópico. Ao adicionar um destino usando a API ou a CLI, você deve criar o perfil do IAM para o destino.

Para criar uma política do IAM para o perfil de destino do AWS IoT Core for LoRaWAN

1. Abra o [Hub de políticas do console do IAM](#).
2. Escolha Criar política e escolha a guia JSON.
3. No editor, exclua qualquer conteúdo do editor e cole este documento de política.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:DescribeEndpoint",
        "iot:Publish"
      ],
      "Resource": "*"
    }
  ]
}
```

4. Escolha Revisar política e, em Nome, insira um nome para essa política. Você precisará desse nome para usar no próximo procedimento.

Você também pode descrever essa política em Descrição, se quiser.

5. Escolha Criar política.

Para criar um perfil do IAM para um destino do AWS IoT Core for LoRaWAN

1. Abra o [Hub de perfis do console do IAM](#) e escolha Criar perfil.
2. Em Selecionar tipo de entidade confiável, escolha Outra Conta da AWS.

3. Em ID da conta, insira a ID da Conta da AWS e escolha Próximo: permissões.
4. Na caixa de pesquisa, insira o nome da política do IAM que você criou no procedimento anterior.
5. Nos resultados da pesquisa, verifique a política do IAM que você criou no procedimento anterior.
6. Escolha Próximo: tags e Próximo: revisar.
7. Em Nome do perfil, insira o nome desse perfil e escolha Criar perfil.
8. Na mensagem de confirmação, escolha o nome da função que você criou para editar o novo perfil.
9. Em Resumo, escolha a guia Relações de confiança e escolha Editar relações de confiança.
10. Em Documento de política, altere a propriedade `Principal` para ficar parecida com o exemplo a seguir.

```
"Principal": {  
  "Service": "iotwireless.amazonaws.com"  
},
```

Depois de alterar a propriedade `Principal`, o documento de política completo deve ser semelhante a este exemplo.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "Service": "iotwireless.amazonaws.com"  
      },  
      "Action": "sts:AssumeRole",  
      "Condition": {}  
    }  
  ]  
}
```

11. Para salvar as alterações e sair, escolha Atualizar política de confiança.

Com esse perfil definido, você pode encontrá-lo na lista de perfis ao configurar os destinos do AWS IoT Core for LoRaWAN.

## Criar regras para processar mensagens de dispositivo LoRaWAN

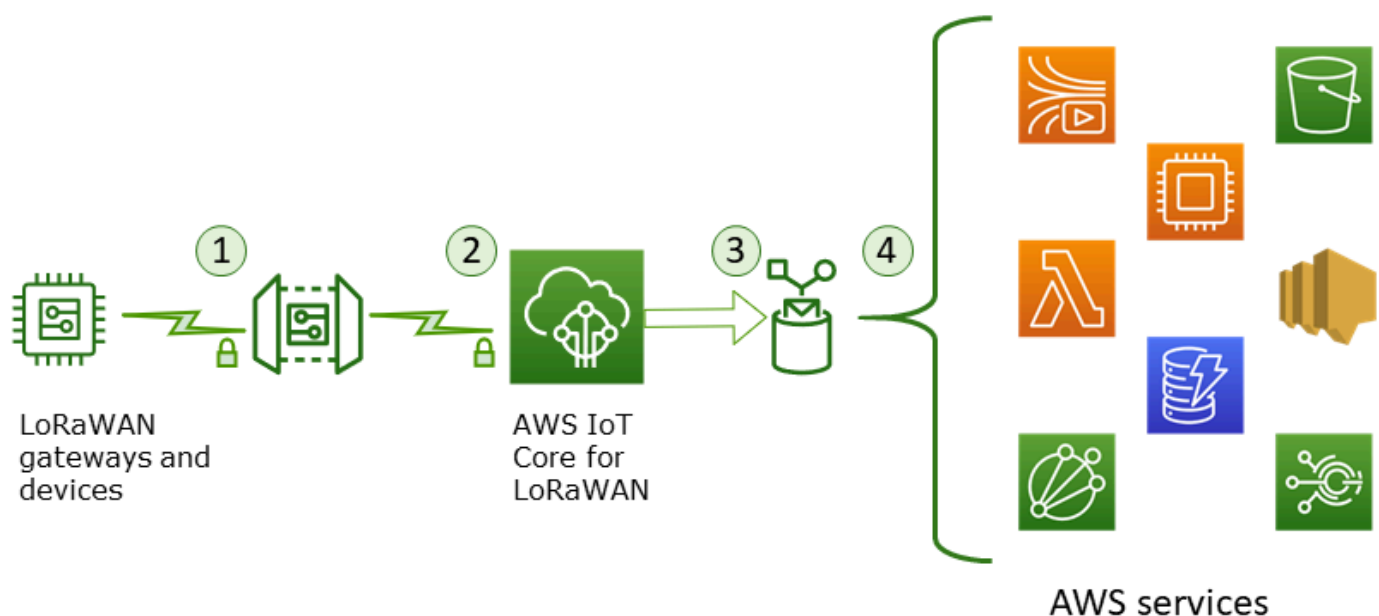
As regras de AWS IoT enviam mensagens de dispositivos a outros serviços. As regras de AWS IoT também podem processar as mensagens binárias recebidas de um dispositivo LoRaWAN para converter as mensagens em outros formatos que podem fazer com que elas sejam mais fáceis de serem usadas por outros serviços.

Os [destinos do AWS IoT Core for LoRaWAN](#) associam um dispositivo sem fio à regra que processa os dados de mensagens do dispositivo para enviar a outros serviços. A regra atua sobre os dados do dispositivo assim que AWS IoT Core for LoRaWAN a recebe. Os [destinos de AWS IoT Core for LoRaWAN](#) podem ser compartilhados por todos os dispositivos cujas mensagens têm o mesmo formato de dados e que enviam esses dados para o mesmo serviço.

Como as regras de AWS IoT processam as mensagens do dispositivo

A forma como uma regra de AWS IoT processa os dados da mensagem de um dispositivo depende do serviço que receberá os dados, do formato dos dados de mensagens do dispositivo e do formato de dados exigido pelo serviço. Normalmente, a regra chama uma função AWS Lambda para converter os dados de mensagens do dispositivo no formato exigido pelo serviço e, em seguida, envia o resultado para o serviço.

A ilustração a seguir mostra como os dados de mensagens são protegidos e processados à medida que são movidos do dispositivo sem fio para um serviço da AWS.



1. O dispositivo sem fio LoRaWAN criptografa as mensagens binárias usando o modo AES128 CTR antes de transmiti-las.
2. O AWS IoT Core for LoRaWAN descriptografa a mensagem binária e codifica a carga útil da mensagem binária descriptografada como uma string base64.
3. A mensagem resultante codificada em base64 é enviada como uma carga útil de mensagem (não é formatada como um documento JSON) à regra do AWS IoT descrita no destino atribuído ao dispositivo.
4. A regra de AWS IoT direciona os dados da mensagem para o serviço descrito na configuração da regra.

A carga útil binária criptografada recebida do dispositivo sem fio não é alterada nem interpretada por AWS IoT Core for LoRaWAN. A carga útil da mensagem binária descriptografada é codificada somente como uma string base64. Para que os serviços acessem os elementos de dados na carga útil da mensagem binária, os elementos de dados devem ser analisados quanto à carga útil por uma função chamada pela regra. A carga útil da mensagem codificada em base64 é uma string ASCII, portanto, ela pode ser armazenada como tal para ser analisada mais tarde.

### Criar regras para dispositivos LoRaWAN

O AWS IoT Core for LoRaWAN usa regras de AWS IoT para enviar com segurança mensagens do dispositivo diretamente para outros serviços da AWS sem a necessidade de usar o agente de mensagens. Ao remover o agente de mensagens do caminho de ingestão, ele reduz os custos e otimiza o fluxo de dados.

Para que uma regra do AWS IoT Core for LoRaWAN envie mensagens do dispositivo para outros serviços da AWS, ela requer um destino do AWS IoT Core for LoRaWAN e uma regra de AWS IoT atribuída a esse destino. A regra de AWS IoT deve conter uma instrução de consulta SQL e pelo menos uma ação de regra.

Normalmente, a instrução de consulta de regra de AWS IoT consiste em:

- Uma cláusula SQL SELECT que seleciona e formata os dados da carga útil da mensagem
- Um filtro de tópico (o objeto FROM na instrução de consulta de regra) que identifica as mensagens a serem usadas
- Uma declaração condicional opcional (uma cláusula SQL WHERE) que especifica condições sobre as quais agir

Confira a seguir um exemplo de declaração de consulta de regra:

```
SELECT temperature FROM iot/topic' WHERE temperature > 50
```

Ao criar regras de AWS IoT para processar cargas úteis de dispositivos LoRaWAN, você não precisa especificar a cláusula FROM como parte do objeto de consulta da regra. A instrução de consulta de regra deve ter a cláusula SQL SELECT e, como opção, pode ter a cláusula WHERE. Se a instrução de consulta usar a cláusula FROM, ela será ignorada.

Confira aqui um exemplo de uma instrução de consulta de regra que pode processar cargas úteis de dispositivos LoRaWAN:

```
SELECT WirelessDeviceId, WirelessMetadata.LoRaWAN.FPort as FPort,  
       WirelessMetadata.LoRaWAN.DevEui as DevEui,  
       PayloadData
```

Neste exemplo, PayloadData é uma carga útil binária codificada em base64 enviada pelo dispositivo LoRaWAN.

Confira aqui um exemplo de instrução de consulta de regra que pode realizar uma decodificação binária da carga útil recebida e transformá-la em um formato diferente, como JSON:

```
SELECT WirelessDeviceId, WirelessMetadata.LoRaWAN.FPort as FPort,  
       WirelessMetadata.LoRaWAN.DevEui as DevEui,  
       aws_lambda("arn:aws:lambda:<region>:<account>:function:<name>",  
                 {  
                   "PayloadData":PayloadData,  
                   "Fport": WirelessMetadata.LoRaWAN.FPort  
                 }) as decodingoutput
```

Para obter mais informações sobre como utilizar as cláusulas SELECT e WHERE, consulte <https://docs.aws.amazon.com/iot/latest/developerguide/iot-sql-reference.html>.

Para obter informações sobre as regras de AWS IoT e como criá-las e usá-las, consulte <https://docs.aws.amazon.com/iot/latest/developerguide/iot-rules.html> e <https://docs.aws.amazon.com/iot/latest/developerguide/iot-rules-tutorial.html>.

Para obter informações sobre como criar e usar destinos do AWS IoT Core for LoRaWAN, consulte [Adicionar destinos ao AWS IoT Core for LoRaWAN](#).

Para obter informações sobre o uso de cargas úteis de mensagens binárias em uma regra, consulte <https://docs.aws.amazon.com/iot/latest/developerguide/binary-payloads.html>.

Para obter mais informações sobre a segurança e a criptografia de dados usadas para proteger a carga útil da mensagem na jornada, consulte [Proteção de dados no AWS IoT Wireless](#).

Para ver uma arquitetura de referência que mostra um exemplo de decodificação e implementação binária para regras de IoT, consulte [Exemplos de soluções do AWS IoT Core for LoRaWAN no GitHub](#).

## Conecte o dispositivo LoRaWAN e verifique o status da conexão

Antes de verificar o status da conexão do dispositivo, você já deve ter adicionado o dispositivo e o conectado ao AWS IoT Core for LoRaWAN. Para obter informações sobre como adicionar um dispositivo, consulte [Adicione o dispositivo sem fio ao AWS IoT Core for LoRaWAN](#).

Depois de adicionar o dispositivo, consulte o manual do usuário do dispositivo para saber como iniciar o envio de uma mensagem de uplink do dispositivo LoRaWAN.

Verificar o status da conexão do dispositivo usando o console

Para verificar o status da conexão usando o console, navegue até a página [Dispositivos](#) do console de AWS IoT e escolha o dispositivo adicionado. Na seção Detalhes da página Detalhes dos dispositivos sem fio, você verá a data e a hora em que o último uplink foi recebido.

Verificar o status da conexão do dispositivo usando a API

Para verificar o status da conexão usando a API, use a API `GetWirelessDeviceStatistics`. Essa API não tem um corpo de solicitação e contém apenas um corpo de resposta que mostra quando o último uplink foi recebido.

```
HTTP/1.1 200
Content-type: application/json

{
  "LastUplinkReceivedAt": "2021-03-24T23:13:08.476015749Z",
  "LoRaWAN": {
    "DataRate": 5,
    "DevEui": "647fda0000006420",
    "Frequency": 868100000
    "Gateways": [
```

```
{
  "GatewayEui": "c0ee40ffff29df10",
  "Rssi": -67,
  "Snr": 9.75
},
"WirelessDeviceId": "30cbdcf3-86de-4291-bfab-5bfa2b12bad5"
}
```

## Próximas etapas

Agora que você conectou o dispositivo e verificou o status da conexão, é possível observar o formato dos metadados de uplink recebidos do dispositivo usando o [Cliente de teste MQTT](#) na página Testar do console de AWS IoT. Para ter mais informações, consulte [Visualizar o formato das mensagens de uplink enviadas a partir de dispositivos LoRaWAN](#).

## Configurar a posição dos recursos sem fio com o AWS IoT Core for LoRaWAN

Antes de usar esse atributo, observe que o provedor terceiro selecionado para resolver informações de posição para dispositivos LoRaWAN depende de feeds e conjuntos de dados fornecidos ou mantidos pelo Serviço Internacional de GNSS (IGS), EarthData via NASA ou outros terceiros. Esses feeds e conjuntos de dados são conteúdo de terceiros (conforme definido no contrato do cliente) e são fornecidos no estado em que se encontram. Para obter mais informações, consulte [Termos de serviço da AWS](#).

É possível utilizar o AWS IoT Core for LoRaWAN para especificar os dados de posição estática ou ativar o posicionamento para identificar a posição de um dispositivo em tempo real utilizando solucionadores de terceiros. É possível adicionar ou atualizar as informações de posição para dispositivos LoRaWAN ou gateways, ou ambos.

Especifique as informações de posição ao adicionar o dispositivo ou o gateway ao AWS IoT Core for LoRaWAN ou ao editar os detalhes da configuração de um dispositivo ou gateway. As informações de posição são especificadas como uma carga [GeoJSON](#). O formato GeoJSON é um formato usado para codificar estruturas de dados geográficos. A carga contém as coordenadas de latitude e longitude da localização do dispositivo, que são baseadas no [sistema de coordenadas do Sistema Geodésico Mundial \(WGS84\)](#).

Depois que os solucionadores calcularem a posição do recurso, se você tiver o Amazon Location Service, será possível ativar um mapa de localização da Amazon, onde será mostrada a posição do recurso. Com os dados de posição, você pode:

- Ativar o posicionamento para identificar e obter a posição de dispositivos LoRaWAN.
- Rastrear e monitorar a posição de gateways e dispositivos.
- Definir regras do AWS IoT que processem atualizações nos dados de posição e as encaminhem para outros AWS service (Serviço da AWS). Para obter uma lista de ações de regras, consulte [AWS IoT rule actions](#) no Guia do desenvolvedor do AWS IoT.
- Criar alertas e receber notificações em dispositivos em caso de atividade incomum usando os dados de posição e o Amazon SNS.

## Como funciona o posicionamento para dispositivos LoRaWAN

É possível ativar o posicionamento para identificar a posição de dispositivos usando solucionadores Wi-Fi e GNSS de terceiros. Essas informações podem ser utilizadas para rastrear e monitorar dispositivos. As etapas a seguir demonstram como ativar o posicionamento e visualizar as informações de posição de dispositivos LoRaWAN.

### Note

Os solucionadores de terceiros podem ser usados apenas com dispositivos LoRaWAN que possuam o chip [LoRa Edge](#). Não pode ser utilizado com gateways LoRaWAN. Para gateways, ainda é possível especificar as informações de posição estática e identificar a localização em um mapa de localização da Amazon.

### 1. Adicione o dispositivo

Antes de ativar o posicionamento, adicione o dispositivo ao AWS IoT Core for LoRaWAN. O dispositivo LoRaWAN deve possuir o chipset LoRa Edge, que é uma plataforma de potência ultrabaixa que integra um transceptor LoRa de longo alcance, um scanner GNSS de várias constelações e um scanner MAC Wi-Fi passivo voltado para aplicativos de geolocalização.

### 2. Ative o posicionamento

Para obter a posição em tempo real de dispositivos, ative o posicionamento. Quando o dispositivo LoRaWAN envia uma mensagem de uplink, os dados de verificação de Wi-Fi e

GNSS contidos na mensagem são enviados ao AWS IoT Core for LoRaWAN utilizando a porta do quadro de geolocalização.

### 3. Recupere informações de posição

Recupere a posição estimada do dispositivo a partir dos solucionadores calculados com base nos resultados da varredura dos transceptores. Se as informações de posição tiverem sido calculadas utilizando os resultados da verificação de Wi-Fi e GNSS, o AWS IoT Core for LoRaWAN selecionará a posição estimada com maior precisão.

### 4. Visualize informações de posição

Depois que o solucionador computar as informações de posição, ele também fornecerá as informações de precisão que indicam a diferença entre a posição calculada pelos solucionadores e as informações de posição estática inseridas. Também é possível visualizar a localização do dispositivo no mapa de localização da Amazon.

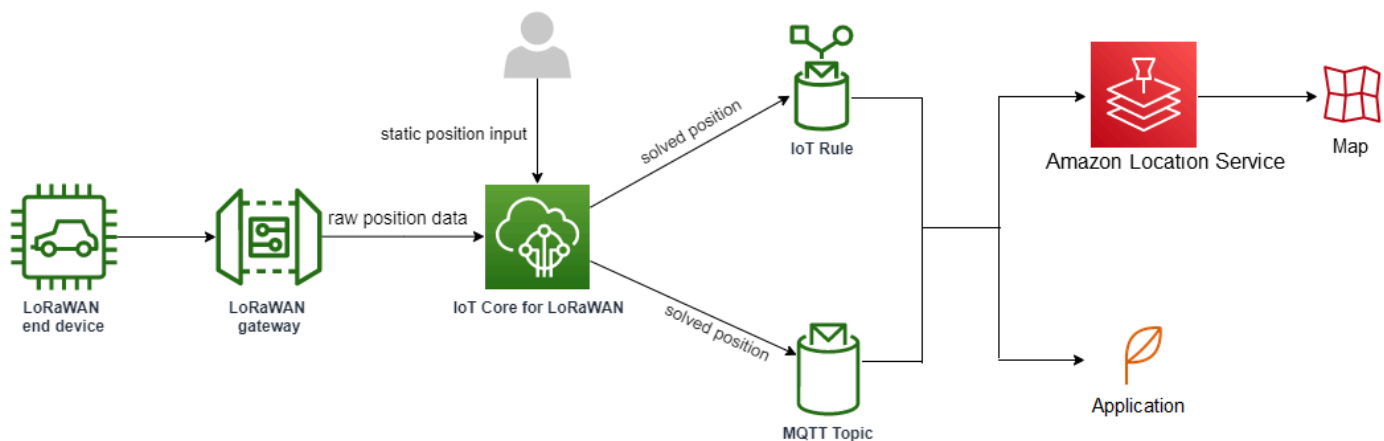
#### Note

Como os solucionadores não podem ser usados para gateways LoRaWAN, as informações de precisão serão relatadas como  $0.0$ .

Para acessar mais informações sobre o formato da mensagem de uplink e as portas de frequência que são usadas para o solucionador de posicionamento, consulte [Mensagem de uplink do AWS IoT Core for LoRaWAN para o mecanismo de regras](#).

## Visão geral do fluxo de trabalho do posicionamento

O diagrama a seguir mostra como o AWS IoT Core for LoRaWAN armazena e atualiza as informações de posição dos dispositivos e gateways.



### 1. Especifique a posição estática do recurso

Especifique as informações de posição estática do dispositivo ou gateway como uma carga GeoJSON usando as coordenadas de latitude e longitude. Também é possível especificar uma coordenada de altitude opcional. Essas coordenadas se baseiam no sistema de coordenadas WGS84. Para acessar mais informações, consulte [Sistema Geodésico Mundial \(WGS84\)](#).

### 2. Ative o posicionamento para dispositivos

Se estiver usando dispositivos LoRaWAN que possuem o chip LoRa Edge, é possível ativar, opcionalmente, o posicionamento para rastrear a posição do dispositivo em tempo real. Quando o dispositivo envia uma mensagem de uplink, os dados de verificação de Wi-Fi e GNSS são enviados ao AWS IoT Core for LoRaWAN utilizando a porta do quadro de geolocalização. Então, os solucionadores usam essas informações para solucionar a posição do dispositivo.

### 3. Adicione um destino aos dados de posição de rota

É possível adicionar um destino que descreva a regra do IoT para processar os dados do dispositivo e rotear as informações de posição atualizadas para o AWS IoT Core for LoRaWAN. Também é possível visualizar a última posição conhecida do recurso em um mapa de localização da Amazon.

## Configuração da posição de um recurso

É possível configurar a posição de um recurso utilizando o Console de gerenciamento da AWS, a API do AWS IoT Wireless ou a AWS CLI.

Se os dispositivos tiverem o chip do LoRa Edge, você poderá ativar o posicionamento para calcular as informações de posição em tempo real. Para os gateways, ainda é possível inserir as coordenadas de posição estática e usar a localização da Amazon para rastrear a posição do gateway em um mapa de localização da Amazon.

## Tópicos

- [Configuração da posição dos gateways LoRaWAN](#)
- [Configuração da posição de dispositivos LoRaWAN](#)

## Configuração da posição dos gateways LoRaWAN

Ao adicionar o gateway ao AWS IoT Core for LoRaWAN, é possível especificar os dados de posição estática. Caso tenha ativado os mapas do Amazon Location Service, os dados da posição serão exibidos em um mapa de localização da Amazon.

### Note

Solucionadores de terceiros não podem ser usados com gateways LoRaWAN. Para gateways, ainda é possível especificar as coordenadas da posição estática. Quando os solucionadores não são usados para calcular a posição, como no caso de gateways, as informações de precisão serão relatadas como 0.0.

É possível configurar a posição do gateway utilizando o Console de gerenciamento da AWS, a API do AWS IoT Wireless ou a AWS CLI.

## Configuração da posição de um gateway com o console

Para configurar a posição de recursos do gateway usando o Console de gerenciamento da AWS, faça login no console e, depois, acesse a página do hub [Gateways](#) do console do AWS IoT.

### Adicionar informações de posição

Para adicionar uma configuração de posição para um gateway

1. Na página do hub Gateways, selecione Adicionar gateway.
2. Informe a EUI do gateway, a banda de frequência (RFRegion) e quaisquer detalhes adicionais do gateway e informações de configuração do LoRaWAN. Para ter mais informações, consulte [Adicionar um gateway usando o console](#).

3. Navegue para a seção Informações de posição - Opcional e informe as informações de posição do gateway usando as coordenadas de latitude e longitude e uma coordenada de altitude opcional. As informações de posição se baseiam no sistema de coordenadas WGS84.

### Visualize a posição do gateway

Depois de configurar a posição do gateway, o AWS IoT Core for LoRaWAN cria um mapa do Amazon Location chamado `iotwireless.map`. É possível visualizar esse mapa na página de detalhes do gateway na guia Posição. Com base nas coordenadas de posição especificadas, a posição do gateway será exibida como um marcador no mapa. É possível ampliar ou reduzir o zoom para visualizar a posição do gateway no mapa com clareza. Na guia Posição, você também terá acesso às informações de precisão e registro de data/hora em que a posição do gateway foi determinada.

#### Note

Se não tiver mapas do Amazon Location Service instalados, será exibida uma mensagem indicando que você deve usar o Amazon Location Service para acessar o mapa e visualizar a posição do gateway. Usar mapas do Amazon Location Service pode incorrer em cobranças adicionais na sua Conta da AWS. Para obter mais informações, consulte [Definição de preços do AWS IoT Core](#).

O mapa `iotwireless.map` atua como uma fonte de dados de mapa que é acessada usando operações de API Get, como [GetMapTile](#). Para acessar mais informações sobre as APIs Get usadas com mapas, consulte [Referência de API do Amazon Location Service](#).

Para obter detalhes adicionais sobre esse mapa, vá para o console do Amazon Location Service, selecione mapas e, depois, selecione [iotwireless.map](#). Para acessar mais informações, consulte [Mapas](#) no Guia do desenvolvedor do Amazon Location Service.

### Atualize a configuração de posição do gateway

Para alterar a configuração da posição do gateway, na página de detalhes do gateway, selecione Editar e atualize as informações de posição e o destino.

**Note**

As informações de dados históricos de posição não estão disponíveis. Quando você atualiza as coordenadas de posição do gateway, os dados de posição relatados anteriormente são substituídos. Depois de atualizar a posição, na guia Posição dos detalhes do gateway, as informações da nova posição serão exibidas. A alteração no registro de data/hora indica que ela corresponde à última posição conhecida do gateway.

## Configurar a posição do gateway usando a API

É possível especificar as informações de posição e configurar a posição do gateway utilizando a API do AWS IoT Wireless ou a AWS CLI.

**Important**

As ações de API [UpdatePosition](#), [GetPosition](#), [PutPositionConfiguration](#), [GetPositionConfiguration](#) e [ListPositionConfigurations](#) não são mais compatíveis. Ao invés disso, as chamadas para atualizar e recuperar as informações de posição devem usar as operações de API [GetResourcePosition](#) e [UpdateResourcePosition](#).

### Adicionar informações de posição

Para adicionar as informações de posição estática de um gateway sem fio determinado, especifique as coordenadas usando a operação de API [UpdateResourcePosition](#) ou o comando [update-resource-position](#) da CLI. Especifique `WirelessGateway` como o `ResourceType`, o ID do gateway sem fio a ser atualizado como o `ResourceIdentifier` e as informações de posição como uma carga GeoJSON.

```
aws iotwireless update-resource-position \  
  --resource-type WirelessGateway \  
  --resource-id "12345678-a1b2-3c45-67d8-e90fa1b2c34d" \  
  --cli-input-json file://gatewayposition.json
```

O exemplo a seguir mostra o conteúdo do arquivo `gatewayposition.json`.

### Conteúdo do gatewayposition.json

```
{
  "type": "Point",
  "coordinates": [33.3318, -22.2155, 13.123],
  "properties": {
    "timestamp": "2018-11-30T18:35:24Z"
  }
}
```

A execução desse comando não retorna nenhuma saída. Para acessar as informações de posição especificadas, use a operação de API `GetResourcePosition`.

### Obter informações de posição

Para acessar as informações de posição de um gateway sem fio determinado, use a operação de API [GetResourcePosition](#) ou o comando [get-resource-position](#) da CLI. Especifique `WirelessGateway` como o `resourceType` e forneça o ID do gateway sem fio como o `resourceIdentifier`.

```
aws iotwireless get-resource-position \
  --resource-type WirelessGateway \
  --resource-id "12345678-a1b2-3c45-67d8-e90fa1b2c34d"
```

Executar esse comando exibe as informações de posição do gateway sem fio como uma carga GeoJSON. Você verá informações sobre as coordenadas de posição, o tipo de informação de posição e propriedades adicionais, tais como o registro de data/hora correspondente à última posição conhecida do gateway.

```
{
  {
    "type": "Point",
    "coordinates": [33.3318, -22.2155, 13.123],
    "properties": {
      "timestamp": "2018-11-30T18:35:24Z"
    }
  }
}
```

## Configuração da posição de dispositivos LoRaWAN

Ao adicionar o dispositivo ao AWS IoT Core for LoRaWAN, é possível especificar as informações de posição estática, opcionalmente ativar o posicionamento e especificar um destino. O destino descreve a regra de IoT que processa as informações de posição do dispositivo e encaminha a posição atualizada para o Amazon Location Service. Após configurar a posição do dispositivo, os dados de posição são exibidos em um mapa de localização da Amazon com as informações de precisão e o destino especificado.

É possível configurar a posição do dispositivo utilizando o Console de gerenciamento da AWS, a API do AWS IoT Wireless ou a AWS CLI.

### Portas de quadros e formato de mensagens de uplink

Se você ativar o posicionamento, será necessário especificar a porta do quadro de geolocalização para transmitir os dados de verificação de Wi-Fi e GNSS do dispositivo para o AWS IoT Core for LoRaWAN. As informações de posição são transmitidas ao AWS IoT Core for LoRaWAN utilizando essa porta de quadro.

A especificação LoRaWAN fornece um campo de entrega de dados (FRMPayload) e um campo Porta (FPort) para distinguir entre diferentes tipos de mensagens. Para comunicar as informações de posição, é possível especificar um valor entre 1 e 223 para a porta do quadro. A FPort 0 é reservada para mensagens MAC, a FPort 224 é reservada para testes de conformidade MAC e as portas 225-255 são reservadas para futuras extensões padronizadas de aplicativos.

### Mensagem de uplink do AWS IoT Core for LoRaWAN para o mecanismo de regras

Quando você adiciona um destino, ele cria uma regra do AWS IoT para rotear os dados para o Amazon Location Service com o mecanismo de regras. As informações de posição atualizadas são, então, exibidas em um mapa de localização da Amazon. Se você não tiver ativado o posicionamento, o destino direcionará os dados de posição quando você atualizar as coordenadas de posição estática do dispositivo.

O código a seguir mostra o formato da mensagem de uplink enviada do AWS IoT Core for LoRaWAN com as informações de posição, precisão, configuração do solucionador e metadados sem fio. Os campos que aparecem destacados abaixo são opcionais. Caso não haja informações de precisão vertical, o valor será `null`.

```
{  
  // Position configuration parameters for given wireless device
```

```
"WirelessDeviceId": "5b58245e-146c-4c30-9703-0ca942e3ff35",

// Position information for a device in GeoJSON format. Altitude
// is optional. If no vertical accuracy information is available
// or positioning isn't activated, the value is set to null.
// The position information coordinates are listed in the order
// [longitude, latitude, altitude].
"coordinates": [33.33000183105469, -22.219999313354492, 99.0],
"type": "Point",
"properties": {
  "horizontalAccuracy": number,
  "verticalAccuracy": number,
  "timestamp": "2022-08-19T03:08:35.061Z"
},

//Parameters controlled by AWS IoT Core for LoRaWAN
"WirelessMetadata":
{
  "LoRaWAN":
  {
    "ADR": false,
    "Bandwidth": 125,
    "ClassB": false,
    "CodeRate": "4/5",
    "DataRate": "0",
    "DevAddr": "00b96cd4",
    "DevEui": "58a0cb000202c99",
    "FOptLen": 2,
    "FCnt": 1,
    "Fport": 136,
    "Frequency": "868100000",
    "Gateways": [
      {
        "GatewayEui": "80029cffffe5cf1cc",
        "Snr": -29,
        "Rssi": 9.75
      }
    ],
    "MIC": "7255cb07",
    "MType": "UnconfirmedDataUp",
    "Major": "LoRaWANR1",
    "Modulation": "LORA",
    "PolarizationInversion": false,
    "SpreadingFactor": 12,
```

```
"Timestamp": "2021-05-03T03:24:29Z"  
  }  
}
```

## Configuração da posição de dispositivos com o console

Para configurar e gerenciar a posição de dispositivos usando o Console de gerenciamento da AWS, faça login no console e, depois, acesse a página do hub [Dispositivos](#) do console do AWS IoT.

### Adicionar informações de posição

Para adicionar informações de posição do dispositivo:

1. Na página do hub Dispositivos, selecione Adicionar dispositivo sem fio.
2. Informe a especificação do dispositivo sem fio, os perfis do dispositivo e do serviço e o destino que define a regra de IoT para roteamento dos dados para outros AWS service (Serviço da AWS). Para ter mais informações, consulte [Integrar os dispositivos ao AWS IoT Core for LoRaWAN](#).
3. Insira as informações de posição, opcionalmente ative a geolocalização e especifique um destino de dados de posição que deseje usar para rotear mensagens.
  - Informações de posição

Especifique os dados de posição do dispositivo usando as coordenadas de latitude e longitude e uma coordenada de altitude opcional. As informações de posição se baseiam no sistema de coordenadas WGS84.

- Geolocalização

Ative o posicionamento se quiser que o AWS IoT Core for LoRaWAN utilize a geolocalização para calcular a posição do dispositivo. Ele usa solucionadores GNSS e Wi-Fi de terceiros para identificar a posição do dispositivo em tempo real.

Para inserir as informações de geolocalização, selecione Ativar posicionamento e insira a porta do quadro de geolocalização para transmitir os dados de verificação de GNSS e Wi-Fi ao AWS IoT Core for LoRaWAN. Você verá as FPorts padrão preenchidas para sua referência. Entretanto, é possível escolher um valor diferente entre 1 e 223.

- Destino dos dados de posição

Escolha um destino para descrever a regra do AWS IoT que processa os dados de posição do dispositivo e os encaminha ao AWS IoT Core for LoRaWAN. Use esse destino apenas para rotear dados de posição. Ele deve ser diferente do destino usado para rotear dados do dispositivo para outros AWS service (Serviço da AWS).

### Visualize a configuração de posição do dispositivo

Depois de configurar a posição do dispositivo, o AWS IoT Core for LoRaWAN cria um mapa do Amazon Location chamado `iotwireless.map`. É possível visualizar esse mapa na página de detalhes do dispositivo na guia Posição. Com base nas coordenadas de posição especificadas ou na posição calculada pelos solucionadores de terceiros, a posição do dispositivo será exibida como um marcador no mapa. É possível ampliar ou reduzir o zoom para visualizar a posição do dispositivo no mapa com clareza. Na página de detalhes do dispositivo, na guia Posição, também é possível ver as informações de precisão, o registro de data/hora em que a posição do seu dispositivo foi determinada e o destino dos dados de posição especificados.

#### Note

Se não tiver ativado os mapas do Amazon Location Service, será exibida uma mensagem indicando que você precisará usar o Amazon Location Service para acessar o mapa e visualizar a posição. Usar mapas do Amazon Location Service pode incorrer em cobranças adicionais na sua Conta da AWS. Para obter mais informações, consulte [Definição de preços do AWS IoT Core](#).

O mapa `iotwireless.map` atua como uma fonte de dados de mapa que é acessada usando operações de API Get, como [GetMapTile](#). Para acessar mais informações sobre as APIs Get usadas com mapas, consulte [Referência de API do Amazon Location Service](#).

Para obter detalhes adicionais sobre esse mapa, vá para o console do Amazon Location Service, selecione mapas e, depois, selecione [iotwireless.map](#). Para acessar mais informações, consulte [Mapas](#) no Guia do desenvolvedor do Amazon Location Service.

### Atualize a configuração de posição do dispositivo

Para alterar a configuração da posição do dispositivo, na página de detalhes do dispositivo, selecione Editar e, em seguida, atualize as informações de posição, configurações de geolocalização e o destino.

**Note**

As informações de dados históricos de posição não estão disponíveis. Quando você atualiza as coordenadas de posição do dispositivo, os dados de posição relatados anteriormente são substituídos. Depois de atualizar a posição, na guia Posição dos detalhes do dispositivo, as informações da nova posição serão exibidas. A alteração no registro de data/hora indica que ela corresponde à última posição conhecida do dispositivo.

## Configurar a posição do dispositivo usando a API

É possível especificar as informações de posição, configurar a posição do dispositivo e ativar a geolocalização opcional utilizando a API do AWS IoT Wireless ou a AWS CLI.

**Important**

As ações de API [UpdatePosition](#), [GetPosition](#), [PutPositionConfiguration](#), [GetPositionConfiguration](#) e [ListPositionConfigurations](#) não são mais compatíveis. Ao invés disso, as chamadas para atualizar e recuperar as informações de posição devem usar as operações de API [GetResourcePosition](#) e [UpdateResourcePosition](#).

## Adicionar informações de posição e configuração

Para adicionar as informações de posição de um dispositivo sem fio determinado, especifique as coordenadas usando a operação de API [UpdateResourcePosition](#) ou o comando [update-resource-position](#) da CLI. Especifique `WirelessDevice` como o `ResourceType`, o ID do dispositivo sem fio a ser atualizado como o `ResourceIdentifier` e as informações de posição.

```
aws iotwireless update-resource-position \  
  --resource-type WirelessDevice \  
  --resource-id "1ffd32c8-8130-4194-96df-622f072a315f" \  
  --position [33.33, -33.33, 10.0]
```

O exemplo a seguir mostra o conteúdo do arquivo `deviceposition.json`. Para especificar os valores de FPort para enviar os dados de geolocalização, use o objeto [Posicionamento](#) com as operações de API [CreateWirelessDevice](#) e [UpdateWirelessDevice](#).

## Conteúdo do deviceposition.json

```
{
  "type": "Point",
  "coordinates": [33.3318, -22.2155, 13.123],
  "properties": {
    "verticalAccuracy": 707,
    "horizontalAccuracy":
    "timestamp": "2018-11-30T18:35:24Z"
  }
}
```

A execução desse comando não retorna nenhuma saída. Para acessar as informações de posição especificadas, use a operação de API `GetResourcePosition`.

Obtenha informações de posição e configuração

Para acessar as informações de posição de um dispositivo sem fio determinado, use a API [GetResourcePosition](#) ou o comando [get-resource-position](#) da CLI. Especifique `WirelessDevice` como o `resourceType` e forneça o ID do dispositivo sem fio como o `resourceIdentifier`.

```
aws iotwireless get-resource-position \
  --resource-type WirelessDevice \
  --resource-id "1ffd32c8-8130-4194-96df-622f072a315f"
```

Executar esse comando exibe as informações de posição do dispositivo sem fio como uma carga GeoJSON. Você verá informações sobre coordenadas de posição, tipo de localização e propriedades que podem incluir informações de precisão e o registro de data/hora correspondente à última posição conhecida do dispositivo.

```
{
  "type": "Point",
  "coordinates": [33.3318, -22.2155, 13.123],
  "properties": {
    "verticalAccuracy": 707,
    "horizontalAccuracy": 389,
    "horizontalConfidenceLevel": 0.68,
    "verticalConfidenceLevel": 0.68,
    "timestamp": "2018-11-30T18:35:24Z"
  }
}
```

# Gerenciar gateways com o AWS IoT Wireless

A seguir estão algumas considerações importantes ao usar os gateways com AWS IoT Core for LoRaWAN. Para obter informações sobre como adicionar o gateway a AWS IoT Core for LoRaWAN, consulte [Integre os gateways ao AWS IoT Core for LoRaWAN](#).

## Requisito de software LoRa Basics Station

Para se conectar a AWS IoT Core for LoRaWAN, o gateway LoRaWAN deve ter um software chamado [LoRa Basics Station](#) em execução nele. O LoRa Basics Station é um software de código aberto mantido pela Semtech Corporation e distribuído pelo repositório [GitHub](#). O AWS IoT Core for LoRaWAN é compatível com o LoRa Basics Station versão 2.0.4 e posterior. A versão mais recente é 2.0.6.

## Usar gateways qualificados do AWS Partner Device Catalog

O [AWS Partner Device Catalog](#) contém gateways e kits de desenvolvedor qualificados para uso com AWS IoT Core for LoRaWAN. Recomendamos que você use esses gateways qualificados porque você não precisa modificar o software de incorporação para conectar os gateways a AWS IoT Core. Esses gateways já têm uma versão do software BasicStation compatível com AWS IoT Core for LoRaWAN.

### Note

Se você tiver um gateway que não esteja listado no Catálogo de Parceiros como um gateway qualificado com AWS IoT Core for LoRaWAN, você ainda poderá usá-lo se o gateway estiver executando o software LoRa Basics Station com a versão 2.0.4 e posterior. Use a Autenticação de servidor e cliente TLS para autenticar o gateway LoRaWAN.

## Usar protocolos CUPS e LNS

O software LoRa Basics Station contém dois subprotocolos para conectar gateways a servidores de rede, os protocolos Servidor da Rede LoRaWAN (LNS) e Configuration and Update Server (CUPS).

O protocolo LNS estabelece uma conexão de dados entre um gateway compatível com LoRa Basics Station e um servidor de rede. As mensagens de uplink e downlink LoRa são trocadas por meio dessa conexão de dados em WebSockets seguros.

O protocolo CUPS permite o gerenciamento de credenciais, a configuração remota e a atualização do firmware dos gateways. AWS IoT Core for LoRaWAN oferece endpoints LNS e CUPS para ingestão de dados LoRaWAN e gerenciamento remoto de gateway, respectivamente.

Para obter mais informações, consulte [Protocolo LNS](#) e [Protocolo CUPS](#).

## Tópicos

- [Configure os recursos de beaconing e filtragem dos gateways LoRaWAN](#)
- [Atualize o firmware do gateway usando o serviço CUPS com AWS IoT Core for LoRaWAN](#)
- [Escolher gateways para receber o tráfego de dados de downlink LoRaWAN](#)

## Configure os recursos de beaconing e filtragem dos gateways LoRaWAN

Ao trabalhar com dispositivos LoRaWAN, você pode configurar certos parâmetros opcionais para os gateways LoRaWAN. Os parâmetros incluem:

- Beaconing

Você pode configurar parâmetros de beaconing para os gateways LoRaWAN que estão atuando como uma ponte para os dispositivos LoRaWAN de classe B. Esses dispositivos recebem uma mensagem de downlink em horários programados, portanto, você deve configurar os parâmetros de beaconing para que os gateways transmitam esses beacons sincronizados com o horário.

- Filtrar

Você pode configurar os parâmetros NetID e JoinEUI para os gateways LoRaWAN para filtrar o tráfego de dados do dispositivo. A filtragem do tráfego ajuda a conservar o uso da largura de banda e reduz o fluxo de tráfego entre os gateways e o LNS.

- Sub-bandas

Você pode configurar as sub-bandas do gateway para especificar a sub-banda específica que deseja usar. Para dispositivos sem fio que não podem alternar entre as várias sub-bandas, você pode usar esse recurso para se comunicar com os dispositivos usando somente os canais de frequência dessa sub-banda específica.

Os tópicos a seguir contêm mais informações sobre esses parâmetros e como configurá-los. Os parâmetros de beaconing não estão disponíveis no Console de gerenciamento da AWS e só podem ser especificados usando a API AWS IoT Wireless ou a AWS CLI.

## Tópicos

- [Configurar os gateways para enviar beacons para dispositivos de classe B](#)
- [Configurar as sub-bandas do gateway e os recursos de filtragem](#)

## Configurar os gateways para enviar beacons para dispositivos de classe B

Se você integrar dispositivos sem fio de classe B a AWS IoT Core for LoRaWAN, os dispositivos receberão mensagens de downlink em horários programados. Os dispositivos abrem esses slots com base em beacons sincronizados com o tempo que são transmitidos pelo gateway. Para que os gateways transmitam esses beacons sincronizados com o tempo, você pode usar AWS IoT Core for LoRaWAN para configurar determinados parâmetros relacionados a beaconing para os gateways.

Para configurar esses parâmetros de beaconing, o gateway deve estar executando o software LoRa Basics Station versão 2.0.6. Consulte [Usar gateways qualificados do AWS Partner Device Catalog](#).

Como configurar os parâmetros de beaconing

### Note

Você só precisa configurar os parâmetros de beaconing do gateway se ele estiver se comunicando com um dispositivo sem fio de classe B.

Você configura os parâmetros de beaconing ao adicionar o gateway a AWS IoT Core for LoRaWAN usando a operação de API [CreateWirelessGateway](#). Ao invocar a operação da API, especifique os seguintes parâmetros usando o objeto `Beaconing` para os gateways. Depois de configurar os parâmetros, os gateways enviarão os beacons aos dispositivos em um intervalo de 128 segundos.

- `DataRate`: a taxa de dados dos gateways que estão transmitindo os beacons.
- `Frequencies`: a lista de frequências dos gateways para transmitir os beacons.

O exemplo a seguir mostra como configurar esses parâmetros para o gateway. O arquivo `input.json` conterá outros detalhes, como o certificado do gateway e as credenciais de provisionamento. Para obter mais informações sobre como adicionar o gateway a AWS IoT Core for LoRaWAN usando a operação da API `CreateWirelessGateway`, consulte [Adicione um gateway usando a API](#).

**Note**

Os parâmetros de beaconing não estão disponíveis quando você adiciona o gateway a AWS IoT Core for LoRaWAN usando o console AWS IoT.

```
aws iotwireless create-wireless-gateway \  
  --name "myLoRaWANGateway" \  
  --cli-input-json file://input.json
```

O exemplo a seguir mostra o conteúdo do arquivo `input.json`.

Conteúdo de `input.json`

```
{  
  "Description": "My LoRaWAN gateway",  
  "LoRaWAN": {  
    "Beaconing": {  
      "DataRate": 8,  
      "Frequencies": ["923300000", "923900000"]  
    },  
    "GatewayEui": "a1b2c3d4567890ab",  
    "RfRegion": "US915",  
    "JoinEuiFilters": [  
      ["0000000000000001", "00000000000000ff"],  
      ["000000000000ff00", "000000000000ffff"]  
    ],  
    "NetIdFilters": ["000000", "000001"],  
    "RfRegion": "US915",  
    "SubBands": [2]  
  }  
}
```

O código a seguir mostra um exemplo de saída para a execução deste comando.

```
{  
  "Arn": "arn:aws:iotwireless:us-east-1:400232685877aa:WirelessGateway/a01b2c34-  
d44e-567f-abcd-0123e445663a",  
  "Id": "a01b2c34-d44e-567f-abcd-0123e445663a"  
}
```

## Obter informações sobre os parâmetros de beaconing

Você pode obter informações sobre os parâmetros de beaconing do gateway usando a operação da API [GetWirelessGateway](#).

### Note

Se um gateway já tiver sido integrado, você não poderá usar a operação da API `UpdateWirelessGateway` para configurar os parâmetros de beaconing. Para configurar os parâmetros, você deve excluir o gateway e depois especificar os parâmetros ao adicionar o gateway usando a operação da API `CreateWirelessGateway`.

```
aws iotwireless get-wireless-gateway \  
  --identifier "12345678-a1b2-3c45-67d8-e90fa1b2c34d" \  
  --identifier-type WirelessGatewayId
```

A execução desse comando retorna informações sobre o gateway e os parâmetros de beaconing.

## Configurar as sub-bandas do gateway e os recursos de filtragem

Os gateways LoRaWAN executam um software [LoRa Basics Station](#) que permite que os gateways se conectem a AWS IoT Core for LoRaWAN. Para se conectar a AWS IoT Core for LoRaWAN, o gateway LoRa primeiro consulta o servidor CUPS para o endpoint LNS e, em seguida, estabelece uma conexão de dados WebSockets com esse endpoint. Depois que a conexão é estabelecida, os quadros de uplink e downlink podem ser trocados por meio dessa conexão.

### Filtragem de quadros de dados LoRa recebidos pelo gateway

Depois que o gateway LoRaWAN estabelece uma conexão com o endpoint, AWS IoT Core for LoRaWAN responde com uma mensagem `router_config` que especifica um conjunto de parâmetros para a configuração do gateway LoRa, incluindo os parâmetros de filtragem `NetID` e `JoinEui`. Para obter mais informações sobre `router_config` e como uma conexão é estabelecida com o Servidor da Rede LoRaWAN (LNS), consulte [Protocolo LNS](#).

```
{  
  "msgtype"      : "router_config"  
  "NetID"       : [ INT, .. ]  
  "JoinEui"     : [ [INT,INT], .. ] // ranges: beg,end inclusive  
  "region"      : STRING           // e.g. "EU863", "US902", ..
```

```
"hwspec"      : STRING
"freq_range"  : [ INT, INT ]      // min, max (hz)
"DRs"        : [ [INT,INT,INT], .. ] // sf,bw,dnonly
"sx1301_conf": [ SX1301CONF, .. ]
"nocca"      : BOOL
"nodc"       : BOOL
"nodwell"    : BOOL
}
```

Os gateways transportam dados do dispositivo LoRaWAN de e para o LNS geralmente em redes de alta largura de banda, como Wi-Fi, Ethernet ou celular. Os gateways geralmente captam todas as mensagens e passam pelo tráfego que chega a elas até AWS IoT Core for LoRaWAN. No entanto, você pode configurar os gateways para filtrar parte do tráfego de dados do dispositivo, o que ajuda a conservar o uso da largura de banda e reduz o fluxo de tráfego entre o gateway e o LNS.

Para configurar o gateway LoRa para filtrar os quadros de dados, você pode usar os parâmetros `NetID` e `JoinEui` na mensagem `router_config`. `NetID` é uma lista de valores de `NetID` que são aceitos. Qualquer quadro de dados LoRa com um quadro de dados diferente dos listados será descartado. `JoinEui` é uma lista de pares de valores inteiros que codificam intervalos de valores `JoinEUI`. Os quadros de solicitação de junção serão eliminados pelo gateway, a menos que o campo `JoinEui` na mensagem esteja dentro do intervalo [`BegEui`, `EndEui`].

### Canais e sub-bandas de frequência

Para regiões de RF US915 e AU915, os dispositivos sem fio têm opções de 64 canais de uplink de 125 KHz e 8 canais de uplink de 500 KHz para acessar as redes LoRaWAN usando os gateways LoRa. Os canais de frequência de uplink são divididos em 8 sub-bandas, cada uma com 8 canais de 125 KHz e um canal de 500 KHz. Para cada gateway regular na região AU915, uma ou mais sub-bandas serão compatíveis.

Alguns dispositivos sem fio não conseguem alternar entre as sub-bandas e usar os canais de frequência em apenas uma sub-banda quando conectados a AWS IoT Core for LoRaWAN. Para que os pacotes de uplink desses dispositivos sejam transmitidos, configure os gateways LoRa para usar essa sub-banda específica. Para gateways em outras regiões de RF, como EU868, essa configuração não é necessária.

Configure o gateway para usar filtragem e sub-bandas usando o console

Você pode configurar o gateway para usar uma sub-banda específica e também habilitar a capacidade de filtrar os quadros de dados LoRa. Para especificar esses parâmetros usando o console:

1. Navegue até a página [AWS IoT Core for LoRaWAN Gateways](#) do console AWS IoT e escolha Adicionar gateway.
2. Especifique os detalhes do gateway, como o Eui do gateway, a Banda de frequência (RFRegion) e um Nome e Descrição opcionais, e escolha se deseja associar a AWS IoT ao gateway. Para obter mais informações sobre como adicionar um gateway, consulte [Adicionar um gateway usando o console](#).
3. Na seção Configuração do LoRaWAN, você pode especificar as sub-bandas e as informações de filtragem.
  - **SubBands**: para adicionar uma sub-banda, escolha Adicionar sub-banda e especifique uma lista de valores inteiros que indiquem quais sub-bandas são compatíveis com o gateway. O parâmetro SubBands só pode ser configurado no RfRegion US915 e no AU915 e deve ter valores no intervalo [1, 8] dentro de uma dessas regiões compatíveis.
  - **NetIdFilters**: para filtrar quadros de uplink, escolha Adicionar NetId e especifique uma lista de valores de string que o gateway usa. O NetID do quadro de uplink de entrada do dispositivo sem fio deve corresponder a pelo menos um dos valores listados; caso contrário, o quadro será descartado.
  - **JoinEuiFilters**: escolha Adicionar intervalo JoinEui e especifique uma lista de pares de valores de string que um gateway usa para filtrar quadros LoRa. O valor de JoinEUI especificado como parte da solicitação de junção do dispositivo sem fio deve estar dentro do intervalo de pelo menos um dos valores de JoinEuiRange, cada um listado como um par de [BegEui, EndEui]; caso contrário, o quadro será descartado.
4. Em seguida, você pode continuar configurando o gateway seguindo as instruções descritas em [Adicionar um gateway usando o console](#).

Depois de adicionar um gateway, na página [AWS IoT Core for LoRaWAN Gateways](#) do console AWS IoT, se você selecionar o gateway que adicionou, poderá ver as SubBands e os filtros NetIdFilters e JoinEuiFilters na seção Detalhes específicos do LoRaWAN da página de detalhes do Gateway.

Configure o gateway para usar filtragem e sub-bandas usando a API

Você pode usar a API [CreateWirelessGateway](#) usada para criar um gateway para configurar as sub-bandas que deseja usar e ativar o recurso de filtragem. Usando a API CreateWirelessGateway, você pode especificar as sub-bandas e os filtros como parte das informações de configuração do gateway que você oferece usando o campo LoRaWAN. Confira a seguir o token de solicitação que inclui essas informações.

```
POST /wireless-gateways HTTP/1.1
Content-type: application/json

{
  "Arn": "arn:aws:iotwireless:us-east-1:400232685877aa:WirelessGateway/
    a11e3d21-e44c-471c-afca-6716c228336a",
  "Description": "Using my first LoRaWAN gateway",
  "LoRaWAN": {
    "GatewayEui": "a1b2c3d4567890ab",
    "JoinEuiFilters": [
      ["0000000000000001", "00000000000000ff"],
      ["000000000000ff00", "000000000000ffff"]
    ],
    "NetIdFilters": ["000000", "000001"],
    "RfRegion": "US915",
    "SubBands": [2]
  },
  "Name": "myFirstLoRaWANGateway"
  "ThingArn": null,
  "ThingName": null
}
```

Você também pode usar a API [UpdateWirelessGateway](#) para atualizar os filtros, mas não as sub-bandas. Se os valores `JoinEuiFilters` e `NetIdfilters` forem nulos, não há atualização para os campos. Se os valores não forem nulos e as listas vazias forem incluídas, a atualização será aplicada. Para obter os valores dos campos especificados, use a API [GetWirelessGateway](#).

## Atualize o firmware do gateway usando o serviço CUPS com AWS IoT Core for LoRaWAN

O software [LoRa Basics Station](#) executado no gateway oferece gerenciamento de credenciais e interface de atualização de firmware usando o protocolo Configuration and Update Server (CUPS). O protocolo CUPS oferece entrega segura de atualizações de firmware com assinaturas ECDSA.

Você precisará atualizar com frequência o firmware do gateway. É possível usar o serviço CUPS com AWS IoT Core for LoRaWAN para fornecer atualizações de firmware para o gateway em que as atualizações também podem ser assinadas. Para atualizar o firmware do gateway, você pode usar o SDK ou a CLI, mas não o console.

O processo de atualização leva cerca de 45 minutos para ser concluído. Pode levar mais tempo se você estiver configurando o gateway pela primeira vez para se conectar a AWS IoT Core for

LoRaWAN. Os fabricantes de gateway geralmente oferecem os próprios arquivos e assinaturas de atualização de firmware para que você possa usá-los e passar para [Fazer upload do arquivo de firmware para um bucket do S3 e adicionar um perfil do IAM](#).

Se você não tiver os arquivos de atualização de firmware, consulte [Gere o arquivo e a assinatura de atualização de firmware](#) para ver um exemplo que você pode usar para adaptar ao seu aplicativo.

Para realizar a atualização do firmware do gateway:

- [Gere o arquivo e a assinatura de atualização de firmware](#)
- [Fazer upload do arquivo de firmware para um bucket do S3 e adicionar um perfil do IAM](#)
- [Agende e execute a atualização do firmware usando uma definição de tarefa](#)

## Gere o arquivo e a assinatura de atualização de firmware

As etapas desse procedimento são opcionais e dependem do gateway que você está usando. Os fabricantes de gateway oferecem a própria atualização de firmware na forma de um arquivo de atualização ou script, e o Basics Station executa esse script em segundo plano. Nesse caso, você provavelmente encontrará o arquivo de atualização do firmware nas notas de lançamento do gateway que está usando. Em vez disso, você pode usar esse arquivo ou script de atualização e passar para [Fazer upload do arquivo de firmware para um bucket do S3 e adicionar um perfil do IAM](#).

Se você não tiver esse script, a seguir são mostrados os comandos a serem executados para gerar o arquivo de atualização do firmware. As atualizações também podem ser assinadas para garantir que o código não tenha sido alterado ou corrompido e que os dispositivos executem códigos publicados somente por autores confiáveis.

Neste procedimento, você vai:

- [Gerar o arquivo de atualização de firmware](#)
- [Gerar a assinatura de atualização de firmware](#)
- [Reveja as próximas etapas](#)

## Gerar o arquivo de atualização de firmware

O software LoRa Basics Station executado no gateway é capaz de receber atualizações de firmware na resposta do CUPS. Se você não tiver um script fornecido pelo fabricante, consulte o seguinte script de atualização de firmware escrito para o RAKWireless Gateway baseado em Raspberry Pi.

Temos um script básico e o novo binário da estação, arquivo de versão, e `station.conf` estão anexados a ele.

### Note

O script é específico para o RAKWireless Gateway. Por isso, será necessário adaptá-lo ao seu aplicativo, dependendo do gateway que você estiver usando.

## Script básico

A seguir é mostrado um exemplo de script básico para o RAKWireless Gateway baseado em Raspberry Pi. Você pode salvar os seguintes comandos em um arquivo `base.sh` e, em seguida, executar o script no terminal do navegador da Web do Raspberry Pi.

```
#!/bin/bash*
execution_folder=/home/pi/Documents/basicstation/examples/aws_lorawan
station_path="$execution_folder/station"
version_path="$execution_folder/version.txt"
station_conf_path="$execution_folder/station_conf"

# Function to find the Basics Station binary at the end of this script
# and store it in the station path
function prepare_station()
{
    match=$(grep --text --line-number '^STATION:$' $0 | cut -d ':' -f 1)
    payload_start=$((match + 1))
    match_end=$(grep --text --line-number '^END_STATION:$' $0 | cut -d ':' -f 1)
    payload_end=$((match_end - 1))
    lines=$((payload_end - payload_start + 1))
    head -n $payload_end $0 | tail -n $lines > $station_path
}

# Function to find the version.txt at the end of this script
# and store it in the location for version.txt
function prepare_version()
{
    match=$(grep --text --line-number '^VERSION:$' $0 | cut -d ':' -f 1)
    payload_start=$((match + 1))
    match_end=$(grep --text --line-number '^END_VERSION:$' $0 | cut -d ':' -f 1)
    payload_end=$((match_end - 1))
    lines=$((payload_end - payload_start + 1))
}
```

```
    head -n $payload_end $0 | tail -n $lines > $version_path
}

# Function to find the version.txt at the end of this script
# and store it in the location for version.txt
function prepare_station_conf()
{
    match=$(grep --text --line-number '^CONF:$' $0 | cut -d ':' -f 1)
    payload_start=$((match + 1))
    match_end=$(grep --text --line-number '^END_CONF:$' $0 | cut -d ':' -f 1)
    payload_end=$((match_end - 1))
    lines=$((payload_end - payload_start + 1))
    head -n $payload_end $0 | tail -n $lines > $station_conf_path
}

# Stop the currently running Basics station so that it can be overwritten
# by the new one
killall station

# Store the different files
prepare_station
prepare_versionp
prepare_station_conf

# Provide execute permission for Basics station binary
chmod +x $station_path

# Remove update.bin so that it is not read again next time Basics station starts
rm -f /tmp/update.bin

# Exit so that rest of this script which has binaries attached does not get executed
exit 0
```

## Adicionar script de carga

Ao script básico, anexamos o binário Basics Station, o version.txt que identifica a versão para a qual atualizar e station.conf em um script chamado addpayload.sh. Em seguida, execute este script.

```
*#!/bin/bash
*
base.sh > fwstation
```

```
# Add station
echo "STATION:" >> fwstation
cat $1 >> fwstation
echo "" >> fwstation
echo "END_STATION:" >> fwstation

# Add version.txt
echo "VERSION:" >> fwstation
cat $2 >> fwstation
echo "" >> fwstation
echo "END_VERSION:" >> fwstation

# Add station.conf
echo "CONF:" >> fwstation
cat $3 >> fwstation
echo "END_CONF:" >> fwstation

# executable
chmod +x fwstation
```

Depois de executar esses scripts, você pode executar o seguinte comando no terminal para gerar o arquivo de atualização do firmware, `fwstation`.

```
$ ./addpayload.sh station version.txt station.conf
```

### Gerar a assinatura de atualização de firmware

O software LoRa Basics Station oferece atualizações de firmware assinadas com assinaturas ECDSA. Para oferecer suporte a atualizações assinadas, você precisará:

- Uma assinatura que deve ser gerada por uma chave privada ECDSA e com menos de 128 bytes.
- A chave privada que é usada para a assinatura e deve ser armazenada no gateway com o nome do arquivo do formato `sig-%d.key`. Recomendamos usar o nome do arquivo `sig-0.key`.
- Um CRC de 32 bits sobre a chave privada.

A assinatura e o CRC serão passados para as APIs AWS IoT Core for LoRaWAN. Para gerar os arquivos anteriores, você pode usar o script `gen.sh` a seguir, inspirado no exemplo [basicstation](#) no repositório do GitHub.

```
*#!/bin/bash
```

```
*function ecdsaKey() {
    # Key not password protected for simplicity
    openssl ecparam -name prime256v1 -genkey | openssl ec -out $1
}

# Generate ECDSA key
ecdsaKey sig-0.prime256v1.pem

# Generate public key
openssl ec -in sig-0.prime256v1.pem -pubout -out sig-0.prime256v1.pub

# Generate signature private key
openssl ec -in sig-0.prime256v1.pub -inform PEM -outform DER -pubin | tail -c 64 >
sig-0.key

# Generate signature
openssl dgst -sha512 -sign sig-0.prime256v1.pem $1 > sig-0.signature

# Convert signature to base64
openssl enc -base64 -in sig-0.signature -out sig-0.signature.base64

# Print the crc
crc_res=$(crc32 sig-0.key)printf "The crc for the private key=%d\n" $((16#$crc_res))

# Remove the generated files which won't be needed later
rm -rf sig-0.prime256v1.pem sig-0.signature sig-0.prime256v1.pub
```

A chave privada gerada pelo script deve ser salva no gateway. O arquivo da chave está em formato binário.

```
./gen_sig.sh fwstation
read EC key
writing EC key
read EC key
writing EC key
read EC key
writing EC key
The crc for the private key=3434210794

$ cat sig-0.signature.base64
```

```
MEQCIDPY/p2s5gXIPNC0gZr+NzeTLpX+WfBo5tYwbh5pQWN3AiBR0en+X1IdMScv  
AsfVfU/ZScJCaIkVNZh4esyS8mNIgA==
```

```
$ ls sig-0.key  
sig-0.key
```

```
$ scp sig-0.key pi@192.168.1.11:/home/pi/Documents/basicstation/examples/iotwireless
```

Reveja as próximas etapas

Agora que você gerou o firmware e a assinatura, vá para o próximo tópico para fazer o upload do arquivo de firmware, `fwstation`, em um bucket do Amazon S3. O bucket é um contêiner que armazenará o arquivo de atualização do firmware como um objeto. Você pode adicionar um perfil do IAM que dará ao servidor CUPS permissão para ler o arquivo de atualização do firmware no bucket do S3.

## Fazer upload do arquivo de firmware para um bucket do S3 e adicionar um perfil do IAM

Você pode usar o Amazon S3 para criar um bucket, que é um contêiner que pode armazenar o arquivo de atualização de firmware. Você pode fazer o upload do arquivo para o bucket do S3 e adicionar um perfil do IAM que permita que o servidor CUPS leia seu arquivo de atualização do bucket. Para obter mais informações sobre o Amazon S3, consulte [Conceitos básicos do Amazon S3](#).

O arquivo de atualização do firmware que você deseja carregar depende do gateway que você está usando. Se seguiu um procedimento semelhante ao descrito em [Gere o arquivo e a assinatura de atualização de firmware](#), você fará o upload do arquivo `fwstation` gerado pela execução dos scripts.

Esse procedimento leva cerca de 20 minutos para ser concluído.

Para fazer o upload do arquivo de firmware:

- [Crie um bucket do Amazon S3 e faça o upload do arquivo de atualização](#)
- [Criar um perfil do IAM com permissões para ler o bucket do S3](#)
- [Reveja as próximas etapas](#)

## Crie um bucket do Amazon S3 e faça o upload do arquivo de atualização

Você criará um bucket do Amazon S3 usando o Console de gerenciamento da AWS e, em seguida, fará upload do arquivo de atualização de firmware no bucket.

### Crie um bucket do S3

Para criar um bucket do S3, abra o [Console do Amazon S3](#). Conecte-se se ainda não tiver feito isso e, em seguida, execute as seguintes etapas:

1. Escolha Criar bucket.
2. Insira um nome exclusivo e significativo para o Nome do bucket (por exemplo, `iotwirelessfwupdate`). Para obter a convenção de nomenclatura recomendada para seu bucket, consulte <https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucketnamingrules.html>.
3. Selecione o Região da AWS escolhido como aquele que você usou para criar seu gateway e dispositivo LoRaWAN, e a configuração Bloquear todo o acesso público está selecionada para que o bucket use as permissões padrão.
4. Escolha Ativar para Versionamento do bucket, que ajudará você a manter várias versões do arquivo de atualização do firmware no mesmo bucket.
5. Confirme se Criptografia do lado do servidor está definido como Desativar e escolha Criar bucket.

### Faça o upload do arquivo de atualização de firmware

Agora, você pode ver seu bucket na lista de buckets exibida no Console de gerenciamento da AWS. Escolha o bucket e conclua as etapas a seguir para fazer o upload do arquivo.

1. Escolha o bucket e, em seguida, escolha Fazer upload.
2. Escolha Adicionar arquivo e, em seguida, faça upload do arquivo de atualização do firmware. Se seguiu o procedimento descrito em [Gere o arquivo e a assinatura de atualização de firmware](#), você fará o upload do arquivo `fwstation`; caso contrário, fará o upload do arquivo fornecido pelo fabricante do gateway.
3. Certifique-se de que todas as configurações estejam definidas como padrão. Verifique se as ACLs predefinidas estão definidas como privadas e escolha Fazer upload para fazer o upload do arquivo.

4. Copie o URI do S3 do arquivo que você carregou. Escolha seu bucket e você verá o arquivo que carregou exibido na lista de Objetos. Escolha o arquivo e, em seguida, escolha Copiar URI do S3. O URI será algo como: `s3://iotwirelessfwupdate/fwstation` se você nomeou seu bucket de forma semelhante ao exemplo descrito anteriormente (`fwstation`). Você utilizará o URI do S3 ao criar o perfil do IAM.

Criar um perfil do IAM com permissões para ler o bucket do S3

Agora, você criará um perfil e uma política do IAM que darão ao CUPS a permissão para ler o arquivo de atualização de firmware no bucket do S3.

Criar uma política do IAM para o seu perfil

Para criar uma política do IAM para seu perfil de destino AWS IoT Core for LoRaWAN, abra o [Hub de políticas do console do IAM](#) e conclua as seguintes etapas:

1. Escolha Criar política e escolha a guia JSON.
2. Exclua qualquer conteúdo do editor e cole este documento de política. A política oferece permissões para acessar o bucket `iotwireless` e o arquivo de atualização do firmware, `fwstation`, armazenados dentro de um objeto.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucketVersions",
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::iotwirelessfwupdate/fwstation",
        "arn:aws:s3:::iotwirelessfwupdate"
      ]
    }
  ]
}
```

3. Escolha Revisar política e, em Nome, insira um nome para essa política (por exemplo, `IoTWirelessFwUpdatePolicy`). Você precisará desse nome para usar no próximo procedimento.
4. Escolha Criar política.

Criar um perfil do IAM com a política anexada

Agora, você criará um perfil do IAM e anexará a política criada anteriormente para acessar o bucket do S3. Abra o [Hub Perfis do console do IAM](#) e conclua as seguintes etapas:

1. Selecione Criar perfil.
2. Em Selecionar tipo de entidade confiável, escolha Outra Conta da AWS.
3. Em ID da conta, insira a ID da Conta da AWS e escolha Próximo: permissões.
4. Na caixa de pesquisa, insira o nome da política do IAM que você criou no procedimento anterior. Verifique a política do IAM (por exemplo, `IoTWirelessFwUpdatePolicy`) que você criou anteriormente nos resultados da pesquisa e escolha-a.
5. Escolha Próximo: tags e Próximo: revisar.
6. Em Nome do perfil, insira um nome dessa função (por exemplo, `IoTWirelessFwUpdateRole`) e escolha Criar perfil.

Edite a relação de confiança do perfil do IAM

Na mensagem de confirmação exibida após a execução da etapa anterior, selecione o nome do perfil criado para editá-lo. Você editará o perfil para adicionar a relação de confiança a seguir.

1. Na seção Resumo do perfil que você criou, escolha a guia Relações de confiança e, em seguida, Editar relação de confiança.
2. Em Documento de política, altere a propriedade `Principal` para ficar parecida com o exemplo a seguir.

```
"Principal": {  
  "Service": "iotwireless.amazonaws.com"  
},
```

Depois de alterar a propriedade `Principal`, o documento de política completo deve ser semelhante a este exemplo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "iotwireless.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {}
    }
  ]
}
```

3. Para salvar as alterações e sair, selecione Atualizar política de confiança.
4. Obtenha o ARN para seu perfil. Escolha o perfil do IAM e, na seção Resumo, você verá um ARN do perfil, como `arn:aws:iam::123456789012:role/IoTWirelessFwUpdateRole`. Copie este ARN do perfil.

Reveja as próximas etapas

Agora que você criou o bucket do S3 e um perfil do IAM que permite que o servidor CUPS leia o bucket do S3, vá para o próximo tópico para agendar e executar a atualização do firmware. Mantenha o URI do S3 e o ARN do perfil que você copiou anteriormente para poder inseri-los para criar uma definição de tarefa que será executada para realizar a atualização do firmware.

## Agende e execute a atualização do firmware usando uma definição de tarefa

Você pode usar uma definição de tarefa para incluir detalhes sobre a atualização do firmware e definir a atualização. AWS IoT Core for LoRaWAN oferece uma atualização de firmware com base nas informações dos três campos a seguir associados ao gateway.

- Estação

A versão e o tempo de compilação do software Basics Station. Para identificar essas informações, você também pode gerá-las usando o software Basics Station que está sendo executado pelo gateway (por exemplo, `2.0.5(rpi/std) 2021-03-09 03:45:09`).

- PackageVersion

A versão do firmware, especificada pelo arquivo `version.txt` no gateway. Embora essas informações possam não estar presentes no gateway, recomendamos que elas sejam uma forma de definir a versão do firmware (por exemplo, `1.0.0`).

- Modelo

A plataforma ou o modelo que está sendo usado pelo gateway (por exemplo, Linux).

Esse procedimento leva 20 minutos para ser concluído.

Para concluir este procedimento:

- [Obtenha a versão atual em execução no gateway](#)
- [Criar uma definição de tarefa de gateway sem fio](#)
- [Execute a tarefa de atualização do firmware e acompanhe o progresso](#)

Obtenha a versão atual em execução no gateway

Para determinar a elegibilidade do gateway para uma atualização de firmware, o servidor CUPS verifica todos os três campos, `Station`, `PackageVersion` e `Model`, em busca de uma correspondência quando o gateway os apresenta durante uma solicitação do CUPS. Quando você usa uma definição de tarefa, esses campos são armazenados como parte do campo `CurrentVersion`.

Você pode usar a API AWS IoT Core for LoRaWAN ou a AWS CLI para obter `CurrentVersion` para o gateway. Os comandos a seguir mostram como obter essas informações usando a CLI.

1. Se você já tiver provisionado um gateway, poderá obter informações sobre ele usando o comando [get-wireless-gateway](#).

```
aws iotwireless get-wireless-gateway \
  --identifier 5a11b0a85a11b0a8 \
  --identifier-type GatewayEui
```

Confira a seguir um exemplo de saída para o comando.

```
{
  "Name": "Raspberry pi",
  "Id": "1352172b-0602-4b40-896f-54da9ed16b57",
```

```
"Description": "Raspberry pi",
"LoRaWAN": {
  "GatewayEui": "5a11b0a85a11b0a8",
  "RfRegion": "US915"
},
"Arn": "arn:aws:iotwireless:us-
east-1:231894231068:WirelessGateway/1352172b-0602-4b40-896f-54da9ed16b57"
}
```

2. Usando o ID do gateway sem fio informado pelo comando `get-wireless-gateway`, você pode usar o comando [get-wireless-gateway-firmware-information](#) para obter `CurrentVersion`.

```
aws iotwireless get-wireless-gateway-firmware-information \
  --id "3039b406-5cc9-4307-925b-9948c63da25b"
```

A seguir, confira um exemplo de saída para o comando, com informações de todos os três campos exibidos pela `CurrentVersion`.

```
{
  "LoRaWAN": {
    "CurrentVersion": {
      "PackageVersion": "1.0.0",
      "Model": "rpi",
      "Station": "2.0.5(rpi/std) 2021-03-09 03:45:09"
    }
  }
}
```

## Criar uma definição de tarefa de gateway sem fio

Ao criar a definição da tarefa, é recomendável especificar a criação automática de tarefas utilizando o parâmetro `AutoCreateTasks`. O `AutoCreateTasks` aplica-se a qualquer gateway que corresponda aos três parâmetros mencionados anteriormente. Se esse parâmetro estiver desativado, os parâmetros deverão ser atribuídos manualmente ao gateway.

Você pode criar a definição da tarefa do gateway sem fio usando a API AWS IoT Core for LoRaWAN ou a AWS CLI. Os comandos a seguir mostram como criar a definição da tarefa usando a CLI.

1. Crie um arquivo, `input.json`, que conterá as informações a serem passadas para a API `CreateWirelessGatewayTaskDefinition`. No arquivo `input.json`, dê as seguintes informações que você obteve anteriormente:

- `UpdateDataSource`

Forneça o link para seu objeto contendo o arquivo de atualização do firmware que você carregou no bucket do S3 (por exemplo, `s3://iotwirelessfwupdate/fwstation`).

- `UpdateDataRole`

Forneça o link para o ARN do perfil do IAM criado, que dá permissões para ler o bucket do S3 (por exemplo, `arn:aws:iam::123456789012:role/IoTWirelessFwUpdateRole`).

- `SigKeyCRC` e `UpdateSignature`

Essas informações podem ser fornecidas pelo fabricante do gateway, mas se seguiu o procedimento descrito em [Gere o arquivo e a assinatura de atualização de firmware](#), você as encontrará ao gerar a assinatura.

- `CurrentVersion`

Apresente a saída `CurrentVersion` que você obteve anteriormente executando o comando `get-wireless-gateway-firmware-information`.

```
cat input.json
```

O exemplo a seguir mostra o conteúdo do arquivo `input.json`.

```
{
  "AutoCreateTasks": true,
  "Name": "FirmwareUpdate",
  "Update": {
    "UpdateDataSource" : "s3://iotwirelessfwupdate/fwstation",
    "UpdateDataRole" : "arn:aws:iam::123456789012:role/IoTWirelessFwUpdateRole",
    "LoRaWAN" : {
      "SigKeyCrc": 3434210794,
      "UpdateSignature": "MEQCIDPY/p2ssgXIPNC0gZr+NzeTLpX+WfBo5tYWbh5pQWN3AiBR0en+XlIdMScvAsfvFU/ZScJCa1kVNZh4esyS8mNIgA==",
      "CurrentVersion" :

```

```
{
  "PackageVersion": "1.0.0",
  "Model": "rpi",
  "Station": "2.0.5(rpi/std) 2021-03-09 03:45:09"
}
```

2. Passe o arquivo `input.json` para o comando [create-wireless-gateway-task-definition](#) para criar a definição da tarefa.

```
aws iotwireless create-wireless-gateway-task-definition \
  --cli-input-json file://input.json
```

Confira a seguir a saída do comando.

```
{
  "Id": "4ac46ff4-efc5-44fd-9def-e8517077bb12",
  "Arn": "arn:aws:iotwireless:us-east-1:231894231068:WirelessGatewayTaskDefinition/4ac46ff4-efc5-44fd-9def-e8517077bb12"
}
```

Execute a tarefa de atualização do firmware e acompanhe o progresso

O gateway está pronto para receber a atualização do firmware e, uma vez ligado, ele se conecta ao servidor CUPS. Quando o servidor CUPS encontra uma correspondência na versão do gateway, ele agenda uma atualização de firmware.

Uma tarefa é uma definição de tarefa em andamento. Como você especificou a criação automática de tarefas definindo `AutoCreateTasks` como `True`, a tarefa de atualização do firmware começará assim que um gateway correspondente for encontrado.

É possível acompanhar o andamento da tarefa usando a API `GetWirelessGatewayTask`. Quando você executa o comando [get-wireless-gateway-task](#) pela primeira vez, ele mostra o status da tarefa como `IN_PROGRESS`.

```
aws iotwireless get-wireless-gateway-task \
  --id 1352172b-0602-4b40-896f-54da9ed16b57
```

Confira a seguir a saída do comando.

```
{
  "WirelessGatewayId": "1352172b-0602-4b40-896f-54da9ed16b57",
  "WirelessGatewayTaskDefinitionId": "ec11f9e7-b037-4fcc-aa60-a43b839f5de3",
  "LastUplinkReceivedAt": "2021-03-12T09:56:12.047Z",
  "TaskCreatedAt": "2021-03-12T09:56:12.047Z",
  "Status": "IN_PROGRESS"
}
```

Quando você executar o comando da próxima vez, se a atualização do firmware entrar em vigor, ela mostrará os campos atualizados, `Package`, `Version` e `Model` e o status da tarefa será alterado para `COMPLETED`.

```
aws iotwireless get-wireless-gateway-task \
  --id 1352172b-0602-4b40-896f-54da9ed16b57
```

Confira a seguir a saída do comando.

```
{
  "WirelessGatewayId": "1352172b-0602-4b40-896f-54da9ed16b57",
  "WirelessGatewayTaskDefinitionId": "ec11f9e7-b037-4fcc-aa60-a43b839f5de3",
  "LastUplinkReceivedAt": "2021-03-12T09:56:12.047Z",
  "TaskCreatedAt": "2021-03-12T09:56:12.047Z",
  "Status": "COMPLETED"
}
```

Neste exemplo, mostramos a atualização do firmware usando o RAKWireless Gateway baseado em Raspberry Pi. O script de atualização do firmware interrompe a execução do BasicStation para armazenar os campos `Package`, `Version` e `Model` atualizados, portanto, BasicStation precisará ser reiniciado.

```
2021-03-12 09:56:13.108 [CUP:INFO] CUPS provided update.bin
2021-03-12 09:56:13.108 [CUP:INFO] CUPS provided signature len=70 keycrc=37316C36
2021-03-12 09:56:13.148 [CUP:INFO] ECDSA key#0 -> VERIFIED
2021-03-12 09:56:13.148 [CUP:INFO] Running update.bin as background process
2021-03-12 09:56:13.149 [SYS:VERB] /tmp/update.bin: Forked, waiting...
2021-03-12 09:56:13.151 [SYS:INFO] Process /tmp/update.bin (pid=6873) completed
2021-03-12 09:56:13.152 [CUP:INFO] Interaction with CUPS done - next regular check in
10s
```

Se a atualização do firmware falhar, você verá um status de `FIRST_RETRY` do servidor CUPS e o gateway enviará a mesma solicitação. Se o servidor CUPS não conseguir se conectar ao gateway após um `SECOND_RETRY`, ele mostrará um status de `FAILED`.

Depois que a tarefa anterior for `COMPLETED` ou `FAILED`, exclua a tarefa antiga usando o comando [delete-wireless-gateway-task](#) antes de iniciar uma nova.

```
aws iotwireless delete-wireless-gateway-task \  
  --id 1352172b-0602-4b40-896f-54da9ed16b57
```

## Escolher gateways para receber o tráfego de dados de downlink LoRaWAN

Ao enviar uma mensagem de downlink de AWS IoT Core for LoRaWAN para o seu dispositivo, você pode escolher os gateways que deseja usar para o tráfego de dados de downlink. Você pode especificar um gateway individual ou escolher em uma lista de gateways para receber o tráfego de downlink.

### Como especificar a lista de gateways

Você pode especificar um gateway individual ou a lista de gateways a serem usados ao enviar uma mensagem de downlink de AWS IoT Core for LoRaWAN para o seu dispositivo usando a operação da API [SendDataToWirelessDevice](#). Ao invocar a operação da API, especifique os seguintes parâmetros usando o objeto `ParticipatingGateways` para os gateways.

#### Note

A lista de gateways que você deseja usar não está disponível no console da AWS IoT. Você pode especificar essa lista de gateways para usar somente ao usar a operação da API `SendDataToWirelessDevice` ou a CLI.

- `DownlinkMode`: indica se a mensagem de downlink deve ser enviada no modo sequencial ou no modo simultâneo. Para dispositivos de classe A, especifique `UsingUplinkGateway` para usar somente os gateways escolhidos da transmissão anterior da mensagem de uplink.
- `GatewayList`: a lista de gateways que você deseja usar para enviar o tráfego de dados de downlink. A carga útil do downlink será enviada para os gateways especificados com a frequência especificada. Isso é indicado usando uma lista de objetos `GatewayListItem`, que consiste nos pares `GatewayId` e `DownlinkFrequency`.

- `TransmissionInterval`: o tempo de espera de AWS IoT Core for LoRaWAN antes de transmitir a carga útil para o próximo gateway.

#### Note

Você pode especificar essa lista de gateways para usar somente ao enviar a mensagem de downlink para um dispositivo sem fio de classe B ou classe C. Se você usar um dispositivo de classe A, o gateway que você escolheu ao enviar a mensagem de uplink será usado quando uma mensagem de downlink for enviada para o dispositivo.

O exemplo a seguir mostra como especificar esses parâmetros para o gateway. O arquivo `input.json` conterá detalhes adicionais. Para obter mais informações sobre o envio de uma mensagem de downlink usando a operação da API `SendDataToWirelessDevice`, consulte [Executar operações de fila de downlink com a API](#).

#### Note

Os parâmetros para especificar a lista de gateways participantes não estão disponíveis quando você envia uma mensagem de downlink de AWS IoT Core for LoRaWAN usando o console AWS IoT.

```
aws iotwireless send-data-to-wireless-device \
  --id "11aa5eae-2f56-4b8e-a023-b28d98494e49" \
  --transmit-mode "1" \
  --payload-data "SGVsbG8gVG8gRGV2c2lt" \
  --cli-input-json file://input.json
```

O exemplo a seguir mostra o conteúdo do arquivo `input.json`.

Conteúdo de `input.json`

```
{
  "WirelessMetadata": {
    "LoRaWAN": {
      "FPort": "1",
      "ParticipatingGateways": {
```

```
"DownlinkMode": "SEQUENTIAL",
"TransmissionInterval": 1200,
"GatewayList": [
  {
    "DownlinkFrequency": 100000000,
    "GatewayID": a01b2c34-d44e-567f-abcd-0123e445663a
  },
  {
    "DownlinkFrequency": 100000101,
    "GatewayID": 12345678-a1b2-3c45-67d8-e90fa1b2c34d
  }
]
}
}
```

A saída da execução desse comando gera um MessageId para a mensagem de downlink. Em alguns casos, mesmo que você receba o MessageId, os pacotes podem ser descartados. Para obter mais informações sobre como resolver o erro, consulte [Solucionar erros na fila de mensagens de downlink](#).

```
{
  MessageId: "6011dd36-0043d6eb-0072-0008"
}
```

## Obtenha informações sobre a lista de gateways participantes

Você pode obter informações sobre a lista de gateways que estão participando do recebimento da mensagem de downlink listando as mensagens na fila de downlink. Para listar mensagens, use a API [ListQueuedMessages](#).

```
aws iotwireless list-queued-messages \
  --wireless-device-type "LoRaWAN"
```

A execução desse comando retorna informações sobre as mensagens na fila e seus parâmetros.

# Gerenciamento de dispositivos com o AWS IoT Core for LoRaWAN

A seguir estão algumas considerações importantes ao usar dispositivos com o AWS IoT Core for LoRaWAN. Para obter informações sobre como adicionar o dispositivo ao AWS IoT Core for LoRaWAN, consulte [Integrar os dispositivos ao AWS IoT Core for LoRaWAN](#).

## Considerações sobre dispositivos

Quando for selecionar um dispositivo que deseja usar para se comunicar com o AWS IoT Core for LoRaWAN, considere o seguinte.

- Sensores disponíveis
- Capacidade de bateria
- Consumo de energia
- Custo
- Tipo de antena e alcance da transmissão

## Uso de dispositivos com gateways qualificados para o AWS IoT Core for LoRaWAN

Os dispositivos usados podem ser emparelhados com gateways sem fio qualificados para uso com o AWS IoT Core for LoRaWAN. É possível encontrar esses gateways e kits de desenvolvedor no [Catálogo de dispositivos do parceiro da AWS](#). Também recomendamos considerar a proximidade desses dispositivos aos gateways. Para ter mais informações, consulte [Usar gateways qualificados do AWS Partner Device Catalog](#).

## Versão LoRaWAN

O AWS IoT Core for LoRaWAN é compatível com todos os dispositivos que estão em conformidade com as especificações LoRaWAN 1.0.x ou 1.1 padronizadas pela LoRa Alliance.

## Modos de ativação

Antes que o dispositivo LoRaWAN possa enviar dados de uplink, é preciso concluir um processo chamado procedimento de ativação ou adesão. Para ativar o dispositivo, você pode usar a OTAA (ativação sem fio) ou a ABP (ativação por personalização). Recomendamos usar a OTAA para ativar

o dispositivo porque novas chaves de sessão são geradas para cada ativação, o que o torna mais seguro.

A especificação do dispositivo sem fio se baseia na versão e modo de ativação do LoRaWAN, que determina as chaves raiz e as chaves de sessão geradas para cada ativação. Para ter mais informações, consulte [Adicione a especificação do dispositivo sem fio ao AWS IoT Core for LoRaWAN usando o console](#).

## Classes de dispositivos

Dispositivos LoRaWAN podem enviar mensagens de uplink a qualquer momento. Escutar mensagens de downlink consome a capacidade de bateria e reduz a duração dela. O protocolo LoRaWAN especifica três classes de dispositivos LoRaWAN.

- Os dispositivos de classe A dormem a maior parte do tempo e escutam mensagens de downlink apenas por um curto período de tempo. Esses dispositivos são, na maioria, sensores alimentados por bateria com uma vida útil de bateria de até 10 anos.
- Os dispositivos de classe B podem receber mensagens em slots de downlink programados. Esses dispositivos são, na maioria, atuadores alimentados por bateria.
- Os dispositivos de classe C nunca dormem e escutam as mensagens recebidas continuamente, portanto, não há muito atraso no recebimento das mensagens. Esses dispositivos são, na maioria, atuadores alimentados pela rede elétrica.

Para acessar mais informações dessas considerações sobre dispositivos sem fio, consulte os recursos mencionados em [Saiba mais sobre o LoRaWAN](#).

### Tópicos

- [Executar a taxa de dados adaptativa \(ADR\) com o AWS IoT Core for LoRaWAN](#)
- [Gerenciar a comunicação entre os dispositivos LoRaWAN e o AWS IoT](#)
- [Gerenciar o tráfego LoRaWAN de redes de dispositivos públicas LoRaWAN \(Everynet\)](#)

## Executar a taxa de dados adaptativa (ADR) com o AWS IoT Core for LoRaWAN

Para otimizar o consumo de energia de transmissão do dispositivo e, ao mesmo tempo, garantir que as mensagens dos dispositivos finais sejam recebidas nos gateways, o AWS IoT Core for

LoRaWAN utiliza a taxa de dados adaptativa. A taxa de dados adaptativa instrui os dispositivos finais a otimizarem a taxa de dados, a potência de transmissão e o número de retransmissões enquanto tentam reduzir a taxa de erros dos pacotes recebidos nos gateways. Por exemplo, se o dispositivo final estiver localizado próximo aos gateways, a taxa de dados adaptativa reduzirá a potência de transmissão e aumentará a taxa de dados.

## Tópicos

- [Como funciona a taxa de dados adaptativa \(ADR\)](#)
- [Configurar limites de taxa de dados \(CLI\)](#)

## Como funciona a taxa de dados adaptativa (ADR)

Para habilitar a ADR, o dispositivo deve definir o bit ADR no cabeçalho do quadro. Depois que o bit ADR é definido, o AWS IoT Core for LoRaWAN envia o comando `LinkADRReq` do MAC e os dispositivos respondem com o comando `LinkADRAns`, que inclui o status de ACK do comando ADR. Depois que os dispositivos aceitarem (ACK) o comando ADR, ele seguirá as instruções da ADR do AWS IoT Core for LoRaWAN e ajustará os valores dos parâmetros de transmissão para obter a taxa de dados ideal.

O algoritmo ADR do AWS IoT Core for LoRaWAN utiliza as informações de SINR no histórico de metadados de uplink para determinar a potência de transmissão e a taxa de dados ideais a serem utilizadas pelos dispositivos. O algoritmo utiliza as vinte mensagens de uplink mais recentes que se iniciam quando o bit ADR é definido no cabeçalho do quadro. Para determinar o número de retransmissões, ele usa a taxa de erro de pacote (PER), que é uma porcentagem do número total de pacotes perdidos. Ao utilizar esse algoritmo, você só pode controlar o intervalo de taxas de dados, ou seja, os limites mínimo e máximo das taxas de dados.

## Configurar limites de taxa de dados (CLI)

Por padrão, o AWS IoT Core for LoRaWAN executará a ADR quando você definir o bit ADR no cabeçalho do quadro do dispositivo LoRaWAN. É possível controlar os limites mínimo e máximo da taxa de dados ao criar um perfil de serviço para os dispositivos LoRaWAN utilizando a operação de API [CreateServiceProfile](#) do AWS IoT Wireless ou o comando [create-service-profile](#) da AWS CLI.

**Note**

Não é possível especificar os limites mínimo e máximo da taxa de dados ao criar um perfil de serviço no Console de gerenciamento da AWS. Só é possível especificá-los utilizando a API do AWS IoT Wireless ou a AWS CLI.

Para especificar os limites mínimo e máximo da taxa de dados, utilize os parâmetros `CreateServiceProfile` e `DrMax` com a operação de API `DrMin`. Os limites mínimo e máximo padrão da taxa de dados são 0 e 15. Por exemplo, o comando da CLI a seguir define um limite mínimo de 3 para a taxa de dados e um limite máximo de 12.

```
aws iotwireless create-service-profile \  
  --lorawan DrMin=3,DrMax=12
```

A execução desse comando gera um ID e um nome do recurso da Amazon (ARN) para o perfil de serviço.

```
{  
  "Arn": "arn:aws:iotwireless:us-east-1:123456789012:ServiceProfile/12345678-  
a1b2-3c45-67d8-e90fa1b2c34d",  
  "Id": "12345678-a1b2-3c45-67d8-e90fa1b2c34d"  
}
```

É possível obter os valores dos parâmetros especificados utilizando a operação de API [GetServiceProfile](#) do AWS IoT Wireless ou o comando [get-service-profile](#) da CLI.

```
aws iotwireless get-service-profile --id "12345678-a1b2-3c45-67d8-e90fa1b2c34d"
```

A execução desse comando gera os valores para os parâmetros do perfil de serviço.

```
{  
  "Arn": "arn:aws:iotwireless:us-east-1:651419225604:ServiceProfile/12345678-  
a1b2-3c45-67d8-e90fa1b2c34d",  
  "Id": "12345678-a1b2-3c45-67d8-e90fa1b2c34d",  
  "LoRaWAN": {  
    "UlRate": 60,  
    "UlBucketSize": 4096,  
    "DlRate": 60,  
  }  
}
```

```
    "DlBucketSize": 4096,  
    "AddGwMetadata": false,  
    "DevStatusReqFreq": 24,  
    "ReportDevStatusBattery": false,  
    "ReportDevStatusMargin": false,  
    "DrMin": 3,  
    "DrMax": 12,  
    "PrAllowed": false,  
    "HrAllowed": false,  
    "RaAllowed": false,  
    "NwkGeoLoc": false,  
    "TargetPer": 5,  
    "MinGwDiversity": 1  
  }  
}
```

Se você criou vários perfis, poderá utilizar a operação de API [ListServiceProfiles](#) ou o comando [list-service-profiles](#) da AWS CLI para listar os perfis de serviço na Conta da AWS e utilizar a API [GetServiceProfile](#) ou o comando [get-service-profile](#) da CLI para recuperar o perfil de serviço para o qual você personalizou os limites da taxa de dados.

## Gerenciar a comunicação entre os dispositivos LoRaWAN e o AWS IoT

Após conectar um dispositivo LoRaWAN ao AWS IoT Core for LoRaWAN, os dispositivos podem começar a enviar mensagens para a nuvem. As mensagens de uplink são mensagens enviadas pelo seu dispositivo e recebidas pelo AWS IoT Core for LoRaWAN. Dispositivos LoRaWAN podem enviar mensagens de uplink a qualquer momento, que são então encaminhadas para outros AWS service (Serviço da AWS) e aplicativos hospedados na nuvem. Mensagens enviadas do AWS IoT Core for LoRaWAN e outros AWS service (Serviço da AWS) e aplicativos para seus dispositivos são chamadas de mensagens de downlink.

Veja a seguir como é possível visualizar e gerenciar mensagens de uplink e downlink enviadas entre os seus dispositivos e a nuvem. É possível manter uma fila de mensagens de downlink e enviá-las para seus dispositivos na ordem em que elas foram adicionadas à fila.

### Tópicos

- [Visualizar o formato das mensagens de uplink enviadas a partir de dispositivos LoRaWAN](#)
- [Formar uma fila de mensagens de downlink para enviar para dispositivos LoRaWAN](#)

## Visualizar o formato das mensagens de uplink enviadas a partir de dispositivos LoRaWAN

Após conectar um dispositivo LoRaWAN ao AWS IoT Core for LoRaWAN, é possível observar o formato da mensagem de uplink que você receberá do seu dispositivo sem fio.

Antes de poder observar as mensagens de uplink

É preciso ter integrado seu dispositivo sem fio e conectado seu dispositivo ao AWS IoT para que ele possa transmitir e receber dados. Para acessar informações sobre a integração de dispositivos ao AWS IoT Core for LoRaWAN, consulte [Integrar os dispositivos ao AWS IoT Core for LoRaWAN](#).

O que contêm as mensagens de uplink?

Dispositivos LoRaWAN se conectam ao AWS IoT Core for LoRaWAN usando gateways LoRaWAN. A mensagem de uplink recebido do dispositivo conterá as seguintes informações.

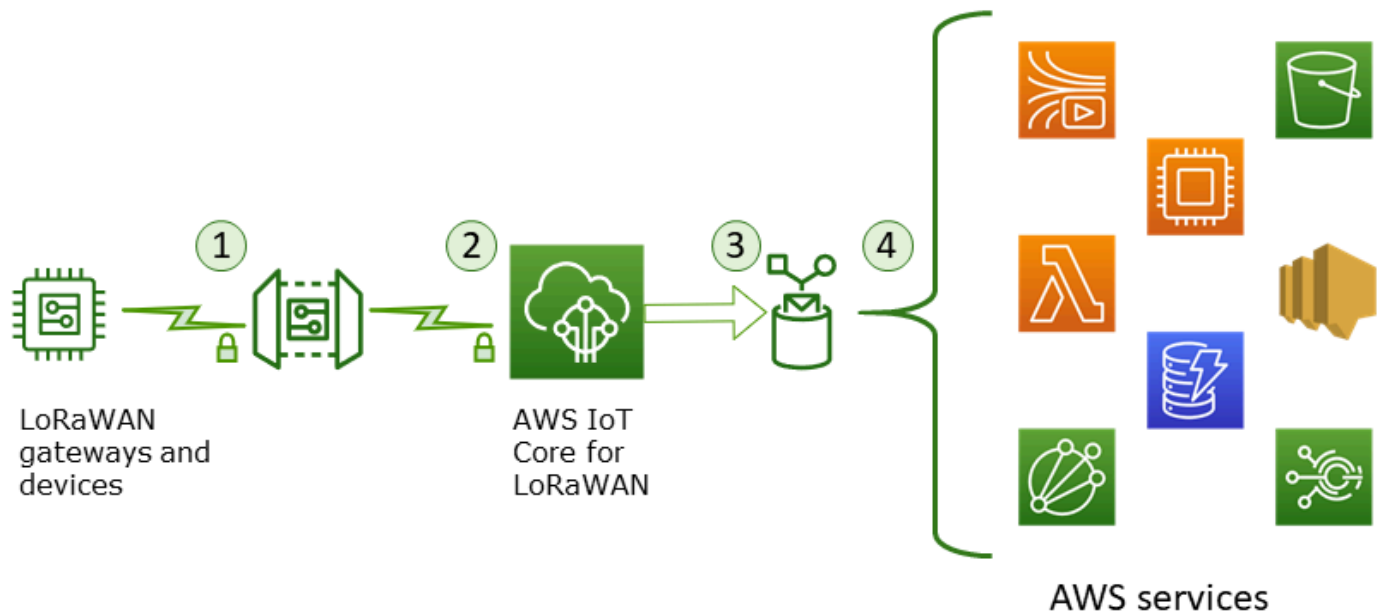
- Dados de carga que correspondem à mensagem criptografada de carga enviada a partir do dispositivo sem fio.
- Metadados sem fio que englobam:
  - Informações do dispositivo, como DevEui, taxa de dados e canal de frequência no qual o dispositivo está operando.
  - Parâmetros adicionais opcionais e informações de gateway sobre gateways conectados ao dispositivo. Os parâmetros do gateway abrangem o EUI do gateway, o SNR e o RSSI.

Usando os metadados sem fio, é possível obter informações úteis sobre o dispositivo sem fio e os dados transmitidos entre seu dispositivo e o AWS IoT. Por exemplo, é possível usar o parâmetro `AckedMessageId` para verificar se a última mensagem de downlink confirmada foi recebida pelo dispositivo. Opcionalmente, se você optar por incluir as informações de gateway, será possível identificar se deseja mudar para um canal de gateway mais forte que esteja mais próximo do dispositivo.

Como fazer para observar as mensagens de uplink?

Após integrar seu dispositivo, é possível usar o [cliente de teste MQTT](#) na página Teste do console do AWS IoT para assinar o tópico que foi especificado ao criar seu destino. Você passará a ver mensagens depois que o dispositivo estiver conectado e começar a enviar dados de carga.

O diagrama a seguir identifica os principais elementos em um sistema LoRaWAN conectado ao AWS IoT Core for LoRaWAN, que mostra o plano de dados primário e como os dados fluem pelo sistema.



Quando o dispositivo sem fio começa a enviar dados de uplink, o AWS IoT Core for LoRaWAN agrupa as informações de metadados sem fio com a carga e as envia para seus aplicativos da AWS.

Exemplo de mensagem de uplink

O exemplo a seguir exibe o formato da mensagem de uplink recebida do seu dispositivo.

```
{
  "WirelessDeviceId": "5b58245e-146c-4c30-9703-0ca942e3ff35",
  "PayloadData": "Cc48AAAAAAAAAAAA=",
  "WirelessMetadata":
  {
    "LoRaWAN":
    {
      "ADR": false,
      "Bandwidth": 125,
      "ClassB": false,
      "CodeRate": "4/5",
      "DataRate": "0",
      "DevAddr": "00b96cd4",
      "DevEui": "58a0cb000202c99",
      "FOptLen": 2,
      "FCnt": 1,
      "Fport": 136,

```

```

    "Frequency": "868100000",
    "Gateways": [
      {
        "GatewayEui": "80029cffffe5cf1cc",
        "Snr": -29,
        "Rssi": 9.75
      }
    ],
    "MIC": "7255cb07",
    "MType": "UnconfirmedDataUp",
    "Major": "LoRaWANR1",
    "Modulation": "LORA",
    "PolarizationInversion": false,
    "SpreadingFactor": 12,
    "Timestamp": "2021-05-03T03:24:29Z"
  }
}
}

```

### Exclusão de metadados do gateway dos metadados de uplink

Se quiser excluir as informações de metadados do gateway dos metadados de uplink, desative o parâmetro `AddGwMetadata` quando criar o perfil de serviço. Para acessar informações sobre como desabilitar esse parâmetro, consulte [Adicionar perfis de serviço](#).

Nesse caso, você não verá a seção `Gateways` nos metadados de uplink, como ilustrado no exemplo a seguir.

```

{
  "WirelessDeviceId": "0d9a439b-e77a-4573-a791-49d5c0f4db95",
  "PayloadData": "AAAAAAA//8=",
  "WirelessMetadata": {
    "LoRaWAN": {
      "ClassB": false,
      "CodeRate": "4/5",
      "DataRate": "1",
      "DevAddr": "01920f27",
      "DevEui": "ffffff10000163b0",
      "FCnt": 1,
      "FPort": 5,
      "Timestamp": "2021-04-29T05:19:43.646Z"
    }
  }
}

```

```
}  
}
```

## Formar uma fila de mensagens de downlink para enviar para dispositivos LoRaWAN

Aplicações hospedadas na nuvem e outros AWS service (Serviço da AWS)s podem enviar mensagens de downlink para os seus dispositivos sem fio. Mensagens de downlink são mensagens enviadas a partir do AWS IoT Core for LoRaWAN para o seu dispositivo sem fio. É possível agendar e enviar mensagens de downlink para cada dispositivo que você integrou ao AWS IoT Core for LoRaWAN.

Se tiver múltiplos dispositivos para os quais deseja enviar uma mensagem de downlink, é possível usar um grupo de multicast. Os dispositivos de um grupo de multicast compartilham o mesmo endereço multicast, que é, então, distribuído para um todo um grupo de dispositivos destinatários. Para ter mais informações, consulte [Crie grupos de multicast para enviar uma carga de downlink para vários dispositivos](#).

Como uma fila de mensagens de downlink funciona

A classe de dispositivo de um dispositivo LoRaWAN determina como as mensagens da fila são enviadas para o dispositivo. Dispositivos de classe A enviam uma mensagem de uplink ao AWS IoT Core for LoRaWAN para indicar que o dispositivo está disponível para recebimento de mensagens de downlink. Os dispositivos de classe B podem receber mensagens em slots de downlink regulares. Os dispositivos de classe C podem receber mensagens de downlink a qualquer momento. Para acessar mais informações sobre classes de dispositivos, consulte [Classes de dispositivos](#).

O seguinte mostra como as mensagens são colocadas em fila e enviadas para seus dispositivos de classe A.

1. O AWS IoT Core for LoRaWAN armazena em buffer a mensagem de downlink que você adicionou à fila com a porta do quadro, os dados da carga e os parâmetros do modo de reconhecimento especificados com o console do AWS IoT ou a API do AWS IoT Wireless.
2. O dispositivo LoRaWAN envia uma mensagem de uplink indicando que ele está on-line e pode começar a receber mensagens de downlink.
3. Caso você tenha adicionado mais de uma mensagem de downlink à fila, o AWS IoT Core for LoRaWAN envia a primeira mensagem de downlink na fila para o seu dispositivo com o sinalizador de reconhecimento (ACK) definido.

4. Seu dispositivo envia uma mensagem de uplink para o AWS IoT Core for LoRaWAN imediatamente ou permanece inativo até a próxima mensagem de uplink e inclui o sinalizador ACK na mensagem.
5. Quando o AWS IoT Core for LoRaWAN recebe a mensagem de uplink com o sinalizador ACK, ele retira a mensagem de downlink da fila, indicando que o seu dispositivo recebeu a mensagem de downlink com êxito. Se o sinalizador ACK estiver ausente da mensagem de uplink após três verificações, a mensagem será descartada.

### Executar operações de fila de downlink com o console

É possível usar o Console de gerenciamento da AWS para enfileirar mensagens de downlink e retirar mensagens individuais, ou toda a fila, conforme necessário. Com dispositivos de classe A, após um uplink ser recebido do dispositivo para indicar que ele está on-line, as mensagens em fila são enviadas para o dispositivo. Depois que a mensagem for enviada, ela será automaticamente removida da fila.

### Colocar mensagens de downlink em fila

Para criar uma fila de mensagens de downlink

1. Acesse o [hub Dispositivos do console do AWS IoT](#) e selecione o dispositivo para o qual deseja enfileirar mensagens de downlink.
2. Na seção Mensagens de downlink da página de detalhes do dispositivo, selecione Enfileirar mensagens de downlink.
3. Especifique os parâmetros a seguir para configurar sua mensagem de downlink:
  - FPort: selecione a porta do quadro usada pelo dispositivo para comunicação como o AWS IoT Core for LoRaWAN.
  - Carga: especifique a mensagem de carga que deseja enviar para o seu dispositivo. O tamanho máximo da carga é de 242 bytes. Se a taxa de dados adaptativa (ADR) estiver ativada, o AWS IoT Core for LoRaWAN a utiliza para escolher a taxa de dados ideal para o tamanho da carga. É possível otimizar ainda mais a taxa de dados conforme necessário.
  - Modo de reconhecimento: confirme se o dispositivo recebeu a mensagem de downlink. Se uma mensagem exigir esse modo, você verá uma mensagem de uplink com o sinalizador ACK no seu fluxo de dados e a mensagem será retirada da fila.
4. Para adicionar sua mensagem de downlink à fila, selecione Enviar.

Sua mensagem de downlink foi adicionada à fila. Caso não veja sua mensagem, ou se receber uma mensagem de erro, você pode solucionar o erro conforme descrito em [Solucionar erros na fila de mensagens de downlink](#).

#### Note

Depois que sua mensagem de downlink for adicionada à fila, não será mais possível editar os parâmetros FPort, Carga e Modo de reconhecimento. Para enviar uma mensagem de downlink com valores diferentes para esses parâmetros, é possível excluir essa mensagem e enfileirar uma nova mensagem de downlink com os valores de parâmetros atualizados.

A fila lista as mensagens de downlink adicionadas. Para visualizar a carga das mensagens de uplink e downlink trocadas entre seus dispositivos e o AWS IoT Core for LoRaWAN, use o analisador de rede. Para ter mais informações, consulte [Monitorar sua frota de recursos sem fio em tempo real usando o analisador de rede](#).

#### Listar fila de mensagens de downlink

A mensagem de downlink criada por você será adicionada à fila. Cada mensagem de downlink subsequente será adicionada à fila após essa mensagem. Você pode visualizar uma lista de mensagens de downlink na seção Mensagens de downlink da página de detalhes do dispositivo. Depois que um uplink for recebido, as mensagens serão enviadas para o dispositivo. Depois que uma mensagem de downlink for recebida pelo dispositivo, ela será removida da fila. A mensagem seguinte, então, sobe na fila para ser enviada ao seu dispositivo.

#### Excluir mensagens de downlink individuais ou limpar toda a fila

Cada mensagem de downlink é retirada da fila automaticamente depois de ser enviada ao seu dispositivo. Também é possível excluir mensagens individuais ou remover toda a fila de downlink. Essas ações são irreversíveis.

- Caso localize mensagens na fila que não deseje enviar, selecione as mensagens e selecione Excluir.
- Se não quiser enviar nenhuma mensagem da fila para o dispositivo, é possível remover toda a fila selecionando Limpar fila de downlink.

## Executar operações de fila de downlink com a API

É possível usar a API do AWS IoT Wireless para enfileirar mensagens de downlink e retirar mensagens individuais, ou toda a fila, conforme necessário.

### Colocar mensagens de downlink em fila

Para criar uma fila de mensagens de downlink, use a operação de API

[SendDataToWirelessDevice](#) ou o comando [send-data-to-wireless-device](#) da CLI.

```
aws iotwireless send-data-to-wireless-device \  
  --id "11aa5eae-2f56-4b8e-a023-b28d98494e49" \  
  --transmit-mode "1" \  
  --payload-data "SGVsbG8gVG8gRGV2c2lt" \  
  --wireless-metadata LoRaWAN={FPort=1}
```

Executando o comando, a saída gera um MessageId para a mensagem de downlink. Em alguns casos, mesmo que você receba o MessageId, os pacotes podem ser descartados. Para obter mais informações sobre como resolver o erro, consulte [Solucionar erros na fila de mensagens de downlink](#).

```
{  
  MessageId: "6011dd36-0043d6eb-0072-0008"  
}
```

### Listar mensagens de downlink na fila

Para listar todas as mensagens de downlink da fila, use a operação de API [ListQueuedMessages](#) ou o comando [list-queued-messages](#) da CLI.

```
aws iotwireless list-queued-messages
```

Por padrão, um máximo de 10 mensagens de downlink são exibidas ao executar esse comando.

### Remover mensagens de downlink individuais ou limpar toda a fila

Para remover mensagens individuais da fila ou limpar a fila inteira, use a operação de API [DeleteQueuedMessages](#) ou o comando [delete-queued-messages](#) da CLI.

- Para remover mensagens individuais, forneça o messageID das mensagens que deseja remover para um dispositivo sem fio, especificado pelo wirelessDeviceId.

- Para limpar a fila de downlinks inteira, especifique o messageID como \* para um dispositivo sem fio, especificado pelo wirelessDeviceId.

## Solucionar erros na fila de mensagens de downlink

Aqui estão algumas objetos para verificar, se não estiver obtendo os resultados esperados:

- As mensagens de downlink não aparecem no console do AWS IoT

Se não estiver vendo sua mensagem de downlink na fila depois de adicioná-la conforme descrito em [Executar operações de fila de downlink com o console](#), seu dispositivo talvez não tenha concluído um processo chamado procedimento de ativação ou adesão. Esse procedimento é realizado quando seu dispositivo é integrado ao AWS IoT Core for LoRaWAN. Para ter mais informações, consulte [Adicione a especificação do dispositivo sem fio ao AWS IoT Core for LoRaWAN usando o console](#).

Após integrar seu dispositivo ao AWS IoT Core for LoRaWAN, é possível monitorá-lo para verificar se a adesão e a readesão foram bem-sucedidas usando o analisador de rede ou o Amazon CloudWatch. Para ter mais informações, consulte [Ferramentas de monitoramento](#).

- Pacotes de mensagens de downlink ausentes ao usar a API

Quando você usa a operação da API `SendDataToWirelessDevice`, a API retorna um único MessageId. Entretanto, não é possível confirmar se o dispositivo LoRaWAN recebeu a mensagem de downlink. Os pacotes de downlink podem ser descartados em casos como quando o dispositivo não concluiu o procedimento de adesão. Para acessar mais informações sobre como solucionar esse erro, consulte a seção anterior.

- Erro de ARN ausente ao enviar mensagem de downlink

Quando enviar uma mensagem de downlink para seu dispositivo a partir da fila, você pode receber um erro de nome do recurso da Amazon (ARN) ausente. Esse erro pode ocorrer porque o destino não foi especificado da maneira correta para o dispositivo que está recebendo a mensagem de downlink. Para solucionar esse erro, verifique os detalhes do destino do dispositivo.

## Gerenciar o tráfego LoRaWAN de redes de dispositivos públicas LoRaWAN (Everynet)

É possível conectar seus dispositivos LoRaWAN à nuvem em minutos usando redes LoRaWAN disponíveis publicamente. O AWS IoT Core for LoRaWAN agora é compatível com a cobertura de rede da Everynet nos EUA e no Reino Unido. Quando usar a rede pública, você pagará uma taxa de conectividade de rede pública por cada dispositivo todos os meses. O preço se aplica a todas as Regiões da AWS em que a conectividade de rede pública é oferecida. Para acessar mais informações sobre os preços desse atributo, consulte a [página Definição de preço do AWS IoT Core](#).

### Important

A rede pública é operada e oferecida como um serviço diretamente pela Everynet. Antes de usar esse atributo, consulte os [Termos de serviço da AWS](#) aplicáveis. Além disso, se usar uma rede pública por meio do AWS IoT Core for LoRaWAN, determinadas informações de dispositivos LoRaWAN, como DevEUI e JoinEUI serão replicadas nas regiões onde o AWS IoT Core for LoRaWAN estiver disponível.

O AWS IoT Core for LoRaWAN é compatível com a rede pública LoRaWAN, de acordo com a especificação da LoRa Alliance para roaming, descrita em [LoRaWAN Backend Interfaces 1.0 Specification](#). O recurso de rede pública pode ser utilizado para conectar os dispositivos finais que estão fora da rede doméstica. Para oferecer compatibilidade com esse recurso e fornecer cobertura de rádio ampliada, o AWS IoT Core for LoRaWAN utiliza a Everynet como parceira.

### Benefícios de usar uma rede pública LoRaWAN

Seus dispositivos LoRaWAN podem usar uma rede pública para conexão com a nuvem, o que reduz o tempo de implantação e o tempo e custo necessários para manutenção de uma rede LoRaWAN privada.

Usando uma rede pública LoRaWAN, você receberá benefícios como extensão de cobertura, execução de núcleo sem rede de rádio e densificação de cobertura. Esse atributo pode ser usado para:

- Fornecer cobertura a dispositivos quando eles saírem da rede doméstica, como o Dispositivo A na imagem exibida na seção [Arquitetura de suporte de rede pública LoRaWAN](#).

- Ampliar a cobertura para dispositivos que não possuem um gateway LoRa para se conectar, como o Dispositivo B na imagem exibida na seção [Arquitetura de suporte de rede pública LoRaWAN](#). O dispositivo poderá, então, usar o gateway fornecido pelo parceiro para se conectar à rede doméstica.

Os dispositivos LoRaWAN podem usar uma rede pública para conexão com a nuvem utilizando o recurso de roaming, o que reduz o tempo de implantação e o tempo e o custo necessários para manutenção de uma rede LoRaWAN privada.

As seções a seguir descrevem a arquitetura de suporte da rede pública, o funcionamento do suporte da rede pública LoRaWAN e como usar esse atributo.

### Tópicos

- [Como funciona o suporte da rede pública LoRaWAN](#)
- [Como usar o suporte de rede pública](#)

## Como funciona o suporte da rede pública LoRaWAN

O AWS IoT Core for LoRaWAN é compatível com o atributo de roaming passivo, conforme a especificação LoRa Alliance. Com o roaming passivo, o processo de roaming é inteiramente transparente para o dispositivo final. Os dispositivos finais em roaming fora da rede doméstica podem se conectar aos gateways nessa rede pública e trocar dados de uplink e de downlink utilizando o servidor de aplicações. Os dispositivos permanecem conectados à rede doméstica no decorrer de todo o processo de roaming.

### Note

O AWS IoT Core for LoRaWAN é compatível somente com o atributo sem estado do roaming passivo. O roaming de transferência não é compatível. No roaming de transferência, o dispositivo mudará para outra operadora quando viajar para fora da rede doméstica.

### Tópicos

- [Conceitos da rede pública LoRaWAN](#)
- [Arquitetura de suporte de rede pública LoRaWAN](#)

## Conceitos da rede pública LoRaWAN

Esses conceitos são utilizados pelo recurso de rede pública compatível com o AWS IoT Core for LoRaWAN.

### Servidor da rede LoRaWAN (LNS)

Um LNS é um servidor privado autônomo que pode ser executado nas suas instalações ou pode ser um serviço baseado em nuvem. O AWS IoT Core for LoRaWAN é um LNS que oferece serviços na nuvem.

### Servidor de rede doméstica (hNS)

A rede doméstica é a rede à qual pertence o dispositivo. O servidor de rede doméstica (hNS) é um LNS em que o AWS IoT Core for LoRaWAN armazena os dados de provisionamento do dispositivo, como DevEUI, AppEUI e chaves de sessão.

### Servidor de rede visitada (vNS)

A rede visitada é a rede através da qual o dispositivo recebe cobertura quando sai da rede doméstica. O servidor de rede visitada (vNS) é um LNS que tem um acordo comercial e técnico com os hNS para poder atender ao dispositivo final. O parceiro da AWS, Everynet, atua como a rede visitada para oferecer cobertura.

### Servidor de rede de atendimento (sNS)

O servidor de rede de atendimento (sNS) é um LNS que lida com os comandos MAC para o dispositivo. Só pode haver um sNS para uma sessão LoRa.

### Servidor de rede de encaminhamento (fNS)

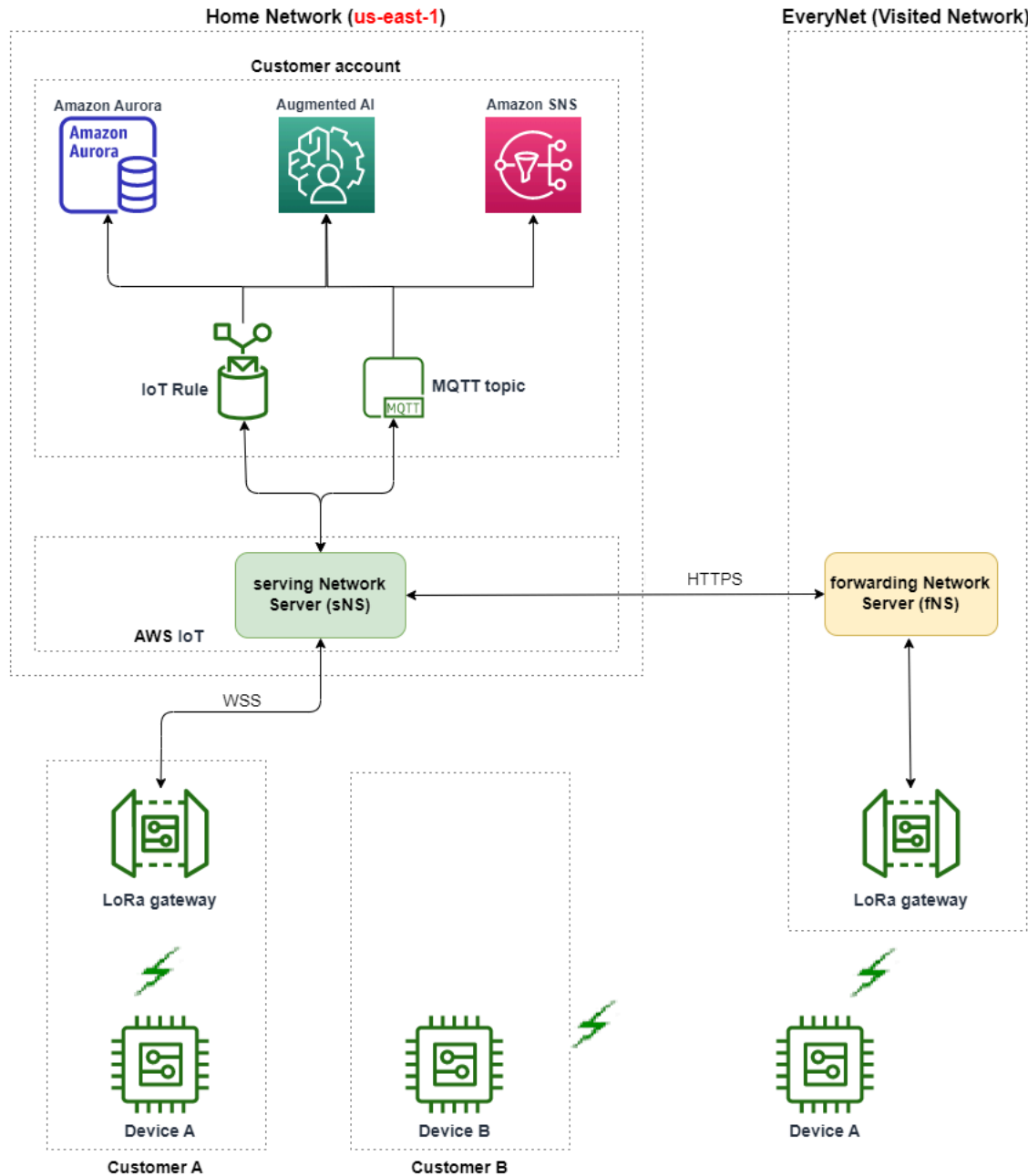
O servidor de rede de encaminhamento (fNS) é um LNS que gerencia os gateways de rádio. Pode ser que haja zero ou mais fNS envolvidos em uma sessão LoRa. Esse servidor de rede gerencia o encaminhamento dos pacotes de dados que são recebidos do dispositivo para a rede doméstica.

## Arquitetura de suporte de rede pública LoRaWAN

O seguinte diagrama de arquitetura demonstra como o AWS IoT Core for LoRaWAN faz parceria com a Everynet para oferecer conectividade de rede pública. Nesse caso, o Dispositivo A está conectado ao hNS (servidor de rede doméstica) fornecido pelo AWS IoT Core for LoRaWAN meio de um gateway LoRa. Quando o Dispositivo A sai da rede doméstica, ele ingressa em uma rede visitada

e é coberto pelo servidor de rede visitada (vNS) oferecido pela Everynet. O vNS também amplia a cobertura ao Dispositivo B, que não tem um gateway LoRa ao qual se conectar.

É possível visualizar as informações de cobertura da rede pública no console do AWS IoT, conforme descrito na seção a seguir.



O AWS IoT Core for LoRaWAN usa uma funcionalidade de hub de roaming, em conformidade com a [Recomendação técnica do de hub de roaming LoRaWAN da LoRa Alliance](#). O hub de roaming

oferece um endpoint para a Everynet rotear o tráfego recebido a partir do dispositivo final. Nesse caso, a Everynet atua como um servidor de rede de encaminhamento (fNS) para encaminhar o tráfego recebido a partir do dispositivo. Ela usa uma API RESTful de HTTP, conforme definido pela especificação da LoRa Alliance.

#### Note

Se o dispositivo sair da rede doméstica e entrar em um local onde tanto a rede doméstica quanto a Everynet estiverem disponíveis, ele se conectará ao primeiro gateway que aparecer (LoRa ou Everynet).

Ao visitar uma rede pública, os hNS e o servidor de rede de atendimento (sNS) são separados. Pacotes de uplink e downlink são, então, trocados entre os sNS e os hNS.

## Como usar o suporte de rede pública

Para habilitar a compatibilidade com a rede pública Everynet, especifique determinados parâmetros de roaming ao criar um perfil de serviço. Nesta versão beta, esses parâmetros estão disponíveis quando você utiliza a API do AWS IoT Wireless ou a AWS CLI. As seções a seguir mostram os parâmetros que devem ser habilitados e como habilitar a rede pública utilizando a AWS CLI.

#### Note

Só é possível ativar o suporte de rede pública ao criar um novo perfil de serviço. Não é possível atualizar um perfil existente para habilitar a rede pública usando esses parâmetros.

## Tópicos

- [Parâmetros de roaming](#)
- [Habilitar o suporte de rede pública para dispositivos](#)

## Parâmetros de roaming

Especifique os seguintes parâmetros quando criar um perfil de serviço para um dispositivo. Especifique esses parâmetros ao adicionar um perfil de serviço no hub [Perfis](#) do console do AWS IoT ou utilizando a operação de API [CreateServiceProfile](#) ou o comando [create-service-profile](#) da AWS CLI.

**Note**

O AWS IoT Core for LoRaWAN não é compatível com roaming de transferência. Na criação do perfil de serviço, não é possível ativar o parâmetro `HrAllowed` que especifica se o roaming de transferência deve ser usado.

- Ativação de roaming permitida (`RaAllowed`): esse parâmetro especifica se a ativação de roaming deve ser habilitada. A ativação de roaming possibilita que um dispositivo final seja ativado sob a cobertura de uma vNS. Ao usar o atributo de roaming, `RaAllowed` deve ser definido como `true`.
- Roaming passivo permitido (`PrAllowed`): esse parâmetro especifica se o roaming passivo deve ser habilitado. Ao usar o atributo de roaming, `PrAllowed` deve ser definido como `true`.

### Habilitar o suporte de rede pública para dispositivos

Para habilitar o suporte de rede pública LoRaWAN nos dispositivos, execute o procedimento a seguir.

**Note**

Só é possível ativar o recurso de rede pública para dispositivos OTAA. Esse atributo não é compatível com dispositivos que usem ABP como método de ativação.

1. Crie um perfil de serviço com parâmetros de roaming

Crie um perfil de serviço habilitando os parâmetros de roaming.

**Note**

Na criação de um perfil de dispositivo para o dispositivo que você associará a esse perfil de serviço, recomendamos especificar um valor grande para o parâmetro `RxDelay1`, ao menos maior que 2 segundos.

- Usar o console de AWS IoT

Vá para o hub [Perfis](#) do console do AWS IoT e selecione Adicionar perfil de serviço. Na criação do perfil, selecione Habilitar rede pública.

- Uso da API AWS IoT Wireless

Para habilitar o roaming ao criar um perfil de serviço, utilize a operação de API [CreateServiceProfile](#) ou o comando [create-service-profile](#) da CLI, conforme mostrado no exemplo a seguir.

```
aws iotwireless create-service-profile \  
  --region us-east-1 \  
  --name roamingprofile1 \  
  --lorawan '{"AddGwMetadata":true,"PrAllowed":true,"RaAllowed":true}'
```

A saída da execução desse comando retorna o ARN e o ID do perfil de serviço.

```
{  
  "Arn": "arn:aws:iotwireless:us-east-1:123456789012:ServiceProfile/12345678-  
a1b2-3c45-67d8-e90fa1b2c34d",  
  "Id": "12345678-a1b2-3c45-67d8-e90fa1b2c34d"  
}
```

## 2. Verifique os parâmetros de roaming no perfil de serviço

Para verificar os parâmetros de roaming especificados, é possível visualizar o perfil do serviço no console ou usar o comando `get-service-profile` da CLI, conforme exibido no exemplo abaixo.

- Usar o console de AWS IoT

Vá para o hub [Perfis](#) do console do AWS IoT e selecione o perfil que você criou. Na guia Configuração do perfil da página de detalhes, você poderá ver `RaAllowed` `PrAllowed` definidos como `true`.

- Uso da API AWS IoT Wireless

Para visualizar os parâmetros de roaming ativados por você, use a operação de API [GetServiceProfile](#) ou o comando [get-service-profile](#) da CLI, conforme exibido no exemplo abaixo.

```
aws iotwireless get-service-profile \  
  --profile-id 12345678-a1b2-3c45-67d8-e90fa1b2c34d
```

```
--region us-east-1 \  
--id 12345678-a1b2-3c45-67d8-e90fa1b2c34d
```

A saída da execução desse comando retorna os detalhes do perfil de serviço, incluindo os valores dos parâmetros de roaming. RaAllowed e PrAllowed.

```
{  
  "Arn": "arn:aws:iotwireless:us-east-1:123456789012:ServiceProfile/12345678-a1b2-3c45-67d8-e90fa1b2c34d",  
  "Id": "12345678-a1b2-3c45-67d8-e90fa1b2c34d",  
  "Name": "roamingprofile1"  
  "LoRaWAN": {  
    "UlRate": 60,  
    "UlBucketSize": 4096,  
    "DlRate": 60,  
    "DlBucketSize": 4096,  
    "AddGwMetadata": true,  
    "DevStatusReqFreq": 24,  
    "ReportDevStatusBattery": false,  
    "ReportDevStatusMargin": false,  
    "DrMin": 0,  
    "DrMax": 15,  
    "PrAllowed": true,  
    "RaAllowed": true,  
    "NwkGeoLoc": false,  
    "TargetPer": 5,  
    "MinGwDiversity": 1  
  }  
}
```

### 3. Anexe o perfil de serviço aos dispositivos

Anexe o perfil de serviço criado com os parâmetros de roaming aos dispositivos finais. Também é possível criar um perfil de dispositivo e adicionar um destino para os dispositivos sem fio. Você usará esse destino para rotear mensagens de uplink que são enviadas a partir do seu dispositivo. Para acessar mais informações sobre como criar perfis de dispositivos e um destino, consulte [Adicionar perfis de dispositivos](#) e [Adicionar destinos ao AWS IoT Core for LoRaWAN](#).

- Integração de dispositivos novos

Caso ainda não tenha integrado seus dispositivos, especifique esse perfil de serviço, que será usado ao adicionar seu dispositivo ao AWS IoT Core for LoRaWAN. O seguinte comando

mostra como você pode usar o comando `create-wireless-device` da CLI para adicionar um dispositivo usando o ID do perfil de serviço criado por você. Para obter informações sobre como adicionar o perfil de serviço utilizando o console, consulte [Adicione a especificação do dispositivo sem fio ao AWS IoT Core for LoRaWAN usando o console](#).

```
aws iotwireless create-wireless-device --cli-input-json file://createdevice.json
```

O exemplo a seguir mostra o conteúdo do arquivo `createdevice.json`.

Conteúdo do `createdevice.json`

```
{
  "Name": "DeviceA",
  "Type": LoRaWAN,
  "DestinationName": "RoamingDestination1",
  "LoRaWAN": {
    "DeviceProfileId": "ab0c23d3-b001-45ef-6a01-2bc3de4f5333",
    "ServiceProfileId": "12345678-a1b2-3c45-67d8-e90fa1b2c34d",
    "OtaaV1_1": {
      "AppKey": "3f4ca100e2fc675ea123f4eb12c4a012",
      "JoinEui": "b4c231a359bc2e3d",
      "NwkKey": "01c3f004a2d6efffe32c4eda14bcd2b4"
    },
    "DevEui": "ac12efc654d23fc2"
  },
}
```

A saída da execução desse comando produz o ARN e o ID do dispositivo sem fio.

```
{
  "Arn": "arn:aws:iotwireless:us-
east-1:123456789012:WirelessDevice/1ffd32c8-8130-4194-96df-622f072a315f",
  "Id": "1ffd32c8-8130-4194-96df-622f072a315f"
}
```

- Atualização de dispositivos existentes

Se já tiver integrado seus dispositivos, é possível atualizar seus dispositivos sem fio existentes para usar esse perfil de serviço. O seguinte comando mostra como você pode usar o comando `update-wireless-device` da CLI para atualizar um dispositivo usando o ID do perfil de serviço criado por você.

```
aws iotwireless update-wireless-device \  
  --id "1ffd32c8-8130-4194-96df-622f072a315f" \  
  --service-profile-id "12345678-a1b2-3c45-67d8-e90fa1b2c34d" \  
  --description "Using roaming service profile A"
```

Esse comando não retorna nenhuma saída. É possível usar a API `GetWirelessDevice` ou o comando `get-wireless-device` da CLI para obter as informações atualizadas.

#### 4. Conectar o dispositivo à nuvem usando a Everynet

Como o roaming foi habilitado, seu dispositivo deve agora realizar uma adesão para obter um novo `DevAddr`. Quando você utiliza o OTAA, o dispositivo LoRaWAN envia uma solicitação de junção e o servidor de rede pode permitir a solicitação. Depois, ele pode se conectar ao Nuvem AWS com a cobertura de rede fornecida pela Everynet. Para obter instruções sobre como realizar o procedimento de ativação ou adesão com o seu dispositivo, consulte a documentação do dispositivo.

#### Note

- É possível habilitar o recurso de roaming e a conexão à rede pública somente para dispositivos que utilizam o OTAA como o método de ativação. Dispositivos ABP não são compatíveis. Para obter instruções sobre como realizar o procedimento de ativação ou adesão com o seu dispositivo, consulte a documentação do dispositivo. Consulte [Modos de ativação](#).
- Para desabilitar o recurso de roaming para os dispositivos, é possível desassociá-los desse perfil de serviço e associá-los a outro perfil de serviço que tenha os parâmetros de roaming definidos como `false`. Após a mudança para esse perfil de serviço, os dispositivos devem realizar outra junção para que não continuem executando na rede pública.

#### 5. Trocar mensagens de uplink e downlink

Depois que o dispositivo se conectar ao AWS IoT Core for LoRaWAN, será possível começar a trocar mensagens entre seu dispositivo e a nuvem.

- Visualizar mensagens de uplink

Ao enviar mensagens de uplink a partir dos seus dispositivos, o AWS IoT Core for LoRaWAN entrega essas mensagens para a sua Conta da AWS usando o destino configurado anteriormente. Essas mensagens serão enviadas a partir do seu dispositivo para a nuvem pela rede da Everynet.

É possível visualizar as mensagens usando o nome da regra do AWS IoT ou usar o cliente MQTT para assinar o tópico MQTT especificado na criação do destino. Para acessar mais informações sobre o nome da regra e outros detalhes do destino que você especificar, consulte [Adicionar um destino usando o console](#).

Para acessar mais informações sobre a visualização de mensagens de uplink e o formato, consulte, [Visualizar o formato das mensagens de uplink enviadas a partir de dispositivos LoRaWAN](#).

- Enviar mensagens de downlink

É possível enfileirar e enviar mensagens de downlink para seus dispositivos a partir do console ou usando o comando de API do AWS IoT Wireless, `SendDataToWirelessDevice`, ou o comando da AWS CLI, `send-data-to-wireless-device`. Para acessar informações sobre como enfileirar e enviar mensagens de downlink, consulte [Formar uma fila de mensagens de downlink para enviar para dispositivos LoRaWAN](#).

O seguinte código exibe um exemplo de como você pode enviar uma mensagem de downlink usando o comando `send-data-to-wireless-device` da CLI. Você especifica o ID do dispositivo sem fio para receber os dados, a carga, se deve usar o modo de reconhecimento e os metadados sem fio.

```
aws iotwireless send-data-to-wireless-device \
  --id "1ffd32c8-8130-4194-96df-622f072a315f" \
  --transmit-mode "1" \
  --payload-data "SGVsbG8gVG8gRGV2c2lt" \
  --wireless-metadata LoRaWAN={FPort=1}
```

Executando o comando, a saída gera um `MessageId` para a mensagem de downlink.

**Note**

Em alguns casos, mesmo que você receba o MessageId, os pacotes podem ser descartados. Para acessar informações sobre como solucionar problemas em tais cenários, consulte [Solucionar erros na fila de mensagens de downlink](#).

```
{  
  MessageId: "6011dd36-0043d6eb-0072-0008"  
}
```

- Visualizar as informações de cobertura

Depois de habilitar a rede pública, será possível visualizar as informações de cobertura da rede no console do AWS IoT. Acesse o hub [Cobertura](#) do console do AWS IoT e, então, pesquise locais para visualizar as informações de cobertura de seus dispositivos no mapa.

**Note**

Esse atributo utiliza o Amazon Location Service para exibir as informações de cobertura dos seus dispositivos em um mapa de localização da Amazon. Antes de usar os mapas de localização da Amazon, examine os Termos e Condições do Amazon Location Service. Observe que a AWS pode transmitir suas consultas de API para o provedor de dados de terceiros selecionado, que pode estar fora da Região da AWS que você usa atualmente. Para obter mais informações, consulte [Termos de serviço da AWS](#).

## Executar a atualização de firmware sem fios (FUOTA) para dispositivos LoRaWAN e grupos multicast

É possível executar a atualização de firmware sem fios para atualizar o firmware de um único dispositivo LoRaWAN ou de um grupo de dispositivos. Para atualizar o firmware do dispositivo ou enviar uma carga útil de downlink a vários dispositivos, crie um grupo multicast. Com o multicast, uma fonte pode enviar dados a um único grupo multicast, que são então distribuídos para um grupo inteiro de dispositivos destinatários.

A compatibilidade do AWS IoT Core for LoRaWAN com o FUOTA e grupos de multicast é baseada nas seguintes especificações da [LoRa Alliance](#):

- LoRaWAN Remote Multicast Setup Specification, TS005-2.0.0
- LoRaWAN Fragmented Data Block Transportation Specification, TS004-2.0.0
- LoRaWAN Application Layer Clock Synchronization Specification, TS003-2.0.0

#### Note

O AWS IoT Core for LoRaWAN executa automaticamente a sincronização de relógio em conformidade com a especificação da LoRa Alliance. Ele usa a função `AppTimeReq` para responder a hora do servidor aos dispositivos que a solicitam usando a sinalização `ClockSync`.

Os tópicos a seguir mostram como criar grupos multicast e executar o FUOTA.

#### Tópicos

- [Preparar dispositivos para configuração multicast e FUOTA](#)
- [Crie grupos de multicast para enviar uma carga de downlink para vários dispositivos](#)
- [Atualização de firmware sem fios \(FUOTA\) para dispositivos do AWS IoT Core for LoRaWAN](#)


## Preparar dispositivos para configuração multicast e FUOTA

Quando adicionar seu dispositivo sem fio ao AWS IoT Core for LoRaWAN, é possível prepará-lo para a configuração multicast e FUOTA usando o console ou a CLI. Se estiver executando essa configuração pela primeira vez, recomendamos que você use o console. Para gerenciar seu grupo de multicast e adicionar ou remover vários dispositivos do grupo, recomendamos que você use a CLI para gerenciar um grande número de recursos.

### GenAppKey e FPorts


Ao adicionar um dispositivo sem fio, para poder adicionar os dispositivos a grupos multicast ou executar o FUOTA, configure os parâmetros a seguir. Antes de configurar esses parâmetros, verifique se seus dispositivos são compatíveis com FUOTA e multicast e se a especificação do dispositivo sem fio é OTAA v1.1 ou OTAAv1.0.x.

- **GenAppKey:** para dispositivos compatíveis com a versão 1.0.x do LoRaWAN e para usar grupos de multicast, a GenAppKey é a chave raiz específica do dispositivo da qual as chaves de sessão do seu grupo de multicast derivam.

 Note

Para dispositivos LoRaWAN que usam a especificação sem fio OTAA v1.1, a AppKey é usada para a mesma finalidade que a GenAppKey.

Para configurar os parâmetros para iniciar a transferência de dados, o AWS IoT Core for LoRaWAN distribui as chaves de sessão para os dispositivos finais. Para acessar mais informações sobre as versões do LoRaWAN, consulte [Versão LoRaWAN](#).

 Note

O AWS IoT Core for LoRaWAN armazena as informações da GenAppKey fornecidas por você em um formato criptografado.

- **FPorts:** em conformidade com as especificações do LoRaWAN para FUOTA e grupos de multicast, o AWS IoT Core for LoRaWAN atribui os valores padrão para os seguintes campos do parâmetro FPorts. Caso você já tenha atribuído algum dos valores de FPort a seguir, será possível escolher um outro valor entre 1 e 223 que esteja disponível.
  - **Multicast:** 200  
Esse valor de FPort é usado para grupos de multicast.
  - **FUOTA:** 201  
Esse valor de FPort é usado para FUOTA.
  - **ClockSync:** 202  
Esse valor de FPort é usado para a sincronização do relógio.

## Perfis de dispositivos para multicast e FUOTA

No início de uma sessão multicast, uma janela de distribuição de classe B ou classe C é utilizada para enviar a mensagem de downlink aos dispositivos do seu grupo. Os dispositivos adicionados por você para multicast e FUOTA devem ser compatíveis com os modos de operação de classe B

ou classe C. Dependendo da classe de dispositivo compatível com seu dispositivo, selecione um perfil de dispositivo para seu dispositivo que esteja com um ou ambos os modos classe B ou classe C ativados.

Para acessar mais informações sobre perfis de dispositivos, consulte [Adicionar perfis ao AWS IoT Core for LoRaWAN](#).

## Preparar dispositivos para multicast e FUOTA com o console

Para especificar os parâmetros FPorts e GenAppKey para configuração de multicast e FUOTA com o console:

1. Navegue até o [hub Dispositivos do console do AWS IoT](#) e selecione Adicionar dispositivo sem fio.
2. Selecione a Especificação do dispositivo sem fio. É preciso que o dispositivo use OTAA para ativação do dispositivo. Quando você seleciona OTAA v1.0.x ou OTAA v1.1, uma seção Configuração FUOTA - Opcional aparecerá.
3. Informe os parâmetros EUI (Identificador Exclusivo Estendido) para seu dispositivo sem fio.
4. Expanda a seção Configuração FUOTA - Opcional e selecione Este dispositivo é compatível com atualizações de firmware sem fio (FUOTA). Você pode agora informar os valores de FPort para multicast, FUOTA e sincronização de relógio. Caso tenha escolhido OTAA v1.0.x para a especificação do dispositivo sem fio, informe a GenAppKey.
5. Adicione seu dispositivo ao AWS IoT Core for LoRaWAN selecionando seus perfis e um destino para roteamento de mensagens. Para o perfil de dispositivo vinculado ao dispositivo, certifique-se de selecionar um ou ambos os modos Compatível com Classe B ou Compatível com Classe C.

### Note

Para especificar os parâmetros de configuração do FUOTA, é preciso usar o [hub Dispositivos do console do AWS IoT](#). Esses parâmetros não aparecerão se você integrar os dispositivos usando a página Introdução do console do AWS IoT.

Para acessar mais informações sobre a especificação de dispositivos sem fio e a integração de um dispositivo, consulte [Adicione o dispositivo sem fio ao AWS IoT Core for LoRaWAN](#).

**Note**

Só é possível especificar esses parâmetros na criação do dispositivo sem fio. Não é possível alterar ou especificar parâmetros ao atualizar um dispositivo existente.

## Preparar dispositivos para multicast e FUOTA com a operação de API

Para utilizar grupos multicast ou executar o FUOTA, configure esses parâmetros utilizando a operação de API [CreateWirelessDevice](#) ou o comando [create-wireless-device](#) da CLI. Além de especificar a chave do aplicativo e os parâmetros FPorts, verifique se o perfil do dispositivo que está vinculado ao dispositivo é compatível com um ou ambos os modos de classe B ou classe C. É possível fornecer um arquivo `input.json` como entrada para o comando `create-wireless-device`.

```
aws iotwireless create-wireless-device \  
  --cli-input-json file://input.json
```

onde:

Conteúdo de `input.json`

```
{  
  "Description": "My LoRaWAN wireless device"  
  "DestinationName": "IoTWirelessDestination"  
  "LoRaWAN": {  
    "DeviceProfileId": "ab0c23d3-b001-45ef-6a01-2bc3de4f5333",  
    "ServiceProfileId": "fe98dc76-cd12-001e-2d34-5550432da100",  
    "FPorts": {  
      "ClockSync": 202,  
      "Fuota": 201,  
      "Multicast": 200  
    },  
    "OtaaV1_0_x": {  
      "AppKey": "3f4ca100e2fc675ea123f4eb12c4a012",  
      "AppEui": "b4c231a359bc2e3d",  
      "GenAppKey": "01c3f004a2d6efffe32c4eda14bcd2b4"  
    },  
    "DevEui": "ac12efc654d23fc2"  
  },  
  "Name": "SampleIoTWirelessThing"
```

```
"Type": LoRaWAN  
}
```

Para obter informações sobre os comandos da CLI que você pode usar, consulte [referência da AWS CLI](#).

#### Note

Após especificar os valores desses parâmetros, não será possível atualizá-los usando a operação de API `UpdateWirelessDevice`. Ao invés disso, você pode criar um novo dispositivo com os valores dos parâmetros `GenAppKey` e `FPorts`.

Para acessar informações sobre os valores especificados para esses parâmetros, é possível usar a operação de API [GetWirelessDevice](#) ou o comando [get-wireless-device](#) da CLI.

## Próximas etapas

Após configurar os parâmetros, é possível criar grupos de multicast e tarefas FUOTA para enviar carga de downlink ou atualizar o firmware dos dispositivos LoRaWAN.

- Para acessar informações sobre a criação de grupos de multicast, consulte [Criar grupos de multicast e adicionar dispositivos ao grupo](#).
- Para acessar informações sobre como criar tarefas FUOTA, consulte [Criar uma tarefa FUOTA e fornecer a imagem de firmware](#).

## Crie grupos de multicast para enviar uma carga de downlink para vários dispositivos

Para enviar uma carga de downlink para vários dispositivos, crie um grupo de multicast. Com o multicast, uma fonte pode enviar dados para um único endereço multicast, que é, então, distribuído para um grupo inteiro de dispositivos destinatários.

Os dispositivos de um grupo de multicast compartilham o mesmo endereço multicast, chaves de sessão e contador de quadros. Usando as mesmas chaves de sessão, os dispositivos de um grupo de multicast podem descriptografar a mensagem quando uma transmissão de downlink for iniciada. Um grupo de multicast é compatível apenas com downlink. Ele não confirma se a carga do downlink foi recebida pelos dispositivos.

Com os grupos multicast do AWS IoT Core for LoRaWAN, você pode:

- Filtrar sua lista de dispositivos com o perfil de dispositivo, RFRegion ou classe de dispositivo e, depois, adicionar esses dispositivos a um grupo de multicast.
- Agendar e enviar uma ou mais mensagens de carga de downlink a dispositivos em um grupo de multicast dentro de uma janela de distribuição de 48 horas.
- Fazer com que os dispositivos mudem temporariamente para o modo Classe B ou Classe C no início da sua sessão multicast para receber a mensagem de downlink.
- Monitorar a configuração de um grupo de multicast e o estado de seus dispositivos, além de solucionar quaisquer problemas.
- Usar atualizações de firmware sem fio (FUOTA) para implantar com segurança atualizações de firmware em dispositivos em um grupo de multicast.

O vídeo a seguir descreve como é possível criar grupos multicast do AWS IoT Core for LoRaWAN e fornece orientações sobre o processo de adição de um dispositivo ao grupo e a programação de uma mensagem de downlink para o grupo.

O seguinte demonstra como criar seu grupo de multicast e programar uma mensagem de downlink.

## Tópicos

- [Criar grupos de multicast e adicionar dispositivos ao grupo](#)
- [Monitorar e solucionar problemas do status de um grupo de multicast e dos dispositivos do grupo](#)
- [Agendar uma mensagem de downlink para enviar para os dispositivos de um grupo de multicast](#)

## Criar grupos de multicast e adicionar dispositivos ao grupo

É possível criar grupos de multicast usando o console ou a CLI. Se estiver criando seu grupo de multicast pela primeira vez, recomendamos usar o console para adicionar seu grupo de multicast. Quando desejar gerenciar seu grupo de multicast e adicionar ou remover dispositivos do grupo, você pode usar a CLI.

Após trocar a sinalização com os dispositivos finais adicionados, o AWS IoT Core for LoRaWAN estabelece as chaves compartilhadas com os dispositivos finais e configura os parâmetros para a transferência de dados.

## Pré-requisitos

Antes de criar grupos de multicast e adicionar dispositivos ao grupo:

- Prepare seus dispositivos para configuração de multicast e FUOTA especificando os parâmetros de configuração da FUOTA GenAppKey e FPorts. Para ter mais informações, consulte [Preparar dispositivos para configuração multicast e FUOTA](#).
- Verifique se os dispositivos são compatíveis com os modos de operação de classe B ou de classe C. Dependendo da classe de dispositivo compatível com seu dispositivo, selecione um perfil de dispositivo que esteja com um ou ambos os modos Compatível com classe B ou Compatível com classe C ativados. Para acessar mais informações sobre perfis de dispositivos, consulte [Adicionar perfis ao AWS IoT Core for LoRaWAN](#).

No início da sessão multicast, uma janela de distribuição de classe B ou classe C é utilizada para enviar mensagens de downlink aos dispositivos do seu grupo.

## Criar grupos de multicast usando o console

Para criar grupos de multicast com o console, acesse a página [Grupos de multicast](#) do console do AWS IoT e selecione Criar grupo de multicast.

### 1. Crie um grupo de multicast

Para criar um grupo de multicast, especifique as propriedades e tags de multicast do grupo.

#### 1. Especifique as propriedades de multicast

Para especificar propriedades de multicast, insira as informações a seguir relativas ao grupo de multicast.

- **Nome:** insira um nome exclusivo do grupo de multicast. O nome só pode conter letras, números, hifens e sublinhado. Ele não pode conter espaços.
- **Descrição:** você pode fornecer uma descrição opcional do grupo de multicast. A descrição pode ser até 2.048 caracteres de comprimento.

#### 2. Tags para grupo de multicast

Opcionalmente, é possível fornecer quaisquer pares de valores-chave como Tags para o grupo de multicast. Para continuar criando o grupo de multicast, selecione Próximo.

## 2. Adicione dispositivos a um grupo de multicast

É possível adicionar dispositivos individuais ou um grupo de dispositivos ao seu grupo de multicast. Para adicionar dispositivos:

### 1. Especifique a RFRegion

Especifique a RFRegion ou a banda de frequência do grupo de multicast. A RFRegion do grupo de multicast deve corresponder à RFRegion dos dispositivos que você adiciona ao grupo de multicast. Para obter mais informações sobre a RFRegion, consulte [Considere a seleção de faixas de frequência LoRa para os gateways e conexão de dispositivos](#).

### 2. Selecione uma classe de dispositivo multicast

Escolha se você deseja que dispositivos do grupo de multicast mudem para o modo classe B ou classe C no início da sessão multicast. Uma sessão de classe B pode receber mensagens de downlink em slots regulares de downlink e uma sessão de classe C pode receber mensagens de downlink a qualquer instante.

### 3. Escolha os dispositivos que deseja adicionar ao grupo

Escolha se você deseja adicionar dispositivos ao grupo de multicast de modo individual ou em lotes.

- Para adicionar os dispositivos individualmente, insira o ID do dispositivo sem fio de cada dispositivo que você quer adicionar ao grupo.
- Para adicionar dispositivos em lotes, é possível filtrar os dispositivos que você deseja adicionar por perfil ou tags do dispositivo. No perfil de dispositivo, você pode adicionar dispositivos com um perfil compatível com classe B, classe C ou ambas as classes de dispositivos.

### 4. Para criar um grupo de multicast, selecione Criar.

Os detalhes do grupo de multicast e os dispositivos adicionados aparecem no grupo. Para acessar informações sobre o status do grupo de multicast e seus dispositivos e para solucionar quaisquer problemas, consulte [Monitorar e solucionar problemas do status de um grupo de multicast e dos dispositivos do grupo](#).

Após criar um grupo de multicast, você pode selecionar Ação para editar, excluir ou adicionar dispositivos ao grupo de multicast. Após adicionar os dispositivos, é possível agendar uma sessão para que a carga de downlink seja enviada para os dispositivos do grupo.

## Criar grupos de multicast usando a API

Para criar grupos de multicast e adicionar dispositivos ao grupo usando a API:

### 1. Crie um grupo de multicast

Para criar o grupo de multicast, use a operação de API [CreateMulticastGroup](#) ou o comando [create-multicast-group](#) da CLI. É possível fornecer um arquivo `input.json` como entrada para o comando `create-multicast-group`.

```
aws iotwireless create-multicast-group \  
  --cli-input-json file://input.json
```

onde:

Conteúdo de `input.json`

```
{  
  "Description": "Multicast group to send downlink payload and perform FUOTA.",  
  "LoRaWAN": {  
    "DlClass": "ClassB",  
    "RfRegion": "US915"  
  },  
  "Name": "MC_group_FUOTA"  
}
```

Após criar seu grupo de multicast, é possível usar as seguintes operações de API ou comandos da CLI para atualizar, excluir ou obter informações sobre os seus grupos de multicast.

- [UpdateMulticastGroup](#) ou [update-multicast-group](#)
- [GetMulticastGroup](#) ou [get-multicast-group](#)
- [ListMulticastGroups](#) ou [list-multicast-groups](#)
- [DeleteMulticastGroup](#) ou [delete-multicast-group](#)

### 2. Adicione dispositivos a um grupo de multicast

É possível adicionar dispositivos ao seu grupo de multicast individualmente ou em lotes.

- Para adicionar dispositivos em lotes ao seu grupo de multicast, use a operação de API [StartBulkAssociateWirelessDeviceWithMulticastGroup](#) ou o comando [start-](#)

[bulk-associate-wireless-device-with-multicast-group](#) da CLI. Para filtrar os dispositivos que você deseja associar em lote ao seu grupo de multicast, forneça uma string de consulta. O seguinte demonstra como você pode adicionar um grupo de dispositivos que tenha um perfil de dispositivo com o ID especificado vinculado a ele.

```
aws iotwireless start-bulk-associate-wireless-device-with-multicast-group \  
  --id "12abd34e-5f67-89c2-9293-593b1bd862e0" \  
  --cli-input-json file://input.json
```

onde:

Conteúdo de input.json

```
{  
  "QueryString": "DeviceProfileName: MyWirelessDevice AND DeviceProfileId:  
d6d8ef8e-7045-496d-b3f4-ebcaa1d564bf",  
  "Tags": [  
    {  
      "Key": "Multicast",  
      "Value": "ClassB"  
    }  
  ]  
}
```


Aqui, `multicast-groups/d6d8ef8e-7045-496d-b3f4-ebcaa1d564bf/bulk` é o URL usado para associar dispositivos ao grupo.

- Para adicionar dispositivos individualmente ao seu grupo de multicast, use a operação de API [AssociateWirelessDeviceWithMulticastGroup](#) ou o comando da CLI [associate-wireless-device-with-multicast-group](#). Forneça o ID do dispositivo sem fio de todos os dispositivos que você deseja adicionar ao grupo.

```
aws iotwireless associate-wireless-device-with-multicast-group \  
  --id "12abd34e-5f67-89c2-9293-593b1bd862e0" \  
  --wireless-device-id "ab0c23d3-b001-45ef-6a01-2bc3de4f5333"
```

Após criar seu grupo de multicast, é possível usar as seguintes operações de API ou comandos da CLI para obter informações sobre seu grupo de multicast ou para desassociar dispositivos.

- [DisassociateWirelessDeviceFromMulticastGroup](#) ou [disassociate-wireless-device-from-multicast-group](#)
- [StartBulkDisassociateWirelessDeviceFromMulticastGroup](#) ou [start-bulk-disassociate-wireless-device-from-multicast-group](#)
- [ListWirelessDevices](#) ou [list-wireless-devices](#)

 Note

A operação de API `ListWirelessDevices` pode ser usada para listar dispositivos sem fio em geral e dispositivos sem fio que estejam associados a um grupo de multicast ou a uma tarefa FUOTA.

- Para listar dispositivos sem fio que estão associados a um grupo de multicast, use a operação de API `ListWirelessDevices` com `MulticastGroupID` como filtro.
- Para listar dispositivos sem fio que estão associados a uma tarefa FUOTA, use a operação de API `ListWirelessDevices` com `FuotaTaskID` como filtro.

## Próximas etapas

Após criar um grupo de multicast e adicionar dispositivos, é possível seguir adicionando dispositivos e monitorar o status do grupo de multicast e de seus dispositivos. Se os dispositivos foram adicionados com êxito ao grupo, é possível configurar e programar uma mensagem de downlink para ser enviada a eles. Antes de poder enviar uma mensagem de downlink, o status dos dispositivos deve ser Pronto para configuração do Multicast. Depois que você agenda uma mensagem de downlink, o status é alterado para Tentativa de sessão. Para ter mais informações, consulte [Agendar uma mensagem de downlink para enviar para os dispositivos de um grupo de multicast](#).

Se quiser atualizar o firmware dos dispositivos do grupo do multicast, é possível realizar atualizações de firmware sem fio (FUOTA) com o AWS IoT Core for LoRaWAN. Para ter mais informações, consulte [Atualização de firmware sem fios \(FUOTA\) para dispositivos do AWS IoT Core for LoRaWAN](#).

Se os dispositivos não foram adicionados, ou se você recebeu um erro no grupo de multicast ou nos status do dispositivo, passe o mouse sobre o erro para obter mais informações e resolvê-lo. Se você ainda receber um erro, para obter informações sobre como solucionar o problema, consulte [Monitorar e solucionar problemas do status de um grupo de multicast e dos dispositivos do grupo](#).

## Monitorar e solucionar problemas do status de um grupo de multicast e dos dispositivos do grupo

Depois que você adicionar dispositivos e criar seu grupo de multicast, abra o Console de gerenciamento da AWS. Navegue até a página [Grupos de multicast](#) do console do AWS IoT e selecione o grupo de multicast que você criou para visualizar seus detalhes. Você verá informações sobre o grupo de multicast, o número de dispositivos adicionados e os detalhes de status dos dispositivos. É possível usar as informações de status para monitorar o progresso da sua sessão multicast e solucionar quaisquer erros.

### Status do grupo de multicast

Seu grupo de multicast pode ter uma das mensagens de status a seguir exibidas no Console de gerenciamento da AWS.

- Pendente

Esse status indica que um grupo de multicast foi criado por você, mas ele ainda não tem uma sessão multicast. Essa mensagem de status será exibida quando um grupo for criado. Durante esse período, é possível atualizar seu grupo de multicast e associar ou desassociar dispositivos ao grupo. Após o status mudar de Pendente, dispositivos adicionais não poderão ser adicionados no grupo.

- Tentativa de sessão

Depois que os dispositivos forem adicionados com êxito ao grupo de multicast, quando o grupo tiver uma sessão multicast agendada, essa mensagem de status será exibida. Durante esse período, não é possível atualizar ou adicionar dispositivos no grupo de multicast. Se cancelar sua sessão multicast, o status do grupo será alterado para Pendente.

- Em sessão

Quando for a primeira sessão da sua sessão multicast, essa mensagem de status será exibida. Um grupo de multicast também permanece nesse estado quando está associado a uma tarefa FUOTA que possui uma sessão contínua de atualização de firmware.

Caso não haja uma tarefa FUOTA associada na sessão e se a sessão multicast for cancelada porque o tempo da sessão excedeu o tempo limite ou porque você cancelou a sessão multicast, o status do grupo será alterado para Pendente.

- Espera de exclusão

Se você excluir um grupo de multicast, o status do grupo será alterado para Espera de exclusão. As exclusões são permanentes e irreversíveis. Essa ação pode levar tempo e o status do grupo será Delete\_Waiting até o grupo de multicast ser excluído. Depois que um grupo de multicast entrar nesse estado, ele não poderá mudar para um dos outros estados.

## Status dos dispositivos no grupo de multicast

Os dispositivos de um grupo de multicast pode ter uma das mensagens de status a seguir exibidas no Console de gerenciamento da AWS. É possível passar o mouse sobre cada mensagem de status para acessar mais informações sobre o que ela indica.

- Tentativa de pacote

Após os dispositivos terem sido associados ao grupo de multicast, o status do dispositivo será Tentativa de pacote. Esse status indica que o AWS IoT Core for LoRaWAN ainda não confirmou se o dispositivo é compatível com a configuração e operação do multicast.

- Pacote incompatível

Após os dispositivos terem sido associados ao grupo de multicast, o AWS IoT Core for LoRaWAN verifica se o firmware do dispositivo é capaz de configurar e operar o multicast. Se o dispositivo não possuir o pacote compatível do multicast, seu status será Pacote incompatível. Para solucionar o erro, verifique se o firmware do dispositivo pode configurar e operar o multicast.

- Tentativa de configuração do multicast

Se os dispositivos associados ao seu grupo de multicast forem capazes de configurar e operar o multicast, o status será Tentativa de configuração do multicast. Esse status representa que o dispositivo ainda não concluiu a configuração do multicast.

- Configuração do multicast concluída

O dispositivo concluiu a configuração do multicast e foi adicionado ao grupo de multicast. Esse status representa que os dispositivos estão prontos para uma sessão multicast e que mensagens de downlink pode ser enviada para esses dispositivos. O status também indica quando é possível usar o FUOTA para atualizar o firmware dos dispositivos do grupo.

- Tentativa de sessão

Uma sessão multicast foi agendada para os dispositivos no grupo de multicast. No início de uma sessão de grupo de multicast, o status do dispositivo é Tentativa de sessão, e as solicitações são

enviadas para uma janela de distribuição de classe B ou classe C ser iniciada para a sessão. Se o tempo decorrida na configuração da sessão multicast exceder o tempo limite ou se você cancelar a sessão multicast, o status será alterado para Configuração do multicast concluída.

- Em sessão

Esse status representa que uma janela de distribuição de classe B ou classe C foi iniciada e que o dispositivo tem uma sessão multicast em andamento. Durante esse período, mensagens de downlink podem ser enviadas a partir do AWS IoT Core for LoRaWAN para dispositivos no grupo de multicast. Se você atualizar o horário da sessão, ele substituirá a sessão atual e o status será alterado para Tentativa de sessão. Quando o horário da sessão se encerra, ou ao cancelar a sessão multicast, o status é alterado para Configuração do multicast concluída.

## Próximas etapas

Agora que você aprendeu os diferentes status de um grupo de multicast e dos dispositivos do grupo e como solucionar quaisquer problemas, como quando um dispositivo não é capaz de configurar o multicast, você pode agendar o envio de uma mensagem de downlink aos dispositivos e o grupo de multicast estará Em sessão. Para acessar informações sobre agendamento de mensagens de downlink, consulte [Agendar uma mensagem de downlink para enviar para os dispositivos de um grupo de multicast](#).

## Agendar uma mensagem de downlink para enviar para os dispositivos de um grupo de multicast

Após adicionar dispositivos com sucesso a um grupo de multicast, é possível iniciar uma sessão multicast e configurar uma mensagem de downlink para ser enviada a esses dispositivos. A mensagem de downlink deve ser agendada dentro de 48 horas e a hora de início do multicast deve ser pelo menos 30 minutos adiante da hora presente.

### Note

Os dispositivos de um grupo de multicast não conseguem reconhecer quando uma mensagem de downlink foi recebida.

## Pré-requisitos

Antes de enviar uma mensagem de downlink, é preciso ter criado um grupo de multicast e adicionado com sucesso dispositivos ao grupo para o qual você deseja enviar uma mensagem de downlink. Não é possível adicionar mais dispositivos depois de um horário de início ter sido agendado para a sessão multicast. Para ter mais informações, consulte [Criar grupos de multicast e adicionar dispositivos ao grupo](#).

Se algum dos dispositivos não tiver sido adicionado com sucesso, o grupo de multicast e o status do dispositivo conterão informações para ajudá-lo a solucionar os erros. Se os erros persistirem, para acessar informações sobre como solucioná-los, consulte [Monitorar e solucionar problemas do status de um grupo de multicast e dos dispositivos do grupo](#).

Agendar uma mensagem de downlink com o console

Para enviar uma mensagem de downlink com o console, acesse a página [Grupos de multicast](#) do console do AWS IoT e selecione o grupo de multicast que você criou. Na página de detalhes do grupo de multicast, selecione Agendar mensagem de downlink e, depois, selecione Agendar sessão de downlink.

### 1. Agendar janela de mensagem de downlink

É possível configurar uma janela de tempo para que uma mensagem de downlink seja enviada aos dispositivos de um grupo de multicast. É preciso que a mensagem de downlink seja agendada em 48 horas.

Para agendar uma sessão multicast, especifique os parâmetros a seguir:

- Data de início e Hora de início: a data e a hora de início devem ser pelo menos 30 minutos depois e 48 horas antes da hora presente.

#### Note

A hora a ser especificada estará em UTC, então considere verificar a diferença de horário pelo fuso horário ao agendar a janela de downlink.

- Tempo limite da sessão: o tempo após o qual você quer que a sessão multicast atinja o tempo limite se nenhuma mensagem de downlink for recebida. O tempo limite mínimo permitido é de 60 segundos. O valor máximo de tempo limite é de 2 dias para grupos de multicast de classe B e 18 horas para grupos de multicast de classe C.

## 2. Configurar uma mensagem de downlink

Para configurar uma mensagem de downlink, especifique os parâmetros a seguir:

- **Taxa de dados:** selecione uma taxa de dados para a mensagem de downlink. A taxa de dados depende da RfRegion e do tamanho da carga. A taxa de dados padrão é 8 para a região US915 e 0 para a região UE868.
- **Frequência:** selecione uma frequência para envio da mensagem de downlink. Para evitar conflitos de mensagens, selecione uma frequência disponível conforme a RfRegion.
- **FPort:** selecione uma porta de frequência disponível para envio da mensagem de downlink para os seus dispositivos.
- **Carga:** especifique o tamanho máximo da carga conforme a taxa de dados. Usando a taxa de dados padrão, pode-se ter um tamanho máximo de carga de 33 bytes na RfRegion US915 e 51 bytes na RfRegion UE868. Com taxas de dados maiores, é possível transferir até um tamanho máximo de carga de 242 bytes.

Para agendar uma mensagem de downlink, selecione Agendar.

### Agendar uma mensagem de downlink com a API

Para agendar uma mensagem de downlink com a API, use a operação de API

[StartMulticastGroupSession](#) ou o comando [start-multicast-group-session](#) da CLI.

É possível utilizar as operações de API ou comandos da CLI a seguir para obter informações sobre um grupo multicast e para excluí-lo.

- [GetMulticastGroupSession](#) ou [get-multicast-group-session](#)
- [DeleteMulticastGroupSession](#) ou [delete-multicast-group-session](#)

Para enviar dados a um grupo de multicast depois do início da sessão, use a operação de API

[SendDataToMulticastGroup](#) ou o comando [send-data-to-multicast-group](#) da CLI.

### Próximas etapas

Após configurar uma mensagem de downlink a ser enviada para os dispositivos, a mensagem será enviada no início da sessão. Os dispositivos de um grupo de multicast não podem confirmar o recebimento da mensagem.

## Configurar mensagens de downlink adicionais

Também é possível configurar mensagens de downlink adicionais a serem enviadas para os dispositivos de um grupo de multicast:

- Para configurar mensagens de downlink adicionais a partir do console:
  1. Acesse a página [Grupos de multicast](#) do console do AWS IoT e selecione o grupo de multicast que você criou.
  2. Na página de detalhes do grupo de multicast, selecione Agendar mensagem de downlink e, depois, selecione Configurar mensagem de downlink adicional.
  3. Especifique os parâmetros Taxa de dados, Frequência, FPort e Carga, da mesma forma como configurou esses parâmetros para a primeira mensagem de downlink.
- Para configurar mensagens de downlink adicionais com a API ou a CLI, chame a operação de API [SendDataToMulticastGroup](#) ou o comando [send-data-to-multicast-group](#) da CLI para cada mensagem de downlink adicional.

## Atualizar o agendamento da sessão

Também é possível atualizar o agendamento da sessão para utilizar uma nova data e hora de início para a sua sessão multicast. O novo agendamento da sessão substituirá a sessão agendada anteriormente.

### Note

Só atualize sua sessão multicast quando for necessário. Essas atualizações podem fazer com que um grupo de dispositivos seja ativado por um longo período, esgotando suas baterias.

- Para atualizar o agendamento da sessão a partir do console:
  1. Acesse a página [Grupos de multicast](#) do console do AWS IoT e selecione o grupo de multicast que você criou.
  2. Na página de detalhes do grupo de multicast, selecione Agendar mensagem de downlink e, depois, selecione Atualizar agendamento de sessão.
  3. Especifique os parâmetros Data do estado, Hora de início e Tempo limite da sessão, da mesma forma como especificou esses parâmetros para a primeira mensagem de downlink.

- Para atualizar o agendamento da sessão a partir da API ou da CLI, use a operação de API [StartMulticastGroupSession](#) ou o comando [start-multicast-group-session](#) da CLI.

## Atualização de firmware sem fios (FUOTA) para dispositivos do AWS IoT Core for LoRaWAN

Use atualizações de firmware sem fio (FUOTA) para implantar atualizações de firmware em dispositivos do AWS IoT Core for LoRaWAN.

Com o FUOTA, é possível enviar atualizações de firmware para dispositivos individuais ou para um grupo de dispositivos. Também é possível enviar atualizações de firmware para vários dispositivos criando um grupo de multicast. Primeiro, adicione os dispositivos ao grupo de multicast e, depois, envie a imagem de atualização de firmware para todos esses dispositivos. Recomendamos assinar digitalmente as imagens de firmware para que os dispositivos que recebem as imagens possam verificar se elas vêm da origem correta.

Com o FUOTA do AWS IoT Core for LoRaWAN, é possível:

- Implantar novas imagens de firmware ou imagens delta em um único dispositivo ou em um grupo de dispositivos.
- Verificar a autenticidade e a integridade do novo firmware depois de implantá-lo nos dispositivos.
- Monitorar o progresso de uma implantação e depurar problemas em caso de falha na implantação.

A compatibilidade do AWS IoT Core for LoRaWAN com o FUOTA e grupos de multicast é baseada nas seguintes especificações da [LoRa Alliance](#):

- LoRaWAN Remote Multicast Setup Specification, TS005-2.0.0
- LoRaWAN Fragmented Data Block Transportation Specification, TS004-2.0.0
- LoRaWAN Application Layer Clock Synchronization Specification, TS003-2.0.0

### Note

O AWS IoT Core for LoRaWAN executa automaticamente a sincronização de relógio em conformidade com a especificação da LoRa Alliance. Ele usa a função `AppTimeReq`

para responder a hora do servidor aos dispositivos que a solicitam usando a sinalização ClockSync.

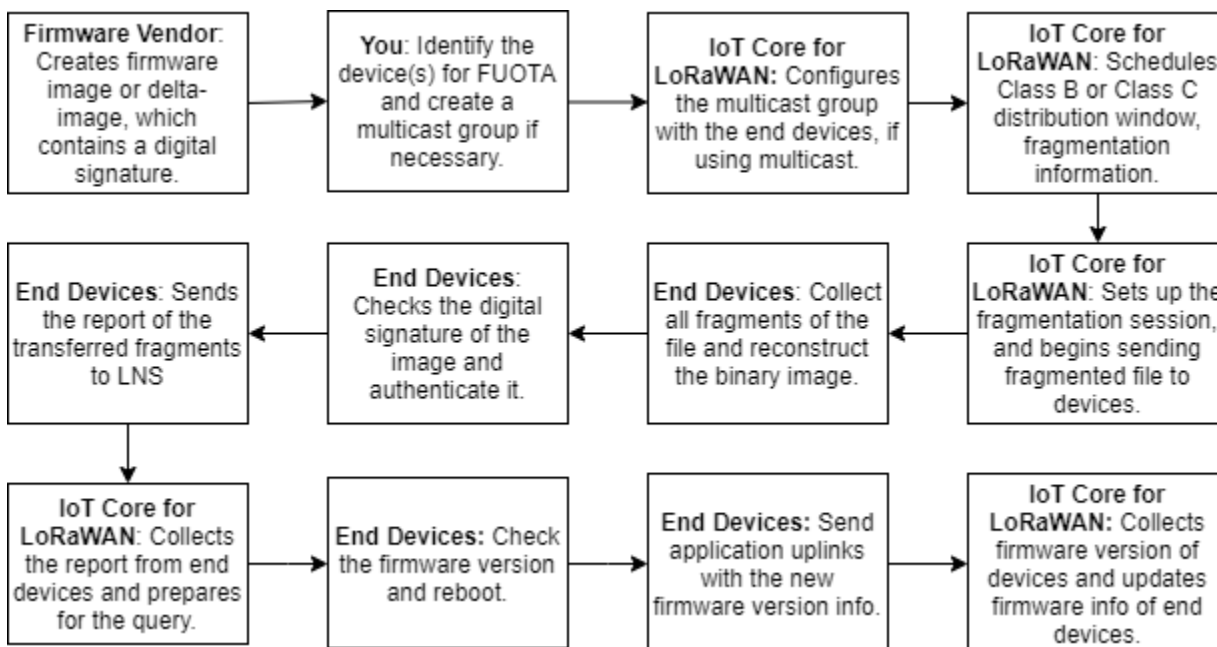
O vídeo a seguir descreve como as tarefas de FUOTA do AWS IoT Core for LoRaWAN podem ser criadas e fornece orientações sobre o processo de adição de dispositivos à tarefa e a programação de uma tarefa FUOTA.

Os tópicos a seguir mostram como executar o FUOTA.

- [Visão geral do processo FUOTA](#)
- [Criar uma tarefa FUOTA e fornecer a imagem de firmware](#)
- [Adicionar dispositivos e grupos de multicast a uma tarefa FUOTA e agendar uma sessão FUOTA](#)
- [Monitorar e solucionar problemas do status de uma tarefa FUOTA e dos dispositivos adicionados à tarefa](#)

## Visão geral do processo FUOTA

O seguinte diagrama exibe como o AWS IoT Core for LoRaWAN executa o processo FUOTA para os dispositivos finais. Se estiver adicionando dispositivos individuais à sua sessão FUOTA, você pode pular as etapas de criação e configuração de um grupo de multicast. É possível adicionar dispositivos diretamente a uma sessão FUOTA e, em seguida, o AWS IoT Core for LoRaWAN iniciará o processo de atualização de firmware.




Para executar o FUOTA nos dispositivos, primeiramente crie uma imagem de firmware assinada digitalmente e configure os dispositivos e grupos multicast a serem adicionados à tarefa FUOTA. Após iniciar uma sessão FUOTA, os dispositivos finais coletam todos os fragmentos, reconstróem a imagem a partir dos fragmentos, reportam o status ao AWS IoT Core for LoRaWAN e aplicam a nova imagem de firmware.

O seguinte demonstra as diferentes etapas do processo FUOTA:

1. Crie uma imagem de firmware ou imagem delta com uma assinatura digital

Para que o AWS IoT Core for LoRaWAN execute o FUOTA nos dispositivos LoRaWAN, é recomendável assinar digitalmente a imagem de firmware ou a imagem delta ao enviar atualizações de firmware sem fios. Os dispositivos que recebem as imagens podem, então, verificar se elas vêm da origem correta.

Sua imagem de firmware não deve ter tamanho superior a 1 megabyte. Quanto maior o tamanho do firmware, mais tempo levará para que o processo de atualização seja concluído. Para realizar uma transferência de dados mais rápida, ou se a nova imagem for maior que 1 megabyte, use uma imagem delta, que é a parte da nova imagem que é o delta entre a nova imagem de firmware e a imagem anterior.

 Note

O AWS IoT Core for LoRaWAN não oferece a ferramenta de geração de assinatura digital e o sistema de gerenciamento de versão de firmware. É possível usar qualquer ferramenta de terceiros para gerar a assinatura digital para a sua imagem de firmware. Nós recomendamos usar uma ferramenta de assinatura digital, como a incorporada no [repositório ARM Mbed do GitHub](#), que também inclui ferramentas para gerar a imagem delta e para dispositivos usarem essa imagem.

2. Identifique e configure os dispositivos para o FUOTA

Após identificar os dispositivos para o FUOTA, envie atualizações de firmware para dispositivos individuais ou para vários dispositivos.

- Para enviar atualizações de firmware para vários dispositivos, crie um grupo de multicast e configure o grupo de multicast com dispositivos finais. Para ter mais informações, consulte [Crie grupos de multicast para enviar uma carga de downlink para vários dispositivos](#).

- Para enviar atualizações de firmware para dispositivos individuais, adicione esses dispositivos à sua sessão FUOTA e, depois, execute a atualização de firmware.

### 3. Agende uma janela de distribuição e configure a sessão de fragmentação

Se você criou um grupo de multicast, é possível especificar a janela de distribuição de classe B ou classe C para determinar quando os dispositivos podem receber os fragmentos do AWS IoT Core for LoRaWAN. Os dispositivos podem estar operando na classe A antes de migrarem para o modo classe B ou classe C. Também é preciso especificar a hora de início da sessão.

Os dispositivos de classe B ou classe C são ativados na janela de distribuição especificada e passam a receber os pacotes de downlink. Dispositivos que operam no modo classe C podem consumir mais energia do que dispositivos da classe B. Para ter mais informações, consulte [Classes de dispositivos](#).

### 4. Os dispositivos finais relatam o status ao AWS IoT Core for LoRaWAN e atualizam a imagem de firmware

Depois que você configurar uma sessão de fragmentação, os dispositivos finais e o AWS IoT Core for LoRaWAN executam as etapas a seguir para atualizar o firmware dos dispositivos.

1. Como os dispositivos LoRaWAN têm uma baixa taxa de dados, para iniciar o processo FUOTA, o AWS IoT Core for LoRaWAN configura uma sessão de fragmentação para fragmentar a imagem de firmware. Depois, ele envia esses fragmentos aos dispositivos finais.
2. Depois que o AWS IoT Core for LoRaWAN enviar os fragmentos da imagem, os dispositivos finais LoRaWAN executam as seguintes tarefas.
  - a. Coleta dos fragmentos e reconstrução da imagem binária a partir desses fragmentos.
  - b. Verificação da assinatura digital da imagem reconstruída para autenticar a imagem e verificar se ela vem da origem correta.
  - c. Comparação da versão de firmware do AWS IoT Core for LoRaWAN com a versão atual.
  - d. Comunicação sobre o status das imagens fragmentadas que foram transferidas ao AWS IoT Core for LoRaWAN e, depois, aplicação da nova imagem de firmware.

#### Note

Em alguns casos, os dispositivos finais relatam o status das imagens fragmentadas que foram transferidas para o AWS IoT Core for LoRaWAN antes de verificar a assinatura digital da imagem de firmware.

Agora que você aprendeu sobre o processo FUOTA, você pode criar sua tarefa FUOTA e adicionar dispositivos à tarefa para atualizar o firmware. Para ter mais informações, consulte [Criar uma tarefa FUOTA e fornecer a imagem de firmware](#).

## Criar uma tarefa FUOTA e fornecer a imagem de firmware

Para atualizar o firmware de dispositivos LoRaWAN, primeiro crie uma tarefa FUOTA e forneça a imagem de firmware assinada digitalmente que deseja usar na atualização. Em seguida, você poderá adicionar os dispositivos e grupos de multicast à tarefa e agendar uma sessão FUOTA. Quando a sessão começa, o AWS IoT Core for LoRaWAN configura uma sessão de fragmentação e os dispositivos finais coletam os fragmentos, reconstroem a imagem e aplicam o novo firmware. Para acessar informações sobre o processo FUOTA, consulte [Visão geral do processo FUOTA](#).

O seguinte demonstra como você pode criar uma tarefa FUOTA e carregar a imagem de firmware ou a imagem delta que você armazenará em um bucket do S3.

### Pré-requisitos

Para poder executar a FUOTA, a imagem de firmware deve estar assinada digitalmente para que os dispositivos finais possam verificar a autenticidade da imagem ao aplicá-la. É possível usar qualquer ferramenta de terceiros para gerar a assinatura digital para a sua imagem de firmware. Nós recomendamos usar uma ferramenta de assinatura digital, como a incorporada no [repositório ARM Mbed do GitHub](#), que também inclui ferramentas para gerar a imagem delta e para dispositivos usarem essa imagem.

### Criar tarefa FUOTA e carregar a imagem de firmware com o console

Para criar uma tarefa FUOTA e carregar sua imagem de firmware com o console, acesse a guia [Tarefas FUOTA](#) do console e, em seguida, selecione Criar tarefa FUOTA.

#### 1. Criar tarefa FUOTA

Para criar uma tarefa FUOTA, especifique as propriedades e tags da tarefa.

##### 1. Especificar propriedades da tarefa FUOTA

Para especificar as propriedades da tarefa FUOTA, insira as informações a seguir relativas à tarefa FUOTA.

- Nome: informe um nome exclusivo para a tarefa FUOTA. O nome só pode conter letras, números, hifens e sublinhado. Ele não pode conter espaços.

- **Descrição:** você pode fornecer uma descrição opcional do grupo de multicast. O campo de descrição pode ter até 2.048 caracteres.
- **RFRegion:** defina a banda de frequência da tarefa FUOTA. A banda de frequência deve corresponder àquela usada para provisionar seus dispositivos sem fio ou grupos de multicast.

## 2. Tags da tarefa FUOTA

Opcionalmente, é possível fornecer quaisquer pares de valores-chave como Tags para a tarefa FUOTA. Para continuar a criação da tarefa, selecione Próximo.

## 2. Carregar imagem de firmware

Selecione o arquivo de imagem de firmware que deseja usar para atualizar o firmware dos dispositivos adicionados à tarefa FUOTA. O arquivo de imagem de firmware é armazenado em um bucket do S3. Você pode fornecer ao AWS IoT Core for LoRaWAN as permissões para acessar a imagem de firmware em seu nome. Nós recomendamos assinar digitalmente as imagens de firmware para que sua autenticidade seja verificada quando a atualização do firmware for realizada.

### 1. Selecione o arquivo de imagem de firmware

É possível carregar um novo arquivo de imagem de firmware em um bucket do S3 ou selecionar uma imagem existente que já tenha sido carregada em um bucket do S3.

#### Note

O arquivo de imagem de firmware não deve ter tamanho superior a 1 megabyte. Quanto maior o tamanho do firmware, mais tempo levará para que o processo de atualização seja concluído.

- Para usar uma imagem existente, selecione Selecionar uma imagem de firmware existente, selecione Procurar no S3 e selecione o arquivo de imagem de firmware que deseja usar.

O AWS IoT Core for LoRaWAN preenche o URL do S3, que é o caminho para o arquivo de imagem de firmware no bucket do S3. O formato do caminho é `s3://bucket_name/file_name`. Para visualizar o arquivo no console do [Amazon Simple Storage Service](#), selecione Exibir.

- Para carregar uma nova imagem de firmware.
  - a. Selecione Carregar uma nova imagem de firmware e carregue a imagem de firmware. O arquivo de imagem não deve ser maior que 1 megabyte.
  - b. Para criar um bucket do S3 e inserir um Nome do bucket para armazenamento do arquivo de imagem de firmware, selecione Criar bucket do S3.

## 2. Permissões de acesso ao bucket

É possível criar um novo perfil de serviço ou selecionar um perfil existente para permitir que o AWS IoT Core for LoRaWAN acesse o arquivo de imagem de firmware no bucket do S3 em seu nome. Escolha Próximo.

Para criar um novo perfil, informe um nome de perfil ou deixe em branco para que um nome aleatório seja gerado automaticamente. Para visualizar as permissões de política que concedem acesso ao bucket do S3, selecione Exibir permissões de política.

Para acessar mais informações sobre como usar um bucket do S3 para armazenar sua imagem e conceder ao AWS IoT Core for LoRaWAN as permissões para acessá-la, consulte [Fazer upload do arquivo de firmware para um bucket do S3 e adicionar um perfil do IAM](#).

## 3. Examinar e criar

Para criar uma tarefa FUOTA, examine a tarefa FUOTA e os detalhes de configuração especificados e, em seguida, selecione Criar tarefa.

Criar tarefa FUOTA e carregar a imagem de firmware com a API

Para criar uma tarefa FUOTA e especificar seu arquivo de imagem de firmware com a API, use a operação da API [CreateFuotaTask](#) ou o comando [create-fuota-task](#) da CLI. É possível fornecer um arquivo `input.json` como entrada para o comando `create-fuota-task`. Quando usar a API ou a CLI, é preciso que o arquivo de imagem de firmware fornecido como entrada já esteja carregado em um bucket do S3. Você também especifica o perfil do IAM que dá ao AWS IoT Core for LoRaWAN acesso à imagem de firmware no bucket do S3.

```
aws iotwireless create-fuota-task \  
  --cli-input-json file://input.json
```

onde:

## Conteúdo de input.json

```
{
  "Description": "FUOTA task to update firmware of devices in multicast group.",
  "FirmwareUpdateImage": "S3:/firmware_bucket/firmware_image
  "FirmwareUpdateRole": "arn:aws:iam::123456789012:role/service-role/ACF1zBEI"
  "LoRaWAN": {
    "RfRegion": "US915"
  },
  "Name": "FUOTA_Task_MC"
}
```

Após criar sua tarefa FUOTA, é possível usar as seguintes operações de API ou comandos da CLI para atualizar, excluir ou obter informações sobre sua tarefa FUOTA.

- [UpdateFuotaTask](#) ou [update-fuota-task](#)
- [GetFuotaTask](#) ou [get-fuota-task](#)
- [ListFuotaTasks](#) ou [list-fuota-tasks](#)
- [DeleteFuotaTask](#) ou [delete-fuota-task](#)

## Próximas etapas

Depois de ter criado uma tarefa FUOTA e fornecido a imagem de firmware, você pode adicionar dispositivos à tarefa para atualizar o firmware. É possível adicionar dispositivos individuais ou grupos de multicast à tarefa. Para ter mais informações, consulte [Adicionar dispositivos e grupos de multicast a uma tarefa FUOTA e agendar uma sessão FUOTA](#).

## Adicionar dispositivos e grupos de multicast a uma tarefa FUOTA e agendar uma sessão FUOTA

Depois de ter criado uma tarefa FUOTA, você pode adicionar dispositivos à tarefa para atualizar o firmware. Depois que os dispositivos forem adicionados com êxito à tarefa FUOTA, você poderá agendar uma sessão FUOTA para atualizar o firmware do dispositivo.

- Se você tiver um número pequeno de dispositivos, poderá adicioná-los diretamente à tarefa FUOTA.
- Se você tiver um número grande de dispositivos para os quais quer atualizar o firmware, é possível adicionar esses dispositivos aos seus grupos de multicast e, depois, adicionar os grupos de

multicast à tarefa FUOTA. Para acessar informações sobre a criação e uso de grupos de multicast, consulte [Crie grupos de multicast para enviar uma carga de download para vários dispositivos](#).

#### Note

É possível adicionar dispositivos individuais ou grupos de multicast à tarefa FUOTA. Não é possível adicionar dispositivos e grupos de multicast à tarefa.

Depois que tiver adicionado os dispositivos ou grupos de multicast, você poderá iniciar uma sessão de atualização de firmware. O AWS IoT Core for LoRaWAN coleta a imagem de firmware, fragmenta as imagens e, depois, armazena os fragmentos em um formato criptografado. Os dispositivos finais coletam os fragmentos e aplicam a nova imagem de firmware. O tempo que leva para a atualização de firmware ser concluída depende do tamanho da imagem e de como as imagens foram fragmentadas. Quando a atualização de firmware for concluída, os fragmentos criptografados da imagem de firmware armazenados pelo AWS IoT Core for LoRaWAN serão excluídos. Você ainda poderá encontrar a imagem de firmware no bucket do S3.

#### Pré-requisitos

Antes de adicionar dispositivos ou grupos de multicast à tarefa FUOTA, realize o seguinte.

- Você já precisa ter criado a tarefa FUOTA e fornecido a imagem de firmware. Para ter mais informações, consulte [Criar uma tarefa FUOTA e fornecer a imagem de firmware](#).
- Forneça os dispositivos sem fio para os quais você deseja atualizar o firmware. Para acessar informações sobre integrar seu dispositivo, consulte [Integrar os dispositivos ao AWS IoT Core for LoRaWAN](#).
- Para atualizar o firmware de vários dispositivos, é possível adicioná-los a um grupo de multicast. Para ter mais informações, consulte [Crie grupos de multicast para enviar uma carga de download para vários dispositivos](#).
- Quando você integrar os dispositivos ao AWS IoT Core for LoRaWAN, especifique o parâmetro de configuração FUOTA `FPorts`. Se estiver usando um dispositivo LoRaWAN v1.0.x, também é preciso especificar a `GenAppKey`. Para obter mais informações sobre os parâmetros de configuração do FUOTA, consulte [Preparar dispositivos para configuração multicast e FUOTA](#).

## Adicionar dispositivos a uma tarefa FUOTA e agendar uma sessão FUOTA com o console

Para adicionar dispositivos ou grupos de multicast e agendar uma sessão FUOTA com o console, acesse a guia [Tarefas FUOTA](#) do console. Depois, selecione a tarefa FUOTA à qual deseja adicionar dispositivos e execute a atualização de firmware.

### Adicionar dispositivos e grupos de multicast

1. É possível adicionar dispositivos individuais ou grupos de multicast à sua tarefa FUOTA. Entretanto, não é possível adicionar dispositivos individuais e grupos de multicast à mesma tarefa FUOTA. Para adicionar dispositivos com o console, faça o seguinte.
  1. Nos Detalhes da tarefa FUOTA, selecione Adicionar dispositivo.
  2. Selecione a banda de frequência ou a RFRegion dos dispositivos adicionados à tarefa. Esse valor deve corresponder à RFRegion escolhida para a tarefa FUOTA.
  3. Escolha se deseja adicionar dispositivos individuais ou grupos de multicast à tarefa.
    - Para adicionar dispositivos individuais, selecione Adicionar dispositivos individuais e informe o ID do dispositivo de cada dispositivo que deseja adicionar à tarefa FUOTA.
    - Para adicionar grupos de multicast, selecione Adicionar grupos de multicast e adicione os grupos de multicast à tarefa. É possível filtrar os grupos de multicast que você deseja adicionar à tarefa usando o perfil ou as tags do dispositivo. Ao filtrar por perfil de dispositivo, é possível escolher grupos de multicast com dispositivos que tenham um perfil com Compatível com Classe B ou Compatível com Classe C habilitado.
2. Agendar uma sessão FUOTA

Depois que seus dispositivos ou grupos de multicast forem adicionados com êxito, você poderá agendar uma sessão FUOTA. Para agendar uma sessão, realize o seguinte.

1. Selecione a tarefa FUOTA para a qual você deseja atualizar o firmware do dispositivo e, depois, selecione Agendar sessão FUOTA.
2. Especifique uma Data de início e uma Hora de início para a sessão FUOTA. Certifique-se de que a hora de início esteja 30 minutos ou mais à frente do horário presente.

### Adicionar dispositivos a uma tarefa FUOTA e agendar uma sessão FUOTA com a API

É possível usar a API do AWS IoT Wireless ou a CLI para adicionar dispositivos sem fio ou grupos de multicast à sua tarefa FUOTA. Depois, você pode agendar uma sessão FUOTA.

## 1. Adicionar dispositivos e grupos de multicast

É possível associar dispositivos sem fio ou grupos de multicast a uma tarefa FUOTA.

- Para associar dispositivos individuais a uma tarefa FUOTA, use a operação de API [AssociateWirelessDeviceWithFuotaTask](#) ou o comando [associate-wireless-device-with-fuota-task](#) da CLI e forneça o `WirelessDeviceID` como entrada.

```
aws iotwireless associate-wireless-device-with-fuota-task \  
  --id "01a23cde-5678-4a5b-ab1d-33456808ecb2" \  
  --wireless-device-id "ab0c23d3-b001-45ef-6a01-2bc3de4f5333"
```

- Para associar grupos de multicast a uma tarefa FUOTA, use a operação de API [AssociateMulticastGroupWithFuotaTask](#) ou o comando [associate-multicast-group-with-fuota-task](#) da CLI e forneça o `MulticastGroupID` como entrada.

```
aws iotwireless associate-multicast-group-with-FUOTA-task \  
  --id 01a23cde-5678-4a5b-ab1d-33456808ecb2" \  
  --multicast-group-id
```

Após associar os dispositivos sem fio ou grupo de multicast a uma tarefa FUOTA, use as operações de API ou comandos de CLI a seguir para listar os dispositivos ou grupos de multicast ou para desassociá-los da tarefa.

- [DisassociateWirelessDeviceFromFuotaTask](#) ou [disassociate-wireless-device-from-fuota-task](#)
- [DisassociateMulticastGroupFromFuotaTask](#) ou [disassociate-multicast-group-from-fuota-task](#)
- [ListWirelessDevices](#) ou [list-wireless-devices](#)
- [ListMulticastGroups](#) ou [list-multicast-groups-by-fuota-task](#)

### Note

A API:

- `ListWirelessDevices` pode listar dispositivos sem fio em geral, e dispositivos associados a um grupo de multicast, quando `MulticastGroupID` é usado como

filtro. A API lista os dispositivos sem fio que estão associados a uma tarefa FUOTA quando o `FuotaTaskID` é usado como filtro.

- `ListMulticastGroups` pode listar grupos de multicast em geral, e grupos de multicast associados a uma tarefa FUOTA, quando o `FuotaTaskID` é usado como filtro.

## 2. Agendar uma sessão FUOTA

Depois que os dispositivos ou grupos de multicast forem adicionados com êxito à tarefa FUOTA, você poderá iniciar uma sessão FUOTA para atualizar o firmware do dispositivo. A nova hora de início do evento deve estar 30 minutos ou mais à frente do horário presente. Para agendar uma sessão FUOTA usando a API ou a CLI, use a operação de API [StartFuotaTask](#) ou o comando [start-fuota-task](#) da CLI.

Após iniciar uma sessão FUOTA, não será mais possível adicionar dispositivos ou grupos de multicast à tarefa. É possível obter informações sobre o status de uma sessão FUOTA usando a operação de API [GetFuotaTask](#) ou o comando [get-fuota-task](#) da CLI.

## Monitorar e solucionar problemas do status de uma tarefa FUOTA e dos dispositivos adicionados à tarefa

Após provisionar os dispositivos sem fio e criar um grupo de multicast que você queira usar, é possível iniciar uma sessão FUOTA realizando as seguintes etapas.

### Status da tarefa FUOTA

Sua tarefa FUOTA pode ter uma das mensagens de status a seguir exibidas no Console de gerenciamento da AWS.

- **Pendente**

Esse status indica que uma tarefa FUOTA foi criada por você, mas ela ainda não tem uma sessão de atualização de firmware. Essa mensagem de status será exibida quando uma tarefa for criada. Durante esse período, é possível atualizar sua tarefa FUOTA e associar ou desassociar dispositivos ou grupos de multicast à tarefa. Após o status mudar de Pendente, dispositivos adicionais não poderão ser adicionados à tarefa.

- **Sessão FUOTA em espera**

Após os dispositivos serem adicionados com êxito à tarefa FUOTA, quando a tarefa tiver uma sessão de atualização de firmware agendada, essa mensagem de status será exibida. Durante esse período, não é possível atualizar ou adicionar dispositivos à sessão FUOTA. Se você cancelar a sessão FUOTA, o status do grupo será alterado para Pendente.

- Em sessão FUOTA

Quando a sessão FUOTA começar, essa mensagem de status será exibida. A sessão de fragmentação terá início e os dispositivos finais coletarão os fragmentos, reconstruirão a imagem de firmware, compararão a nova versão do firmware com a versão original e aplicarão a nova imagem.

- FUOTA concluído

Após os dispositivos finais informarem o AWS IoT Core for LoRaWAN que a nova imagem de firmware foi aplicada, ou com a expiração da sessão, a sessão FUOTA será marcada como concluída e esse status será exibido.

Esse status também será exibido em qualquer um dos casos a seguir, portanto, verifique se a atualização de firmware foi aplicada corretamente aos dispositivos.

- Quando o status da tarefa FUOTA é Sessão FUOTA em espera e há um erro no bucket do S3, como o link para o arquivo de imagem no bucket do S3 estar incorreto ou o AWS IoT Core for LoRaWAN não ter permissões suficientes para acessar o arquivo no bucket.
- Quando o status da tarefa FUOTA é Sessão FUOTA em espera e há uma solicitação para iniciar uma sessão FUOTA, mas uma resposta não é recebida a partir dos dispositivos ou grupos de multicast na tarefa FUOTA.
- Quando o status da tarefa FUOTA é Em sessão FUOTA e os dispositivos ou grupos de multicast não enviaram nenhum fragmento por um determinado período de tempo, o que resulta em esgotamento do tempo limite da sessão.
- Espera de exclusão

Se você excluir uma tarefa FUOTA que está em algum dos outros estados, esse status será exibido. Uma ação de exclusão é permanente e não pode ser desfeita. Essa ação pode levar tempo e o status da tarefa será Espera de exclusão até a tarefa FUOTA ser excluída. Depois que uma tarefa FUOTA entrar nesse estado, ela não poderá mudar para um dos outros estados.

## Status de dispositivos em uma tarefa FUOTA

Os dispositivos em uma tarefa FUOTA podem ter uma das mensagens de status a seguir exibidas no Console de gerenciamento da AWS. É possível passar o mouse sobre cada mensagem de status para acessar mais informações sobre o que ela indica.

- Inicial

Quando for o horário de início da sessão FUOTA, o AWS IoT Core for LoRaWAN verifica se o dispositivo tem o pacote compatível para a atualização de firmware. Caso o dispositivo tenha o pacote compatível, a sessão FUOTA do dispositivo será iniciada. A imagem de firmware está fragmentada e os fragmentos são enviados para o dispositivo. Quando esse status é exibido, isso indica que a sessão FUOTA do dispositivo ainda não foi começado.

- Pacote incompatível

Caso o dispositivo não tenha o pacote FUOTA compatível, esse status será exibido. Se o pacote de atualização de firmware não for compatível, a sessão FUOTA do dispositivo não poderá ser iniciada. Para solucionar esse erro, verifique se o firmware do dispositivo pode receber atualizações de firmware usando o FUOTA.

- Algoritmo de fragmentação incompatível

No início da sessão FUOTA, o AWS IoT Core for LoRaWAN configura uma sessão de fragmentação para o dispositivo. Se esse status for exibido, o tipo de algoritmo de fragmentação usado não pode ser aplicado à atualização de firmware do dispositivo. O erro ocorre porque o dispositivo não tem o pacote FUOTA compatível. Para solucionar esse erro, verifique se o firmware do dispositivo pode receber atualizações de firmware usando o FUOTA.

- Não há memória suficiente

Após o AWS IoT Core for LoRaWAN enviar os fragmentos da imagem, os dispositivos finais coletam os fragmentos da imagem e reconstroem a imagem binária a partir desses fragmentos. Esse status é exibido quando o seu dispositivo não tem memória suficiente para juntar os fragmentos de entrada da imagem de firmware, o que pode resultar no encerramento prematuro da sessão de atualização de firmware. Para solucionar o erro, verifique se o hardware do dispositivo é capaz de receber essa atualização. Se o dispositivo não for capaz de receber essa atualização, use uma imagem delta para atualizar o firmware.

- Índice de fragmentação incompatível

O índice de fragmentação identifica uma das quatro sessões de fragmentação simultaneamente possíveis. Caso o dispositivo não seja compatível com o valor do índice de fragmentação indicado, esse status será exibido. Para solucionar esse erro, execute um ou mais dos seguintes procedimentos.

- Inicie uma tarefa FUOTA nova para o dispositivo.
  - Se o erro persistir, mude do modo unicast para o modo multicast.
  - Se o erro ainda não for resolvido, verifique o firmware do seu dispositivo.
- Erro de memória

Esse status indica que o dispositivo apresentou um erro de memória ao receber os fragmentos recebidos do AWS IoT Core for LoRaWAN. Se esse erro ocorrer, pode ser que o dispositivo não seja capaz de receber essa atualização. Para solucionar o erro, verifique se o hardware do dispositivo é capaz de receber essa atualização. Se preciso, utilize uma imagem delta para atualizar o firmware do dispositivo.

- Descritor incorreto

O dispositivo é incompatível com o descritor indicado. O descritor é um campo que descreve o arquivo a ser transportado na sessão de fragmentação. Se você receber esse erro, entre em contato com o [AWS Support Center](#).

- Repetição da contagem de sessão

Esse status indica que o dispositivo já usou essa contagem de sessões anteriormente. Para solucionar o erro, inicie uma nova tarefa FUOTA para o dispositivo.

- Fragmentos ausentes

Conforme o dispositivo coleta os fragmentos da imagem do AWS IoT Core for LoRaWAN, ele reconstrói a nova imagem de firmware a partir dos fragmentos codificados e independentes. Se o dispositivo não tiver recebido todos os fragmentos, a nova imagem não poderá ser reconstruída e esse status será exibido. Para solucionar o erro, inicie uma nova tarefa FUOTA para o dispositivo.

- Erro de MIC

Quando o seu dispositivo reconstrói a nova imagem de firmware a partir dos fragmentos coletados, ele executa um MIC (Verificação de Integridade da Mensagem) para verificar a autenticidade da imagem e se ela vem da origem correta. Caso o dispositivo detecte uma incompatibilidade no MIC após a remontagem dos fragmentos, esse status será exibido. Para solucionar o erro, inicie uma nova tarefa FUOTA para o dispositivo.

- Com êxito

A sessão FUOTA do dispositivo foi obtive êxito.

#### Note

Embora essa mensagem de status indique que os dispositivos reconstruíram a imagem a partir dos fragmentos e que ela foi verificada, o firmware do dispositivo pode não ter sido atualizado quando o dispositivo relata o status para o AWS IoT Core for LoRaWAN. Verifique se o firmware do seu dispositivo foi atualizado.

### Próximas etapas

Você aprendeu sobre os diferentes status da tarefa FUOTA e seus dispositivos e como pode solucionar qualquer problema. Para acessar mais informações sobre cada um desses status, consulte a [Especificação de transporte de blocos de dados fragmentados LoRaWAN, TS004-1.0.0](#).

## Monitorar sua frota de recursos sem fio em tempo real usando o analisador de rede

O analisador de rede usa uma conexão WebSocket padrão para receber logs de mensagens de rastreamento em tempo real para os recursos de conectividade sem fio. Ao usar o analisador de rede, você pode adicionar os recursos que deseja monitorar, ativar uma sessão de rastreamento de mensagens e começar a receber mensagens de rastreamento em tempo real.

Para monitorar recursos, você também pode usar o Amazon CloudWatch. Para usar o CloudWatch, defina um perfil do IAM para configurar o log e, em seguida, espere que as entradas do log sejam exibidas no console. O analisador de rede reduz significativamente o tempo necessário para configurar uma conexão e começar a receber mensagens de rastreamento, apresentando informações de log em tempo hábil para a frota de recursos. Para obter informações sobre como utilizar o CloudWatch para monitoramento, consulte [Monitorar os recursos do AWS IoT Wireless utilizando o Amazon CloudWatch Logs](#).

Ao reduzir o tempo de configuração e usar as informações das mensagens de rastreamento, você pode monitorar os recursos com mais eficiência, obter insights significativos e solucionar erros. É possível monitorar os dispositivos e os gateways LoRaWAN. Por exemplo, você pode identificar com

rapidez um erro de junção ao integrar um dos dispositivos LoRaWAN. Para depurar o erro, use as informações no log de mensagens de rastreamento apresentado.

## Como usar o analisador de rede

Para monitorar a frota de recursos e começar a receber mensagens de rastreamento, execute as etapas a seguir

### 1. Crie a configuração do analisador de rede e adicione recursos

Antes de ativar as mensagens de rastreamento, crie uma configuração do analisador de rede e adicione recursos à configuração. Primeiro, especifique as configurações, que incluem níveis de log e informações sobre quadros de dispositivos. Adicione os recursos que deseja monitorar utilizando o gateway sem fio e os identificadores dos dispositivos sem fio.

### 2. Transmita mensagens de rastreamento com WebSockets

Você pode gerar um URL de solicitação pré-assinado usando as credenciais do perfil do IAM para transmitir mensagens de rastreamento do analisador de rede usando o protocolo WebSocket.

### 3. Ative a sessão de rastreamento de mensagens e monitore as mensagens de rastreamento

Para começar a receber mensagens de rastreamento, ative sua sessão de rastreamento de mensagens. Para evitar custos adicionais, você pode desativar ou fechar a sessão de mensagens de rastreamento do analisador de rede.

O vídeo a seguir descreve como o analisador de rede do AWS IoT Core for LoRaWAN funciona e fornece orientações sobre a adição de recursos e o rastreamento de atividades de junção utilizando o analisador de rede.

Os tópicos a seguir mostram como criar a configuração, adicionar recursos e ativar a sessão de rastreamento de mensagens.

## Tópicos

- [Adicionar o perfil do IAM necessário para o analisador de rede](#)
- [Criar a configuração do analisador de rede e adicionar recursos](#)
- [Transmitir mensagens de rastreamento do analisador de rede com WebSockets](#)
- [Visualize e monitore os logs de mensagens de rastreamento do analisador de rede em tempo real](#)
- [Depure e solucione problemas de seus grupos multicast e tarefas FUOTA usando o analisador de rede](#)

## Adicionar o perfil do IAM necessário para o analisador de rede

Ao usar o analisador de rede, você deve conceder permissão de usuário para usar as operações de API [UpdateNetworkAnalyzerConfiguration](#) e [GetNetworkAnalyzerConfiguration](#) para acessar os recursos do analisador de rede. Confira a seguir as políticas do IAM que você usa para conceder permissões.

### Políticas do IAM para analisador de rede

Use uma das opções a seguir:

- Política sem fio de acesso total

Conceda a política de acesso total do AWS IoT Core for LoRaWAN anexando a política `AWSIoTWirelessFullAccess` ao perfil. Para obter mais informações, consulte [Resumo da política de AWSIoTWirelessFullAccess](#).

- Política do IAM com escopo definido para a API Get and Update

Crie a seguinte política do IAM acessando a página [Criar política](#) do console do IAM, e na guia Editor visual:

1. Escolha `IoTWireless` para Serviço.
2. Em Nível de acesso, expanda `Ler`, escolha `GetNetworkAnalyzerConfiguration` e expanda `Gravar` e escolha `UpdateNetworkAnalyzerConfiguration`.
3. Escolha Próximo: tags e insira um Nome para a política, como `IoTWirelessNetworkAnalyzerPolicy`. Escolha `Criar política`.

Confira a seguir a política `IoTWirelessNetworkAnalyzerPolicy` que você criou. Para obter mais informações sobre a criação de uma política, consulte [Criar políticas do IAM](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:UpdateNetworkAnalyzerConfiguration"
      ],
      "Resource": "*"
    }
  ]
}
```

```

    }
  ]
}

```

## Política com escopo definido para acessar recursos específicos

Para configurar um controle de acesso mais refinado, adicione os gateways sem fio e os dispositivos ao campo Recurso. A política a seguir utiliza o ARN curinga para conceder acesso a todos os gateways e dispositivos. É possível controlar o acesso a gateways e dispositivos específicos utilizando `WirelessGatewayId` e `WirelessDeviceId`.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:UpdateNetworkAnalyzerConfiguration"
      ],
      "Resource": [
        "arn:aws:iotwireless:*:{accountId}:WirelessDevice/*",
        "arn:aws:iotwireless:*:{accountId}:WirelessGateway/*",
        "arn:aws:iotwireless:*:{accountId}:NetworkAnalyzerConfiguration/*"
      ]
    }
  ]
}

```

Para conceder permissão a um usuário para utilizar o analisador de rede, mas não para utilizar gateways ou dispositivos sem fio, utilize a política a seguir. A menos que especificado, as permissões para usar os recursos são negadas implicitamente.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [

```

```
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:UpdateNetworkAnalyzerConfiguration"
    ],
    "Resource": [
        "arn:aws:iotwireless:*:{accountId}:NetworkAnalyzerConfiguration/*"
    ]
}
]
```

## Próximas etapas

Agora que você criou a política, pode adicionar recursos à configuração do analisador de rede e receber informações de rastreamento de mensagens para esses recursos. Para ter mais informações, consulte [Criar a configuração do analisador de rede e adicionar recursos](#).

## Criar a configuração do analisador de rede e adicionar recursos

Antes de transmitir mensagens de rastreamento, crie uma configuração do analisador de rede e adicione os recursos que você deseja monitorar a essa configuração. Ao criar uma configuração, você pode:

- Especificar um nome de configuração e uma descrição opcional.
- Personalizar as configurações, como informações do quadro e nível de detalhes das mensagens de log.
- Adicionar os recursos que você deseja monitorar. Os recursos podem ser dispositivos ou gateways sem fio ou ambos.

As configurações que você especificar determinarão as informações de rastreamento de mensagens que você receberá dos recursos adicionados à configuração. Talvez você também queira criar várias configurações, dependendo do caso de uso de monitoramento.

Veja a seguir como criar uma configuração e adicionar recursos.

### Tópicos

- [Criar uma configuração do analisador de rede](#)
- [Adicionar recursos e atualizar a configuração do analisador de rede](#)

## Criar uma configuração do analisador de rede

Para poder monitorar os gateways ou os dispositivos sem fio, crie uma configuração para o analisador de rede. Ao criar a configuração, você só precisa especificar um nome de configuração. Você pode personalizar as configurações e adicionar os recursos que deseja monitorar à sua configuração mesmo depois de criada. As configurações determinam as informações de rastreamento de mensagens que você receberá para esses recursos.

Dependendo dos recursos que você deseja monitorar e do nível de informações que deseja receber sobre eles, talvez você queira criar várias configurações. Por exemplo, você pode criar uma configuração que exiba somente informações de erro para um conjunto de gateways em sua Conta da AWS. Você também pode criar uma configuração que exiba todas as informações sobre um dispositivo sem fio que você queira monitorar.

As seções a seguir mostram as várias definições de configuração e como criar a configuração.

### Definições de configuração

Ao criar ou atualizar a configuração do analisador de rede, você também pode personalizar os parâmetros a seguir para filtrar as informações do fluxo de logs.

- Informações sobre o quadro

Essa configuração é a informação do quadro dos recursos do seu dispositivo sem fio para mensagens de rastreamento. As informações do quadro podem ser usadas para depurar a comunicação entre o servidor de rede e os dispositivos finais. Ele é habilitado por padrão.

- Níveis de log

Você pode ver os logs de informações ou de erros, ou pode desativar o log.

- Informações

Os logs com um nível de log de Informações são mais detalhados e contêm fluxos de logs de erros e fluxos de logs informativos. Os logs informativos podem ser usados para visualizar alterações no estado de um dispositivo ou gateway.

**Note**

A coleta de fluxos de logs mais detalhados pode gerar custos adicionais. Para obter mais informações sobre a definição de preço, consulte [Definição de preço do AWS IoT Core](#).

- Erro

Os logs com um nível de log de Erro são menos detalhados e exibem somente informações de erro. Você pode usar esses logs quando um aplicativo tem um erro, como um erro de conexão do dispositivo. Ao usar as informações do fluxo de logs, você pode identificar e solucionar erros nos recursos da sua frota.

Criar uma configuração usando o console

É possível criar uma configuração do analisador de rede e personalizar os parâmetros opcionais utilizando o console do AWS IoT ou a API do AWS IoT Wireless. Você também pode criar várias configurações e, posteriormente, excluir qualquer configuração que não esteja mais usando.

Criar uma configuração do analisador de rede

1. Abra o [Hub do analisador de rede do console de AWS IoT](#) e escolha Criar configuração.

2. Especifique as definições da configuração.

- Nome, descrição e tags

Especifique um Nome de configuração exclusivo que contenha somente letras, números, hifens ou sublinhados. Utilize o campo opcional Descrição, para fornecer informações sobre a configuração, e o campo Tags, para adicionar pares de chave-valor de metadados sobre a configuração. Para obter mais informações sobre nomenclatura e descrição dos recursos, consulte [Descrever os recursos do AWS IoT Wireless](#).

- Definições de configuração

Escolha se deseja desativar as informações do quadro e use Selecionar níveis de log para escolher os níveis de log que você deseja usar para seus logs de mensagens de rastreamento. Escolha Próximo.

3. Adicione recursos à configuração. Você pode adicionar recursos agora ou escolher Criar e adicioná-los mais tarde. Para adicionar recursos posteriormente, escolha Criar.

Na página Hub do analisador de rede, você verá a configuração que criou junto com as configurações. Para visualizar os detalhes da nova configuração, escolha o nome da configuração.

## Excluir a configuração do analisador de rede

É possível criar várias configurações do analisador de rede dependendo dos recursos que você deseja monitorar e do nível de informações de rastreamento de mensagens que deseja receber sobre eles.

Para remover configurações do console

1. Vá para o [Hub do analisador de rede do console de AWS IoT](#) e escolha a configuração que deseja remover.
2. Escolha Ações e, em seguida, escolha Excluir.

## Criar uma configuração usando a API

Para criar uma configuração do analisador de rede usando a API, use a operação de API [CreateNetworkAnalyzerConfiguration](#) ou o comando da CLI [create-network-analyzer-configuration](#).

Ao criar a configuração, você só precisa especificar um nome de configuração. Você também pode usar essa operação de API para especificar as definições de configuração e adicionar recursos ao criar a configuração. Também é possível especificá-las posteriormente utilizando a operação de API [UpdateNetworkAnalyzerConfiguration](#) ou o [update-network-analyzer-configuration](#) da CLI.

- Criar uma configuração

Ao criar sua configuração, é necessário especificar um nome. Por exemplo, o comando a seguir cria uma configuração apresentando somente um nome e uma descrição opcional. Por padrão, a configuração tem as informações do quadro ativadas e usa um nível de log de INFO.

```
aws iotwireless create-network-analyzer-configuration \  
  --configuration-name My_Network_Analyzer_Config \  
  --description "My first network analyzer configuration"
```

A execução desse comando exibe o ARN e o ID da configuração do analisador de rede.

```
{
  "Arn": "arn:aws:iotwireless:us-
east-1:123456789012:NetworkAnalyzerConfiguration/12345678-a1b2-3c45-67d8-
e90fa1b2c34d",
  "Id": "12345678-a1b2-3c45-67d8-e90fa1b2c34d"
}
```

- Criar configurações com recursos

Para personalizar as definições de configuração, use o parâmetro `trace-content`. Para adicionar recursos, utilize os parâmetros `WirelessDevices` e `WirelessGateways` para especificar os gateways e dispositivos que você deseja adicionar à configuração. Por exemplo, o comando a seguir personaliza as definições de configuração e adiciona os recursos sem fio, especificados por `WirelessGatewayID` e `WirelessDeviceID`, à configuração.

```
aws iotwireless create-network-analyzer-configuration \
  --configuration-name My_NetworkAnalyzer_Config \
  --trace-content WirelessDeviceFrameInfo=DISABLED,LogLevel="ERROR" \
  --wireless-gateways "12345678-a1b2-3c45-67d8-e90fa1b2c34d" "90123456-
de1f-2b3b-4c5c-bb1112223cd1"
  --wireless-devices "1ffd32c8-8130-4194-96df-622f072a315f"
```

O exemplo a seguir mostra a saída da execução do comando:

```
{
  "Arn": "arn:aws:iotwireless:us-
east-1:123456789012:NetworkAnalyzerConfiguration/12345678-a1b2-3c45-67d8-
e90fa1b2c34d",
  "Id": "12345678-a1b2-3c45-67d8-e90fa1b2c34d"
}
```

## Listar configurações do analisador de rede

É possível criar várias configurações do analisador de rede dependendo dos recursos que você deseja monitorar e do nível de detalhes das informações de rastreamento de mensagens que deseja receber sobre eles. Depois de criar essas configurações, você pode usar a operação de API [ListNetworkAnalyzerConfigurations](#) ou o comando da CLI [list-network-analyzer-configuration](#) para obter uma lista dessas configurações.

```
aws iotwireless list-network-analyzer-configurations
```

A execução desse comando exibe todas as configurações do analisador de rede na Conta da AWS. Você também pode usar o parâmetro `max-results` para especificar quantas configurações deseja exibir. Confira a seguir a saída de execução desse comando.

```
{
  "NetworkAnalyzerConfigurationList": [
    {
      "Arn": "arn:aws:iotwireless:us-
east-1:123456789012:NetworkAnalyzerConfiguration/12345678-a1b2-3c45-67d8-e90fa1b2c34d",
      "Name": "My_Network_Analyzer_Config1"
    },
    {
      "Arn": "arn:aws:iotwireless:us-
east-1:123456789012:NetworkAnalyzerConfiguration/90123456-a1a2-9a87-65b4-c12bf3c2d09a",
      "Name": "My_Network_Analyzer_Config2"
    }
  ]
}
```

## Excluir a configuração do analisador de rede

Você pode excluir uma configuração que não esteja mais usando com a operação de API [DeleteNetworkAnalyzerConfiguration](#) ou o comando da CLI [delete-network-analyzer-configuration](#).

```
aws iotwireless delete-network-analyzer-configuration \
  --configuration-name My_NetworkAnalyzer_Config
```

A execução desse comando não retorna nenhuma saída. Para ver as configurações disponíveis, você pode usar a operação de API `ListNetworkAnalyzerConfigurations`.

## Próximas etapas

Agora que criou uma configuração do analisador de rede, você pode adicionar recursos à sua configuração ou atualizar as definições de configuração. Para ter mais informações, consulte [Adicionar recursos e atualizar a configuração do analisador de rede](#).

## Adicionar recursos e atualizar a configuração do analisador de rede

Para poder ativar as mensagens de rastreamento, adicione os recursos à configuração. É possível utilizar uma única configuração padrão do analisador de rede. O AWS IoT Core for LoRaWAN atribui o nome `NetworkAnalyzerConfig_Default` a essa configuração, e esse campo não pode ser editado. Essa configuração é adicionada automaticamente ao Conta da AWS quando você utiliza o analisador de rede no console.

É possível adicionar os recursos que deseja monitorar à configuração padrão. Os recursos podem ser dispositivos LoRaWAN e gateways LoRaWAN. Para adicionar cada recurso à configuração, utilize o gateway sem fio e os identificadores dos dispositivos sem fio.

### Definições de configuração

Para definir as configurações, primeiro adicione recursos à configuração padrão e ative as mensagens de rastreamento. Após o recebimento dos logs de mensagens de rastreamento, também é possível personalizar os parâmetros a seguir para atualizar a configuração padrão e filtrar o fluxo de logs.

- Informações sobre o quadro


Essa configuração são as informações de quadro dos recursos de dispositivos sem fio para mensagens de rastreamento. As informações de quadro são habilitadas por padrão e podem ser utilizadas para depurar a comunicação entre o servidor de rede e os dispositivos finais.

- Níveis de log

Você pode ver os logs de informações ou de erros, ou pode desativar o log.

- Informações

Os logs com o nível Informações são mais detalhados e contêm fluxos de logs tanto informativos como de erros. Os logs informativos podem ser utilizados para visualizar alterações no estado de um dispositivo ou de um gateway.

 Note

A coleta de fluxos de logs mais detalhados pode gerar custos adicionais. Para obter mais informações sobre a definição de preço, consulte [Definição de preço do AWS IoT Core](#).

- Erro

Os logs com um nível de log de Erro são menos detalhados e exibem somente informações de erro. Você pode usar esses logs quando um aplicativo tem um erro, como um erro de conexão do dispositivo. Ao usar as informações do fluxo de logs, você pode identificar e solucionar erros nos recursos da sua frota.

## Pré-requisitos

Para poder adicionar recursos, os gateways e dispositivos a serem monitorados já devem estar integrados ao AWS IoT Core for LoRaWAN. Para ter mais informações, consulte [Conectar gateways e dispositivos ao AWS IoT Core for LoRaWAN](#).

Adicionar recursos e atualizar a configuração do analisador de rede com o console

É possível adicionar recursos e personalizar os parâmetros opcionais utilizando o console do AWS IoT ou a API do AWS IoT Wireless. Além dos recursos, você também pode editar as definições de configuração e salvar a configuração atualizada.

Como adicionar recursos à configuração (console)

1. Abra o [Hub do analisador de rede no console do AWS IoT](#) e escolha a configuração do analisador de rede, NetworkAnalyzerConfig\_Default.
2. Selecione Adicionar recursos.
3. Adicione os recursos que deseja monitorar usando o gateway sem fio e os identificadores de dispositivos sem fio. É possível adicionar até 250 gateways ou dispositivos sem fio. Para adicionar o recurso:
  - a. Utilize a guia Visualizar gateways ou Visualizar dispositivos para ver a lista de gateways e dispositivos que você adicionou ao Conta da AWS.
  - b. Copie o WirelessDeviceID ou o WirelessGatewayID do dispositivo ou do gateway que você deseja monitorar e insira o valor do identificador para o recurso correspondente.
  - c. Para continuar a adicionar recursos, escolha Adicionar gateway ou Adicionar dispositivo e adicione o gateway ou dispositivo sem fio. Se você adicionou um recurso que não deseja mais monitorar, escolha Remover recurso.
4. Depois de adicionar todos os recursos, escolha Adicionar.

Você verá o número de gateways e dispositivos que adicionou na página Hub do analisador de rede. É possível continuar adicionando gateways e dispositivos até que a sessão de rastreamento

de mensagens seja ativada. Depois que a sessão for ativada, para adicionar recursos, será necessário desativar a sessão.

Como editar a configuração do analisador de rede (console)

É possível editar a configuração do analisador de rede e escolher se deseja desabilitar as informações de quadro e o nível de log das mensagens de rastreamento.

1. Abra o [Hub do analisador de rede no console do AWS IoT](#) e escolha a configuração do analisador de rede, `NetworkAnalyzerConfig_Default`.
2. Selecione a opção Editar.
3. Escolha se deseja desativar as informações do quadro e use Selecionar níveis de log para escolher os níveis de log que você deseja usar para os logs de mensagens de rastreamento. Escolha Salvar.

Você verá as definições de configuração especificadas na página de detalhes da configuração do analisador de rede.

Adicionar recursos e atualizar a configuração do analisador de rede com a API

É possível utilizar as [operações de API do AWS IoT Wireless](#) ou os [comandos da CLI do AWS IoT Wireless](#) para adicionar recursos e atualizar as configurações do analisador de rede.

- Para adicionar recursos ou atualizar a configuração do analisador de rede, utilize a API [UpdateNetworkAnalyzerConfiguration](#) ou o comando [update-network-analyzer-configuration](#) da CLI.

- Adicionar recursos

Para os dispositivos sem fio que você deseja adicionar, utilize `WirelessDevicesToAdd` para inserir o `WirelessDeviceID` dos dispositivos como uma matriz de strings. Para os gateways sem fio que você deseja adicionar, utilize `WirelessGatewaysToAdd` para inserir o `WirelessGatewayID` dos gateways como uma matriz de strings.

- Editar a configuração

Para editar a configuração do analisador de rede, utilize o parâmetro `TraceContent` para especificar se `WirelessDeviceFrameInfo` deve ser `ENABLED` ou `DISABLED`, e se o parâmetro `LogLevel` deve ser `INFO`, `ERROR` ou `DISABLED`.

```
{
  "TraceContent": {
    "LogLevel": "string",
    "WirelessDeviceFrameInfo": "string"
  },
  "WirelessDevicesToAdd": [ "string" ],
  "WirelessDevicesToRemove": [ "string" ],
  "WirelessGatewaysToAdd": [ "string" ],
  "WirelessGatewaysToRemove": [ "string" ]
}
```

- Para obter informações sobre a configuração e os recursos adicionados, utilize a operação de API [GetNetworkAnalyzerConfiguration](#) ou o comando [get-network-analyzer-configuration](#). Forneça o nome da configuração do analisador de rede, `NetworkAnalyzerConfig_Default`, como entrada.

## Próximas etapas

Agora que adicionou recursos e especificou todas as definições opcionais para a configuração, é possível utilizar o protocolo WebSocket para estabelecer uma conexão com o AWS IoT Core for LoRaWAN e utilizar o analisador de rede. Em seguida, você pode ativar as mensagens de rastreamento e começar a receber essas mensagens para os recursos. Para ter mais informações, consulte [Transmitir mensagens de rastreamento do analisador de rede com WebSockets](#).

## Transmitir mensagens de rastreamento do analisador de rede com WebSockets

Ao usar o protocolo WebSocket, você pode transmitir mensagens de rastreamento do analisador de rede em tempo real. Quando você envia uma solicitação, o serviço responde com uma estrutura JSON. Depois de ativar as mensagens de rastreamento, você pode usar os logs de mensagens para obter informações sobre os recursos e solucionar erros. Para obter mais informações, consulte [Protocolo WebSocket](#).

A seguir, é mostrado como transmitir mensagens de rastreamento do analisador de rede com WebSockets.

## Tópicos

- [Gerar uma solicitação pré-assinada com a biblioteca WebSocket](#)

- [Mensagens e códigos de status do WebSocket](#)

## Gerar uma solicitação pré-assinada com a biblioteca WebSocket

A seguir, descrevemos como gerar uma solicitação pré-assinada para que seja possível utilizar a biblioteca WebSocket para enviar solicitações ao serviço.

Adicionar uma política para solicitações WebSocket ao perfil do IAM

Para usar o protocolo WebSocket para chamar o analisador de rede, anexe a política a seguir ao perfil do AWS Identity and Access Management (IAM) que faz a solicitação.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iotwireless:StartNetworkAnalyzerStream",
      "Resource": "*"
    }
  ]
}
```

### Criar um URL pré-assinado

Crie um URL para a solicitação WebSocket que contenha as informações necessárias para configurar a comunicação entre o aplicativo e o analisador de rede. Para verificar a identidade da solicitação, o streaming WebSocket usa o processo do Amazon Signature versão 4 para assinar solicitações. Para obter mais informações sobre o Signature versão 4, consulte [Assinar solicitações de API da AWS](#) na Referência geral do Amazon Web Services.

Para chamar o analisador de rede, use o URL de solicitação StartNetworkAnalyzerStream. A solicitação será assinada usando as credenciais do perfil do IAM mencionado anteriormente. O URL tem o formato a seguir com quebras de linha adicionadas para facilitar a leitura.

```
GET wss://api.iotwireless.<region>.amazonaws.com/start-network-analyzer-stream?X-Amz-Algorithm=AWS4-HMAC-SHA256
  &X-Amz-Credential=Signature Version 4 credential scope
  &X-Amz-Date=date
  &X-Amz-Expires=time in seconds until expiration
  &X-Amz-Security-Token=security-token
```

```
&X-Amz-Signature=Signature Version 4 signature
&X-Amz-SignedHeaders=host
```

Use os valores a seguir para os parâmetros de Signature versão 4:

- X-Amz-Algorithm – O algoritmo que você está usando no processo de assinatura. O único valor válido é AWS4-HMAC-SHA256.
- X-Amz-Credential – Uma string separada por barras ("/") formada concatenando o ID de chave de acesso e os componentes de escopo de credencial. O escopo de credencial inclui a data no formato AAAAMMDD, a Região da AWS, o nome do serviço e uma string de terminação (aws4\_request).
- X-Amz-Date – A data e a hora em que a assinatura foi criada. Gere a data e a hora seguindo as instruções em [Tratamento de datas no Signature versão 4](#) na Referência geral do Amazon Web Services.
- X-Amz-Expires – O tempo, em segundos, até que as credenciais expirem. O valor máximo é de 300 segundos (5 minutos).
- X-Amz-Security-Token – (opcional) Um token do Signature versão 4 para credenciais temporárias. Se você especificar esse parâmetro, inclua-o na solicitação canônica. Para obter mais informações, consulte [Solicitação de credenciais de segurança temporárias](#) no Guia do usuário do AWS Identity and Access Management.
- X-Amz-Signature – A assinatura do Signature versão 4 que você gerou para a solicitação.
- X-Amz-SignedHeaders – Os cabeçalhos que são assinados ao criar a assinatura para a solicitação. O único valor válido é host.

Crie o URL da solicitação e crie a assinatura do Signature versão 4

Para criar o URL para a solicitação e criar a assinatura do Signature versão 4, siga as etapas a seguir. Os exemplos estão em pseudocódigo.

Tarefa 1: Criar uma solicitação canônica

Crie uma string que inclua as informações da solicitação em um formato padronizado. Isso garante que quando a AWS receber a solicitação, ela poderá calcular a mesma assinatura que você calcular em [Tarefa 3: Calcular a assinatura](#). Para obter mais informações, consulte [Criar uma solicitação canônica para o Signature versão 4](#) na Referência geral do Amazon Web Services.

1. Defina variáveis para a solicitação no seu aplicativo.

```
# HTTP verb
method = "GET"
# Service name
service = "iotwireless"
# Região da AWS
region = "Região da AWS"
# Service streaming endpoint
endpoint = "wss://api.iotwireless.<region>.amazonaws.com"
# Host
host = "api.iotwireless.<region>.amazonaws.com"
# Date and time of request
amz-date = YYYYMMDD'T'HHMMSS'Z'
# Date without time for credential scope
datestamp = YYYYMMDD
```

2. Crie um URI canônico (identificador uniforme de recursos). O URI canônico é a parte do URI entre o domínio e a string de consulta.

```
canonical_uri = "/start-network-analyzer-stream"
```

3. Crie cabeçalhos canônicos e cabeçalhos assinados. Observe o `\n` que aparece no final dos cabeçalhos canônicos.
  - Anexe o nome do cabeçalho em minúscula seguido por dois pontos.
  - Anexe uma lista separada por vírgulas de valores para esse cabeçalho. Não classifique os valores em cabeçalhos que têm vários valores.
  - Anexe uma nova linha (`\n`).

```
canonical_headers = "host:" + host + "\n"
signed_headers = "host"
```

4. Faça uma correspondência entre o algoritmo e o algoritmo de hash. Você deve usar SHA-256.

```
algorithm = "AWS4-HMAC-SHA256"
```

5. Crie o escopo da credencial, que define o escopo da chave derivada como a data, a Região e o serviço ao qual a solicitação foi feita.

```
credential_scope = datestamp + "/" + region + "/" + service + "/" + "aws4_request"
```

6. Crie a string de consulta canônica. Os valores de string de consulta devem ser codificados por URI e classificados por nome.
  - Classifique os nomes de parâmetro por ponto de código de caracteres em ordem ascendente. Parâmetros com nomes duplicados devem ser classificados pelo valor. Por exemplo, um nome de parâmetro que começa com a letra maiúscula F precede um nome de parâmetro que começa com uma letra minúscula b.
  - Não codifique em URI nenhum dos caracteres não reservados definidos pela [RFC 3986](#): A–Z, a–z, 0–9, hífen ( - ), sublinhado ( \_ ), ponto ( . ) e til ( ~ ).
  - Codifique em percentual todos os outros caracteres com %XY, em que X e Y são caracteres hexadecimais (de 0 a 9 e maiúsculas de A a F). Por exemplo, o caractere de espaço deve ser codificado como %20 (não usando '+', como alguns esquemas de codificação) e deve haver caracteres UTF-8 estendidos na forma %XY%ZA%BC.
  - Codifique duas vezes todos os caracteres de sinal de igual (=) em valores de parâmetro.

```
canonical_querystring = "X-Amz-Algorithm=" + algorithm
canonical_querystring += "&X-Amz-Credential=" + URI-encode(access key + "/" +
  credential_scope)
canonical_querystring += "&X-Amz-Date=" + amz_date
canonical_querystring += "&X-Amz-Expires=300"
canonical_querystring += "&X-Amz-Security-Token=" + token
canonical_querystring += "&X-Amz-SignedHeaders=" + signed_headers
canonical_querystring += "&language-code=en-US&media-encoding=pcm&sample-
  rate=16000"
```

7. Crie um hash da carga útil. Para uma solicitação GET, a carga útil é uma string vazia.

```
payload_hash = HashSHA256("").Encode("utf-8").HexDigest()
```

8. Combine todos os elementos para criar a solicitação canônica.

```
canonical_request = method + '\n'
  + canonical_uri + '\n'
  + canonical_querystring + '\n'
  + canonical_headers + '\n'
  + signed_headers + '\n'
```

```
+ payload_hash
```

## Tarefa 2: Criar a string para assinar

A string para assinar inclui metainformações sobre sua solicitação. Você usará a string para assinar na próxima etapa, quando calcular a assinatura da solicitação. Para obter mais informações, consulte [Criar uma string para assinar o Signature versão 4](#) na Referência geral do Amazon Web Services.

```
string_to_sign=algorithm + "\n"  
+ amz_date + "\n"  
+ credential_scope + "\n"  
+ HashSHA256(canonical_request.Encode("utf-8")).HexDigest()
```

## Tarefa 3: Calcular a assinatura

Você derivará uma chave de assinatura da sua chave de acesso secreta da AWS. Para obter um grau maior de proteção, a chave derivada é específica à data, ao serviço e à Região da AWS. Você usa a chave derivada para assinar a solicitação. Para obter mais informações, consulte [Calcular a assinatura do Signature versão 4 da AWS](#) na Referência geral do Amazon Web Services.

O código pressupõe que você tenha implementado a função `GetSignatureKey` para gerar uma chave de assinatura. Para obter mais informações e exemplos de funções, consulte [Exemplos de como derivar uma chave de assinatura do Signature versão 4](#) na Referência geral do Amazon Web Services.

A função `HMAC(key, data)` representa uma função HMAC-SHA256 que retorna os resultados em formato binário.

```
#Create the signing key  
signing_key = GetSignatureKey(secret_key, timestamp, region, service)  
  
# Sign the string_to_sign using the signing key  
signature = HMAC.new(signing_key, (string_to_sign).Encode("utf-8"), Sha256()).HexDigest
```

## Tarefa 4: Adicionar informações de assinatura à solicitação e criar o URL da solicitação

Depois de calcular a assinatura, adicione-a à string de consulta. Para obter mais informações, consulte [Adicionar a assinatura à solicitação](#) na Referência geral do Amazon Web Services.

```
#Add the authentication information to the query string
canonical_querystring += "&X-Amz-Signature=" + signature

# Sign the string_to_sign using the signing key
request_url = endpoint + canonical_uri + "?" + canonical_querystring
```

## Próximas etapas

Você pode usar o URL da solicitação com a biblioteca WebSocket para fazer a solicitação ao serviço e observar as mensagens. Para ter mais informações, consulte [Mensagens e códigos de status do WebSocket](#).

## Mensagens e códigos de status do WebSocket

Depois de criar uma solicitação pré-assinada, você pode usar o URL da solicitação com a biblioteca WebSocket ou com uma biblioteca adequada à sua linguagem de programação para fazer solicitações ao serviço. Para obter mais informações sobre como gerar essa solicitação pré-assinada, consulte [Gerar uma solicitação pré-assinada com a biblioteca WebSocket](#).

## Mensagens WebSocket

O protocolo WebSocket pode ser usado para estabelecer uma conexão bidirecional. As mensagens podem ser transmitidas de cliente para servidor e de servidor para cliente. No entanto, o analisador de rede suporta somente mensagens enviadas do servidor para o cliente. Qualquer mensagem recebida do cliente é inesperada e o servidor encerrará automaticamente a conexão do WebSocket se uma mensagem for recebida do cliente.

Quando a solicitação é recebida e uma sessão de rastreamento de mensagens é iniciada, o servidor responde com uma estrutura JSON, que é a carga útil. Para obter mais informações sobre a carga útil e como você pode ativar o rastreamento de mensagens a partir do Console de gerenciamento da AWS, consulte [Visualize e monitore os logs de mensagens de rastreamento do analisador de rede em tempo real](#).

## Códigos de status WebSocket

O seguinte mostra os códigos de status do WebSocket para a comunicação do servidor com o cliente. Os códigos de status do WebSocket seguem o [Padrão RFC de encerramento normal de conexões](#).

A opção a seguir mostra os códigos de status compatíveis:

- 1000

Esse código de status indica um encerramento normal, ou seja, que a conexão do WebSocket foi estabelecida e a solicitação foi atendida. Esse status pode ser observado quando uma sessão está ociosa, fazendo com que a conexão atinja o tempo limite.

- 1.002

Esse código de status indica que o endpoint está encerrando a conexão devido a um erro de protocolo.

- 1003

Esse código de status indica um status de erro em que o endpoint encerrou a conexão porque recebeu dados em um formato que não pode aceitar. O endpoint suporta somente dados de texto e pode exibir esse código de status se receber uma mensagem binária ou uma mensagem do cliente que esteja usando um formato incompatível.

- 1008

Esse código de status indica um status de erro em que o endpoint encerrou a conexão porque recebeu uma mensagem que viola essa política. Esse status é genérico e é exibido quando os outros códigos de status, como 1003 ou 1009, não são aplicáveis. Você também verá esse status exibido se houver necessidade de ocultar a política ou quando houver uma falha na autorização, como uma assinatura expirada.

- 1011

Esse código de status indica um status de erro em que o servidor está encerrando a conexão porque encontrou uma condição inesperada ou um erro interno que o impediu de atender à solicitação.

## Próximas etapas

Agora que você aprendeu como gerar uma solicitação pré-assinada e como observar as mensagens do servidor usando a conexão WebSocket, você pode ativar o rastreamento de mensagens e começar a receber logs de mensagens para o gateway sem fio e os recursos do dispositivo sem fio. Para ter mais informações, consulte [Visualize e monitore os logs de mensagens de rastreamento do analisador de rede em tempo real](#).

# Visualize e monitore os logs de mensagens de rastreamento do analisador de rede em tempo real

Se adicionou recursos à configuração do analisador de rede, você pode ativar as mensagens de rastreamento para começar a receber mensagens de rastreamento para seus recursos. É possível utilizar o Console de gerenciamento da AWS, a API do AWS IoT Wireless ou a AWS CLI.

## Pré-requisitos

Antes de ativar o rastreamento de mensagens usando o analisador de rede, você deve ter:

- Adicionado os recursos que deseja monitorar à configuração padrão do analisador de rede. Para ter mais informações, consulte [Adicionar recursos e atualizar a configuração do analisador de rede](#).
- Gerado uma solicitação pré-assinada usando o URL da solicitação `StartNetworkAnalyzerStream`. A solicitação será assinada usando as credenciais do perfil do AWS Identity and Access Management que faz essa solicitação. Para ter mais informações, consulte [Criar um URL pré-assinado](#).

## Ativado o rastreamento de mensagens usando o console

Para ativar o rastreamento de mensagens

1. Abra o [Hub do analisador de rede do console de AWS IoT](#) e escolha a configuração do analisador de rede, `NetworkAnalyzerConfig_Default`.
2. Na página de detalhes da configuração do analisador de rede, escolha **Ativar rastreamento de mensagens** e, em seguida, escolha **Ativar**.

Você começará a receber mensagens de rastreamento quando a mensagem de rastreamento mais recente aparecer primeiro no console.

### Note

Após o início da sessão de mensagens, o recebimento de mensagens de rastreamento pode gerar custos adicionais até que você desative a sessão ou saia da sessão de rastreamento. Para obter mais informações sobre a definição de preço, consulte [Definição de preço do AWS IoT Core](#).

## Visualizar e monitorar mensagens de rastreamento

Depois de ativar o rastreamento de mensagens, a conexão do WebSocket é estabelecida e as mensagens de rastreamento começam a aparecer em tempo real, primeiro as mais recentes. Você pode personalizar as preferências para especificar o número de mensagens de rastreamento a serem exibidas em cada página e exibir somente os campos relevantes para cada mensagem. Por exemplo, você pode personalizar o log de mensagens de rastreamento para mostrar somente logs de recursos de gateway sem fio que tenham o Nível de log definido como ERROR, para que você possa identificar e depurar erros com rapidez com seus gateways. As mensagens de rastreamento contêm as seguintes informações:

- Número da mensagem: um número exclusivo que mostra a última mensagem recebida primeiro.
- ID do recurso: o gateway sem fio ou ID do dispositivo sem fio do recurso.
- Carimbo de data/hora: a hora em que a mensagem foi recebida.
- ID da mensagem: um identificador que o AWS IoT Core for LoRaWAN atribui a cada mensagem recebida.
- FPort: a porta de frequência para comunicação com o dispositivo usando a conexão WebSocket.
- DevEui: o identificador exclusivo estendido (EUI) para o dispositivo sem fio.
- Recurso: se o recurso monitorado é um dispositivo sem fio ou um gateway sem fio.
- Evento: o evento de uma mensagem de log para um dispositivo sem fio, que pode ser Join, Rejoin, Uplink\_Data, Downlink\_Data ou Registration.
- Nível de log: informações sobre os fluxos de logs INFO ou ERROR para o dispositivo.

## Mensagem de log JSON do analisador de rede

Você também pode escolher uma mensagem de rastreamento por vez para visualizar a carga útil JSON dessa mensagem. Dependendo da mensagem selecionada nos logs de mensagens de rastreamento, você verá informações na carga útil JSON que indicam que há duas partes: CustomerLog e LoRaFrame.

### CustomerLog

A parte CustomerLog do JSON exibe o tipo e o identificador do recurso que recebeu a mensagem, o nível do log e o conteúdo da mensagem. O exemplo a seguir mostra uma mensagem de log CustomerLog. Você pode usar o campo message no JSON para obter mais informações sobre o erro e como ele pode ser resolvido.

## LoRaFrame

A parte LoRaFrame do JSON tem um ID de mensagem e contém informações sobre a carga útil física do dispositivo e os metadados sem fio.

O exemplo a seguir mostra a estrutura da mensagem de rastreamento.

```
export type TraceMessage = {
  ResourceId: string;
  Timestamp: string;
  LoRaFrame:
  {
    MessageId: string;
    PhysicalPayload: any;
    WirelessMetadata:
    {
      fPort: number;
      dataRate: number;
      devEui: string;
      frequency: number;
      timestamp: string;
    },
  },
  CustomerLog:
  {
    resource: string;
    wirelessDeviceId: string;
    wirelessDeviceType: string;
    event: string;
    logLevel: string;
    messageId: string;
    message: string;
  },
};
```

## Revisão e próximas etapas

Nesta seção, você visualizou mensagens de rastreamento e aprendeu como usar as informações para depurar erros. Depois de ver todas as mensagens, você pode:

- Desativar o rastreamento de mensagens

Para evitar custos adicionais, você pode desativar a sessão de rastreamento de mensagens. A desativação da sessão desconecta a conexão WebSocket para que você não receba nenhuma mensagem de rastreamento adicional. Você ainda pode continuar a visualizar as mensagens existentes no console.

- Edite as informações do quadro para a configuração

Você pode editar a configuração do analisador de rede e escolher se deseja desativar as informações do quadro e escolher os níveis de log para suas mensagens. Antes de atualizar a configuração, considere desativar a sessão de rastreamento de mensagens. Para fazer essas edições, abra a [página de detalhes do analisador de rede no console de AWS IoT](#) e escolha Editar. Em seguida, você pode atualizar a configuração com as novas definições de configuração e ativar o rastreamento de mensagens para ver as mensagens atualizadas.

- Adicionar recursos à configuração

Você também pode adicionar mais recursos à configuração do analisador de rede e monitorá-los em tempo real. Você pode adicionar um total combinado de 250 recursos de gateway sem fio e dispositivo sem fio. Para adicionar recursos, na [página de detalhes do analisador de rede do console de AWS IoT](#), escolha a guia Recursos e Adicionar recursos. Em seguida, você pode atualizar a configuração com os novos recursos e ativar o rastreamento de mensagens para ver as mensagens atualizadas dos recursos adicionais.

Para obter mais informações sobre como atualizar a configuração do analisador de rede editando as definições de configuração e adicionando recursos, consulte [Adicionar recursos e atualizar a configuração do analisador de rede](#).

## Depure e solucione problemas de seus grupos multicast e tarefas FUOTA usando o analisador de rede

Os recursos sem fio que você pode monitorar incluem dispositivos LoRaWAN, gateways LoRaWAN e grupos multicast. Você também pode usar o analisador de rede para depurar e solucionar quaisquer problemas com a tarefa FUOTA. Você também pode monitorar e rastrear mensagens relacionadas à configuração, transmissão de dados e consulta de status quando a tarefa FUOTA está em andamento.

Para monitorar a tarefa FUOTA, se a tarefa contiver grupos multicast, você deverá adicionar o grupo multicast e os dispositivos no grupo à configuração do analisador de rede. Ative também as

informações de quadros e de quadros multicast para rastrear as mensagens unicast e multicast de uplink e downlink trocadas com o grupo multicast e os dispositivos enquanto a tarefa FUOTA estiver em andamento.

Para monitorar grupos multicast, é possível adicioná-los à configuração do analisador de rede e utilizar as informações de quadros multicast para solucionar problemas de mensagens multicast de downlink enviadas a esses grupos. Para solucionar problemas de dispositivos que estão tentando se juntar a um grupo em que a comunicação unicast é utilizada, inclua esses dispositivos também na configuração do analisador de rede. Para monitorar somente a comunicação unicast com os dispositivos do grupo, ative as informações do quadro para os dispositivos sem fio. Essa abordagem garante monitoramento e diagnóstico abrangentes para grupos multicast e dispositivos que estão se juntando ao grupo.

As seções a seguir descrevem como depurar e solucionar problemas de grupos multicast e tarefas FUOTA usando o analisador de rede.

## Tópicos

- [Depurar tarefas FUOTA que contêm dispositivos](#)
- [Depure tarefas FUOTA com grupos multicast](#)
- [Depure dispositivos que estão tentando se juntar a um grupo multicast](#)
- [Depurar uma sessão de grupo multicast](#)

## Depurar tarefas FUOTA que contêm dispositivos

Você pode usar o analisador de rede para depurar uma tarefa FUOTA que tenha apenas dispositivos LoRaWAN adicionados à tarefa. Para obter informações sobre como adicionar dispositivos a uma tarefa FUOTA, consulte [Adicionar dispositivos e grupos de multicast a uma tarefa FUOTA e agendar uma sessão FUOTA](#). Para depurar a tarefa FUOTA, execute as seguintes etapas:

1. Crie uma configuração do analisador de rede ativando as informações de quadros para os dispositivos sem fio, para que seja possível monitorar as mensagens FUOTA de uplink e downlink trocadas com os dispositivos enquanto a tarefa está em andamento.
2. Adicione os dispositivos na tarefa FUOTA à configuração do analisador de rede usando os identificadores de dispositivos sem fio.
3. Ative o rastreamento de mensagens para começar a receber mensagens de rastreamento para os dispositivos na configuração do analisador de rede.

Na coluna `applicationCommandType` das informações da mensagem de rastreamento, você começará a receber mensagens unicast de downlink relacionadas à configuração de transmissão e fragmentação de dados.

#### Note

Se você não vir a coluna `applicationCommandType` na tabela de mensagens de rastreamento, poderá ajustar as configurações para mostrar essa coluna na tabela.

Você também pode ver `applicationCommandType` e outras mensagens detalhadas na mensagem de log JSON em `WirelessMetadata > ApplicationInfo`.

## Depure tarefas FUOTA com grupos multicast

Você pode usar o analisador de rede para depurar uma tarefa FUOTA que tenha grupos multicast e dispositivos LoRaWAN adicionados ao grupo. Para obter informações sobre como adicionar dispositivos a uma tarefa FUOTA, consulte [Adicionar dispositivos e grupos de multicast a uma tarefa FUOTA e agendar uma sessão FUOTA](#). Para depurar a tarefa FUOTA, execute as seguintes etapas:

1. Crie uma configuração do analisador de rede ativando as configurações de informações do quadro e de informações do quadro multicast para os dispositivos sem fio e grupos multicast.
2. Adicione o grupo multicast na tarefa FUOTA à configuração do analisador de rede usando o identificador de grupo multicast. Ao ativar as informações do quadro multicast, você pode depurar a mensagem de dados do firmware e as mensagens de consulta de status FUOTA que são enviadas ao grupo enquanto a tarefa FUOTA está em andamento.
3. Adicione os dispositivos no grupo multicast à configuração do analisador de rede usando os identificadores de dispositivos sem fio. Ao ativar as informações do quadro, você pode monitorar as mensagens de uplink e downlink que são trocadas diretamente com os dispositivos enquanto a tarefa FUOTA está em andamento.
4. Ative o rastreamento de mensagens para começar a receber mensagens de rastreamento para os dispositivos e grupos multicast na configuração do analisador de rede.

É possível visualizar as mensagens de rastreamento e depurá-las utilizando a coluna `applicationCommandType` da tabela de mensagens de rastreamento e usando os detalhes na mensagem do log JSON, conforme descrito em [Depurar tarefas FUOTA que contêm dispositivos](#).

## Depure dispositivos que estão tentando se juntar a um grupo multicast

Você pode usar o analisador de rede para depurar dispositivos que estão tentando se juntar a um grupo multicast. Para obter informações sobre como adicionar dispositivos a um grupo multicast, consulte [Criar grupos de multicast e adicionar dispositivos ao grupo](#). Para depurar o grupo multicast, execute as seguintes etapas:

1. Crie uma configuração do analisador de rede ativando as informações do quadro para os dispositivos sem fio.
2. Adicione os dispositivos que deseja monitorar à configuração do analisador de rede usando os identificadores de dispositivos sem fio.
3. Ative o rastreamento de mensagens para começar a receber mensagens de rastreamento para os dispositivos na configuração do analisador de rede.
4. Comece a associar os dispositivos ao grupo multicast depois que as mensagens de rastreamento forem ativadas para os dispositivos do grupo.

## Depurar uma sessão de grupo multicast

Você pode usar o analisador de rede para depurar uma sessão de grupo multicast. Para ter mais informações, consulte [Agendar uma mensagem de downlink para enviar para os dispositivos de um grupo de multicast](#). Para depurar uma sessão de grupo multicast, execute as seguintes etapas:

1. Crie uma configuração do analisador de rede ativando as informações do quadro multicast para o grupo multicast.
2. Adicione o grupo multicast que deseja monitorar à configuração do analisador de rede usando o identificador de grupo multicast.
3. Antes do início da sessão multicast, ative o rastreamento de mensagens para começar a receber mensagens de rastreamento para a sessão de grupo multicast.
4. Inicie a sessão do grupo multicast e monitore o status visualizando as mensagens que são exibidas na tabela de mensagens de rastreamento e na mensagem de log JSON.

Na tabela de mensagens de rastreamento, `MulticastAddr` será exibido na coluna `DevAddr`. Na mensagem de log JSON, você pode visualizar informações detalhadas como `MulticastGroupId` em `WirelessMetadata > ApplicationInfo`.

# AWS IoT Core for LoRaWAN e endpoint da VPC de interface (AWS PrivateLink)

Você pode se conectar diretamente ao AWS IoT Core for LoRaWAN usando [endpoints da VPC de interface \(AWS PrivateLink\)](#) na nuvem privada virtual (VPC) em vez de se conectar pela Internet pública. Quando você usa um endpoint da VPC de interface, a comunicação entre a VPC e o AWS IoT Core for LoRaWAN é realizada de forma integral e segura na rede da AWS.

O AWS IoT Core for LoRaWAN é compatível com endpoints de interface da nuvem privada virtual da Amazon desenvolvidos pelo AWS PrivateLink. Cada endpoint da VPC é representado por uma ou mais [interfaces de rede elástica](#) com endereços IP privados em suas sub-redes da VPC. Para obter mais informações, consulte [Endpoints da VPC de interface \(AWS PrivateLink\)](#) no Manual do Usuário do Amazon VPC.

Para obter mais informações sobre a VPC e os endpoints, consulte [O que é a Amazon VPC?](#)

Para obter mais informações sobre o AWS PrivateLink, consulte [AWS PrivateLink e endpoints da VPC](#).

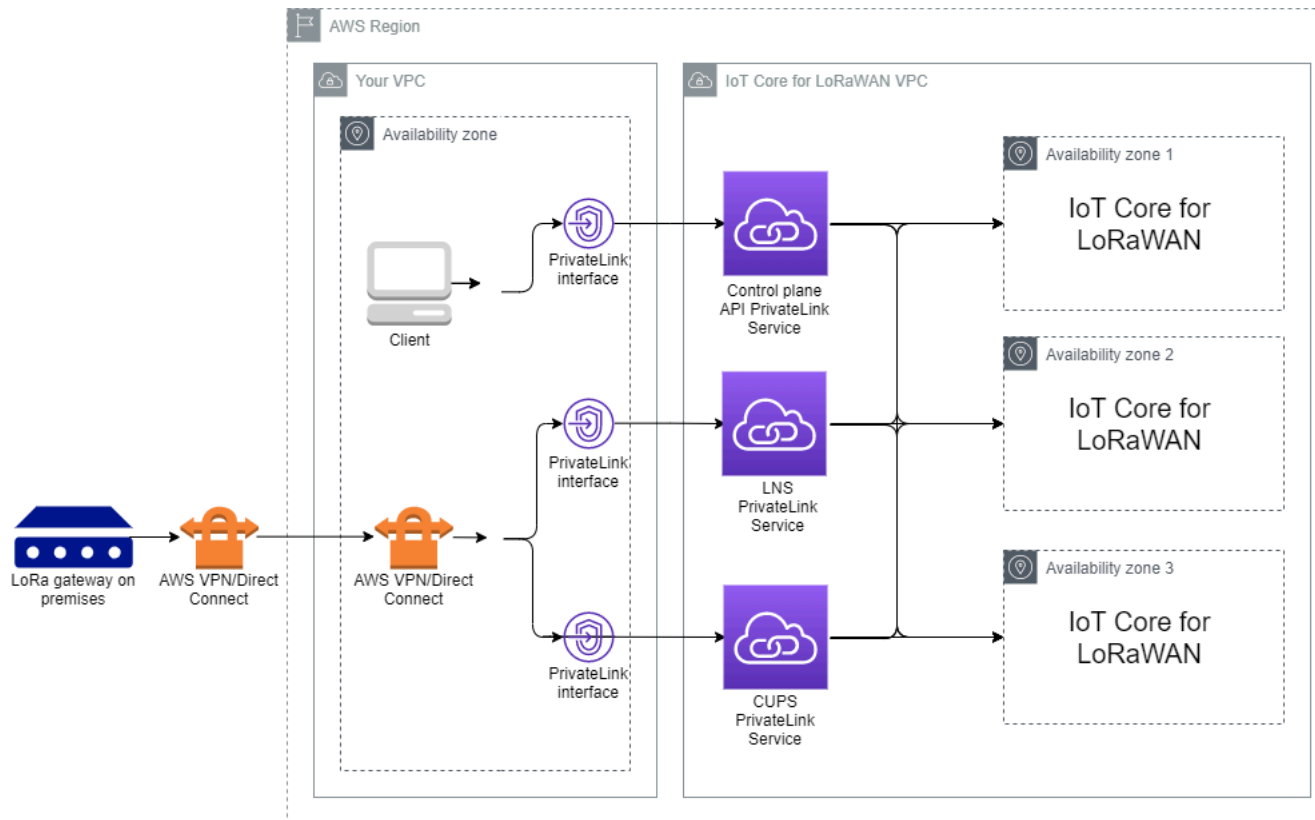
## Considerações sobre os endpoints da VPC do AWS IoT Wireless

Antes de configurar um endpoint da VPC de interface para o AWS IoT Wireless, leia [Interface endpoint properties and limitations](#) no Guia do usuário do Amazon VPC.

O AWS IoT Wireless permite chamadas para todas as ações de API da VPC. As políticas de endpoint da VPC não são compatíveis com o AWS IoT Wireless. Por padrão, o acesso completo ao AWS IoT Wireless é permitido pelo endpoint. Para obter mais informações, consulte [Controlar o acesso a serviços com endpoints da VPC](#) no Guia do usuário da Amazon VPC.

## Arquitetura de link privado do AWS IoT Core for LoRaWAN

O diagrama a seguir mostra a arquitetura de link privado do AWS IoT Core for LoRaWAN. A arquitetura usa um Transit Gateway e um Route 53 Resolver para compartilhar os endpoints de interface do AWS PrivateLink entre a VPC, a VPC do AWS IoT Core for LoRaWAN e um ambiente on-premises. Você encontrará um diagrama de arquitetura mais detalhado ao configurar a conexão com os endpoints da VPC de interface.



## Endpoints do AWS IoT Core for LoRaWAN

O AWS IoT Core for LoRaWAN tem três endpoints públicos. Cada endpoint público tem um endpoint da VPC de interface correspondente. Os endpoints públicos podem ser classificados em endpoints de ambiente de gerenciamento e de plano de dados. Para obter mais informações sobre esses endpoints, consulte [Endpoints da API AWS IoT Core for LoRaWAN](#).

- Endpoints da API do ambiente de gerenciamento

Você pode usar endpoints de API do ambiente de gerenciamento para interagir com as APIs AWS IoT Wireless. Esses endpoints podem ser acessados a partir de um cliente hospedado na Amazon VPC usando AWS PrivateLink.

- Endpoints de API do plano de dados

Os endpoints de API do plano de dados são os endpoints do Servidor da Rede LoRaWAN (LNS) e do Servidor de Configuração e Atualização (CUPS) que você pode usar para interagir com os endpoints LNS e CUPS do AWS IoT Core for LoRaWAN. Esses endpoints podem ser acessados dos gateways LoRa on-premises usando a Site-to-Site VPN ou AWS Direct Connect. Você

obtem esses endpoints ao integrar o gateway ao AWS IoT Core for LoRaWAN. Para ter mais informações, consulte [Adicionar um gateway ao AWS IoT Core for LoRaWAN](#).

## Tópicos

- [Endpoint de API do ambiente de gerenciamento do AWS IoT Core for LoRaWAN integrado](#)
- [Endpoints de API do plano de dados AWS IoT Core for LoRaWAN integrados](#)

## Endpoint de API do ambiente de gerenciamento do AWS IoT Core for LoRaWAN integrado

Você pode usar os endpoints de API do ambiente de gerenciamento do AWS IoT Core for LoRaWAN para interagir com as APIs AWS IoT Wireless. Por exemplo, você pode usar esse endpoint para executar a API [SendDataToWirelessDevice](#) para enviar dados da AWS IoT para o dispositivo LoRaWAN. Para obter mais informações, consulte [Endpoints da API do ambiente de gerenciamento do AWS IoT Core for LoRaWAN](#).

Você pode usar o cliente hospedado na Amazon VPC para acessar os endpoints do ambiente de gerenciamento que são desenvolvidos pelo AWS PrivateLink. Esses endpoints podem ser usados para você se conectar à API AWS IoT Wireless por meio de um endpoint de interface na nuvem privada virtual (VPC) em vez de se conectar pela Internet pública.

Para integrar o endpoint do ambiente de gerenciamento:

- [Crie sua Amazon VPC e sub-rede](#)
- [Execute uma instância do Amazon EC2 na sub-rede](#)
- [Criar endpoint de interface da Amazon VPC](#)
- [Testar a conexão com o endpoint da interface](#)

## Crie sua Amazon VPC e sub-rede

Antes de se conectar ao endpoint da interface, você deve criar uma VPC e uma sub-rede. Em seguida, você iniciará uma instância do EC2 em sua sub-rede, que poderá ser usada para se conectar ao endpoint da interface.

Para criar a VPC:

1. Navegue até a página [VPCs](#) do console da Amazon VPC e escolha Criar VPC.

## 2. Na página Criar VPC:

- Insira um nome para a Tag de nome da VPC - opcional (por exemplo, **VPC-A**).
- Insira um intervalo de endereço IPv4 para a VPC no bloco CIDR IPv4 (por exemplo, **10.100.0.0/16**).

## 3. Mantenha os valores padrão para outros campos e escolha Criar VPC.

Para criar sua sub-rede:

### 1. Navegue até a página [Sub-redes](#) do console da Amazon VPC e escolha Criar sub-rede.

### 2. Na página Criar sub-rede:

- Para ID da VPC, escolha a VPC criada anteriormente (por exemplo, VPC-A).
- Insira um nome em Nome da sub-rede (por exemplo, **Private subnet**).
- Escolha a Zona de disponibilidade para sua sub-rede.
- Insira o bloco de endereço IP da sub-rede em Bloco CIDR IPv4 no formato CIDR (por exemplo, **10.100.0.0/24**).

### 3. Para criar uma sub-rede e adicioná-la à VPC, escolha Criar sub-rede.

Para obter mais informações, consulte [Trabalhar com VPCs e sub-redes](#).

## Execute uma instância do Amazon EC2 na sub-rede

Para executar uma instância EC2:

### 1. Navegue até o console do [Amazon EC2](#) e escolha Executar instância.

### 2. Para AMI, escolha Amazon Linux 2 AMI (HVM), Tipo de volume SSD e, em seguida, escolha o tipo de instância t2 micro. Para configurar os detalhes da instância, escolha Próximo.

### 3. Na página Configurar detalhes da instância:

- Para Rede, escolha a VPC criada anteriormente (por exemplo, VPC-A).
- Para Sub-rede, escolha a sub-rede criada anteriormente (por exemplo, **Private subnet**).
- Para Perfil do IAM, escolha o perfil AWSIoTWirelessFullAccess para conceder a política de acesso total ao AWS IoT Core for LoRaWAN. Para obter mais informações, consulte [Resumo da política de AWSIoTWirelessFullAccess](#).
- Para Assumir IP privado, use um endereço IP, por exemplo, 10.100.0.42.

4. Escolha Próximo: adicionar armazenamento e, depois, escolha Próximo: adicionar tags. Se quiser, você pode adicionar qualquer tag para associar à instância do EC2. Escolha Próximo: configurar grupo de segurança.
5. Na página Configurar grupo de segurança, configure o grupo de segurança para permitir:
  - Abrir Todo o TCP para código-fonte como `10.200.0.0/16`.
  - Abrir Todo o ICMP - IPV4 para código-fonte como `10.200.0.0/16`.
6. Para revisar os detalhes da instância e iniciar sua instância do EC2, escolha Revisar e iniciar.

Para obter mais informações, consulte [Introdução às instâncias do Amazon EC2 Linux](#).

## Criar endpoint de interface da Amazon VPC

É possível criar um endpoint para a VPC, que pode ser acessada pela API do EC2. Para criar o endpoint:

1. Navegue até o console [Endpoints da VPC](#) e escolha Criar endpoint.
2. Na página Criar endpoint, especifique as seguintes informações.
  - Escolha AWS service (Serviço da AWS)s para a Categoria de serviço.
  - Para Nome do serviço, pesquise inserindo a palavra-chave **iotwireless**. Na lista de serviços `iotwireless` exibida, escolha o endpoint da API do ambiente de gerenciamento para sua região. O endpoint será do formato `com.amazonaws.region.iotwireless.api`.
  - Para VPC e Sub-redes, escolha a VPC em que deseja criar o endpoint e as Zonas de disponibilidade (AZs) nas quais deseja criar a rede do endpoint.

### Note

O serviço `iotwireless` talvez não seja compatível com todas as Zonas de disponibilidade.

- Em Ativar nome DNS, escolha Ativar para este endpoint.

A escolha dessa opção resolverá de forma automática o DNS e criará uma rota em Amazon Route 53 Public Data Plane para que as APIs usadas depois para testar a conexão passem pelos endpoints do privatelink.

- Em Grupo de segurança, selecione os grupos de segurança a serem associados às interfaces de rede do endpoint.

- Se quiser, adicione ou remova tags. As tags são pares de nome-valor usados para associar ao seu endpoint.

3. Para criar um endpoint da VPC, selecione Criar endpoint.

## Testar a conexão com o endpoint da interface

Você pode usar um SSH para acessar sua instância do Amazon EC2 e, em seguida, usar a AWS CLI para se conectar aos endpoints da interface do privatelink.

Antes de se conectar ao endpoint da interface, baixe a versão mais recente da AWS CLI seguindo as instruções descritas em [Instalação, atualização e desinstalação da versão 2 da AWS CLI no Linux](#).

Os exemplos a seguir mostram como você pode testar sua conexão com o endpoint da interface usando a CLI.

```
aws iotwireless create-service-profile \  
  --endpoint-url https://api.iotwireless.region.amazonaws.com \  
  --name='test-privatelink'
```

A opção a seguir mostra um exemplo de execução do comando.

```
Response:  
{  
  "Arn": "arn:aws:iotwireless:region:acct_number:ServiceProfile/1a2345ba-4c5d-67b0-ab67-  
e0c8342f2857",  
  "Id": "1a2345ba-4c5d-67b0-ab67-e0c8342f2857"  
}
```

Da mesma forma, você pode executar os comandos a seguir para obter as informações do perfil de serviço ou listar todos os perfis de serviço.

```
aws iotwireless get-service-profile \  
  --endpoint-url https://api.iotwireless.region.amazonaws.com  
  --id="1a2345ba-4c5d-67b0-ab67-e0c8342f2857"
```

A opção a seguir mostra um exemplo do comando list-device-profiles.

```
aws iotwireless list-device-profiles \  
  --endpoint-url https://api.iotwireless.region.amazonaws.com
```

## Endpoints de API do plano de dados AWS IoT Core for LoRaWAN integrados

Os endpoints do plano de dados AWS IoT Core for LoRaWAN consistem nos seguintes endpoints. Você obtém esses endpoints ao adicionar um gateway ao AWS IoT Core for LoRaWAN. Para ter mais informações, consulte [Adicionar um gateway ao AWS IoT Core for LoRaWAN](#).

- Endpoints do Servidor da rede LoRaWAN (LNS)

Os endpoints do LNS são do formato *account-specific-prefix*.lns.lorawan.region.amazonaws.com. Você pode usar esse endpoint para estabelecer uma conexão para trocar mensagens de uplink e downlink LoRa.

- Endpoints do Servidor de configuração e atualização (CUPS)

Os endpoints do CUPS são do formato *account-specific-prefix*.cups.lorawan.region.amazonaws.com. Você pode usar esse endpoint para gerenciamento de credenciais, configuração remota e atualização de firmware de gateways.

Para ter mais informações, consulte [Usar protocolos CUPS e LNS](#).

Para encontrar endpoints de API do plano de dados para a Conta da AWS e região, use o comando da CLI [get-service-endpoint](#) mostrado aqui ou a API REST [GetServiceEndpoint](#). Para obter mais informações, consulte [Endpoints da API do plano de dados do AWS IoT Core for LoRaWAN](#).

Você pode conectar seu gateway LoRaWAN on-premises para se comunicar com os endpoints do AWS IoT Core for LoRaWAN. Para estabelecer essa conexão, primeiro conecte seu gateway on-premises à sua Conta da AWS no VPC usando uma conexão VPN. Em seguida, você pode se comunicar com os endpoints da interface do plano de dados na VPC do AWS IoT Core for LoRaWAN que são desenvolvidos pelo privatelink.

As opções a seguir mostram como integrar esses endpoints.

- [Crie um endpoint de interface de VPC e uma zona hospedada privada](#)
- [Use VPN para conectar gateways LoRa à sua Conta da AWS](#)

### Crie um endpoint de interface de VPC e uma zona hospedada privada

O AWS IoT Core for LoRaWAN tem dois endpoints do plano de dados, endpoint Servidor de configuração e atualização (CUPS) e endpoint Servidor da Rede LoRaWAN (LNS). O processo

de configuração para estabelecer uma conexão de privatelink com os dois endpoints é o mesmo. Portanto, podemos usar o endpoint do LNS para fins ilustrativos.

Para os endpoints do plano de dados, os gateways LoRa primeiro se conectam à sua Conta da AWS na Amazon VPC, que, então, se conecta ao endpoint da VPC na VPC do AWS IoT Core for LoRaWAN.

Ao se conectar aos endpoints, os nomes DNS podem ser resolvidos em uma VPC, mas não podem ser resolvidos em várias VPCs. Para desativar o DNS privado ao criar o endpoint, desative a configuração Ativar nome DNS. É possível usar uma zona hospedada privada para fornecer informações sobre como você deseja que Route 53 responda às consultas ao DNS de suas VPCs. Para compartilhar a VPC com um ambiente on-premises, você pode usar um Route 53 Resolver para facilitar o DNS híbrido.

Para concluir este procedimento, execute as seguintes etapas.

- [Crie uma Amazon VPC e uma sub-rede](#)
- [Crie um endpoint de interface da Amazon VPC](#)
- [Configurar zona hospedada privada](#)
- [Configurar o resolvidor de entrada do Route 53](#)
- [Próximas etapas](#)

Crie uma Amazon VPC e uma sub-rede

Você pode reutilizar uma Amazon VPC e a sub-rede criada ao integrar o endpoint do ambiente de gerenciamento. Para ter mais informações, consulte [Crie sua Amazon VPC e sub-rede](#).

Crie um endpoint de interface da Amazon VPC

Você pode criar um endpoint da VPC para uma VPC, que é semelhante à forma como você criaria um para o endpoint do ambiente de gerenciamento.

1. Navegue até o console [Endpoints da VPC](#) e escolha Criar endpoint.
2. Na página Criar endpoint, especifique as seguintes informações.
  - Escolha AWS service (Serviço da AWS)s para a Categoria de serviço.
  - Para Nome do serviço, pesquise inserindo a palavra-chave **lns**. Na lista de serviços Lns exibida, escolha o endpoint da API do plano de dados do LNS para a região. O endpoint será do formato com `.amazonaws.region.lorawan.lns`.

**Note**

Se você estiver seguindo esse procedimento para o endpoint do CUPS, pesquise por cups. O endpoint será do formato `com.amazonaws.region.lorawan.cups`.

- Para VPC e Sub-redes, escolha a VPC em que deseja criar o endpoint e as Zonas de disponibilidade (AZs) nas quais deseja criar a rede do endpoint.

**Note**

O serviço `iotwireless` talvez não seja compatível com todas as Zonas de disponibilidade.

- Em Ativar nome DNS, certifique-se de que a opção Ativar para este endpoint não esteja selecionada.

Ao não selecionar esta opção, você pode desativar o DNS privado para o endpoint da VPC e, em vez disso, usar a zona hospedada privada.

- Em Grupo de segurança, selecione os grupos de segurança a serem associados às interfaces de rede do endpoint.
- Se quiser, adicione ou remova tags. As tags são pares de nome-valor usados para associar ao seu endpoint.

### 3. Para criar um endpoint da VPC, selecione Criar endpoint.

#### Configurar zona hospedada privada


Depois de criar o endpoint de privatelink, na guia Detalhes do endpoint, você verá uma lista de nomes DNS. Você pode usar um desses nomes DNS para configurar a zona hospedada privada. O nome DNS terá o formato `vpce-xxxx.ins.lorawan.region.vpce.amazonaws.com`.

#### Criar a zona hospedada privada

Para criar a zona hospedada privada:

1. Navegue até o console de Zonas hospedadas do [Route 53](#) e escolha Criar zona hospedada.
2. Na página Criar zona hospedada, especifique as seguintes informações.

- Em Nome do domínio, insira o nome completo do serviço para o endpoint do LNS, **lns.lorawan.region.amazonaws.com**.

 Note

Se você estiver seguindo esse procedimento para o endpoint do CUPS, insira **cups.lorawan.region.amazonaws.com**.

- Em Tipo, escolha Zona hospedada privada.
  - Opcionalmente, você pode adicionar ou remover tags para associar à zona hospedada.
3. Para criar a zona hospedada privada, escolha Criar zona hospedada.

Para ver mais informações, consulte [Criar uma zona hospedada privada](#).

Depois de criar uma zona hospedada privada, é possível criar um registro que informe ao DNS como você deseja que o tráfego seja direcionado para esse domínio.

### Criar um registro

Depois de criar uma zona hospedada privada, é possível criar um registro que informe ao DNS como você deseja que o tráfego seja direcionado para esse domínio. Para criar um registro:

1. Na lista de zonas hospedadas exibida, escolha a zona hospedada privada que você criou antes e escolha Criar registro.
2. Use o método do assistente para criar o registro. Se o console apresentar o método de Criação rápida, escolha Alternar para assistente.
3. Escolha Roteamento simples em Política de roteamento e, em seguida, Próximo.
4. Na página Configurar registros, escolha Definir registro simples.
5. Na página Definir registro simples:
  - Em Nome do registro, insira o alias do número da sua Conta da AWS. Você obtém esse valor ao integrar o gateway ou ao usar a API REST [GetServiceEndpoint](#).
  - Em Tipo de registro, mantenha o valor como A - Routes traffic to an IPv4 address and some AWS resources.
  - Em Valor/rotear tráfego para, escolha Alias para VPC endpoint. Em seguida, escolha sua região e o endpoint que você criou anteriormente, conforme descrito em [Crie um endpoint de interface da Amazon VPC](#) na lista de endpoints exibida.

## 6. Escolha Definir registro simples para criar um registro.

### Configurar o resolvedor de entrada do Route 53

Para compartilhar o endpoint da VPC com um ambiente on-premises, você pode usar um Route 53 Resolver para facilitar o DNS híbrido. O resolvedor de entrada permitirá que você roteie o tráfego da rede on-premises para os endpoints do plano de dados sem passar pela Internet pública. Para retornar os valores do endereço IP privado do serviço, crie o Route 53 Resolver na mesma VPC do endpoint da VPC.

Ao criar o resolvedor de entrada, você só precisa especificar a VPC e as sub-redes que você criou antes nas Zonas de Disponibilidade (AZs). O Route 53 Resolver usa essas informações para atribuir de modo automático um endereço IP para rotear o tráfego para cada uma das sub-redes.

Para criar o resolvedor de entrada:

1. Navegue até o console [Endpoints de entrada do](#) Route 53 e escolha Criar endpoint de entrada.

#### Note

Verifique se você está usando a mesma Região da AWS que usou ao criar o endpoint e a zona hospedada privada.

2. Na página Criar endpoint de entrada, especifique as seguintes informações.
  - Insira um nome em Nome do endpoint (por exemplo, **VPC\_A\_Test**).
  - Para VPC na região, escolha a mesma VPC que você usou ao criar o endpoint da VPC.
  - Configure o Grupo de segurança desse endpoint para permitir o tráfego de entrada da rede on-premises.
  - Em Endereço IP, escolha Usar um endereço IP selecionado automaticamente.
3. Escolha Enviar para criar o resolvedor de entrada.

Neste exemplo, vamos supor que os endereços IP `10.100.0.145` e `10.100.192.10` foram atribuídos ao Route 53 Resolver de entrada para o roteamento do tráfego.

## Próximas etapas

Você criou a zona hospedada privada e um resolvedor de entrada para rotear o tráfego para as entradas de DNS. Agora é possível usar um Site-to-Site VPN ou um endpoint do Client VPN. Para ter mais informações, consulte [Use VPN para conectar gateways LoRa à sua Conta da AWS](#).

## Use VPN para conectar gateways LoRa à sua Conta da AWS

Para conectar gateways on-premises à Conta da AWS, é possível usar uma conexão do Site-to-Site VPN ou um endpoint do Client VPN.

Antes de conectar gateways on-premises, você deve ter criado o endpoint da VPC e configurado uma zona hospedada privada e um resolvedor de entrada para que o tráfego dos gateways não passe pela Internet pública. Para ter mais informações, consulte [Crie um endpoint de interface de VPC e uma zona hospedada privada](#).

### Endpoint do Site-to-Site VPN

Se não tiver o hardware do gateway ou quiser testar a conexão VPN usando uma Conta da AWS diferente, você pode usar uma conexão Site-to-Site VPN. Você pode usar o Site-to-Site VPN para se conectar aos endpoints da VPC a partir da mesma Conta da AWS ou de outra Conta da AWS que você esteja usando em uma Região da AWS diferente.

#### Note

Se você tiver o hardware do gateway com você e quiser configurar uma conexão VPN, recomendamos que você use o Client VPN em vez disso. Para obter instruções, consulte [Endpoint do cliente VPN](#).

Para configurar um Site-to-Site VPN:

1. Crie outra VPC no site a partir do qual você deseja configurar a conexão. Em VPC-A, é possível reutilizar a VPC criada antes. Para criar outra VPC (por exemplo, VPC-B), use um bloco CIDR que não se sobreponha ao bloco CIDR da VPC que você criou antes.

Para obter informações sobre como configurar as VPCs, siga as instruções descritas em [Configurar a conexão do Site-to-Site VPN da AWS](#).

**Note**

O método VPN do Site-to-Site VPN descrito no documento usa o OpenSWAN para a conexão VPN, compatível somente com um túnel VPN. Se você usar um software comercial diferente para a VPN, poderá configurar dois túneis entre os sites.

2. Depois de configurar a conexão VPN, atualize o arquivo `/etc/resolv.conf` adicionando o endereço IP do resolvedor de entrada da Conta da AWS. Use esse endereço IP para o servidor de nomes. Para obter informações sobre como obter esse endereço IP, consulte [Configurar o resolvedor de entrada do Route 53](#). Neste exemplo, podemos usar o endereço IP `10.100.0.145` que foi atribuído quando você criou o Route 53 Resolver.

```
options timeout:2 attempts:5
; generated by /usr/sbin/dhclient-script
search region.compute.internal
nameserver 10.100.0.145
```

3. Agora podemos testar se a conexão VPN usa o endpoint AWS PrivateLink em vez de acessar a Internet pública usando um comando `nslookup`. A opção a seguir mostra um exemplo de execução do comando.

```
nslookup account-specific-prefix.lns.lorawan.region.amazonaws.com
```

A opção a seguir mostra um exemplo de saída da execução do comando, que mostra um endereço IP privado indicando que a conexão foi estabelecida com o endpoint do LNS do AWS PrivateLink.

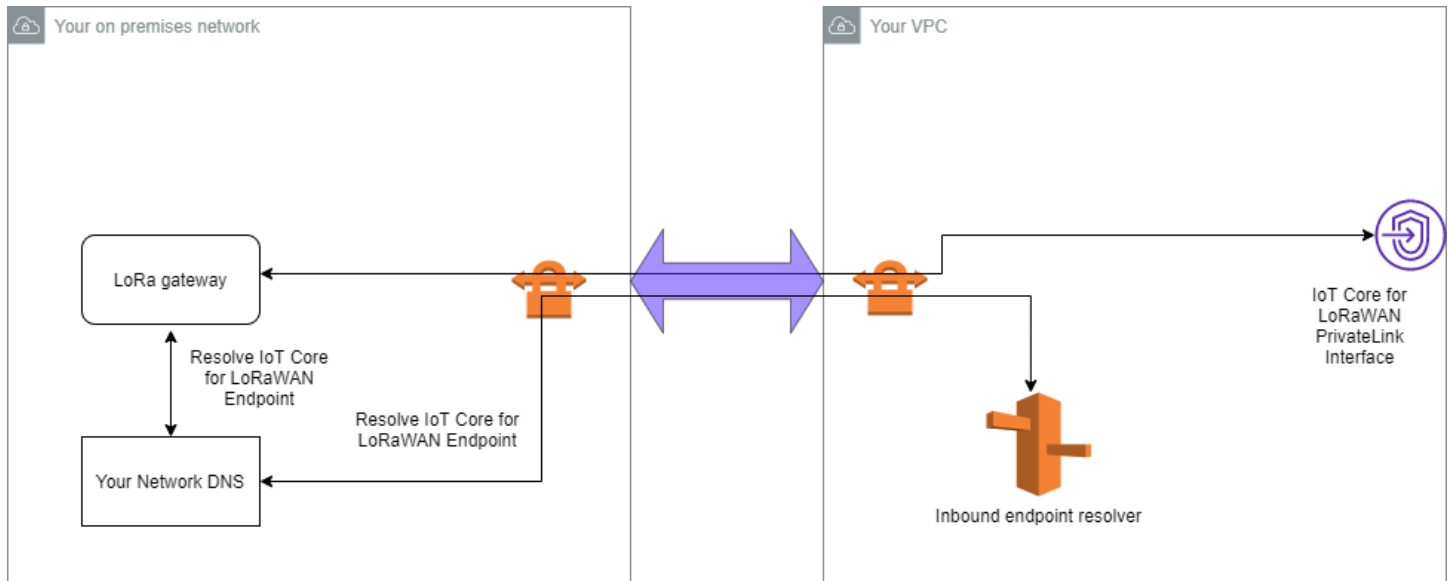
```
Server: 10.100.0.145
Address: 10.100.0.145

Non-authoritative answer:
Name: https://xxxxx.lns.lorawan.region.amazonaws.com
Address: 10.100.0.204
```

Para obter informações sobre como usar uma conexão do Site-to-Site VPN, consulte [Como o Site-to-Site VPN funciona](#).

## Endpoint do cliente VPN

O AWS Client VPN é um serviço de VPN gerenciado com base no cliente que permite que você acesse com segurança recursos da AWS e recursos na rede on-premises. A opção a seguir mostra a arquitetura do serviço Client VPN.



Para estabelecer uma conexão VPN com um endpoint do Client VPN:

1. Crie um endpoint do Client VPN seguindo as instruções descritas em [Introdução ao AWS Client VPN](#).
2. Faça login na rede on-premises (por exemplo, um roteador Wi-Fi) usando o URL de acesso desse roteador (por exemplo, 192.168.1.1) e encontre o nome raiz e a senha.
3. Configure o gateway LoRaWAN seguindo as instruções na documentação do gateway e, em seguida, adicione o gateway ao AWS IoT Core for LoRaWAN. Para obter informações sobre como adicionar o gateway, consulte [Integre os gateways ao AWS IoT Core for LoRaWAN](#).
4. Verifique se o firmware do gateway está atualizado. Se o firmware estiver desatualizado, você poderá seguir as instruções fornecidas na rede on-premises para atualizar o firmware do gateway. Para ter mais informações, consulte [Atualize o firmware do gateway usando o serviço CUPS com AWS IoT Core for LoRaWAN](#).
5. Verifique se o OpenVPN foi ativado. Se tiver sido ativado, vá para a próxima etapa para configurar o cliente OpenVPN dentro da rede on-premises. Se ele não tiver sido ativado, siga as instruções no [Guia para instalar o OpenVPN para OpenWrt](#).

**Note**

Neste exemplo, usamos OpenVPN. Você pode usar outros clientes VPN, como Site-to-Site VPN ou AWS Direct Connect, para configurar a conexão do Client VPN.

6. Configure o cliente OpenVPN com base nas informações da configuração do cliente e em como você pode usar o [cliente OpenVPN usando o LuCi](#).
7. Faça SSH na rede on-premises e atualize o arquivo `/etc/resolv.conf` adicionando o endereço IP do resolvedor de entrada à Conta da AWS (10.100.0.145).
8. Para que o tráfego do gateway use o AWS PrivateLink para se conectar ao endpoint, substitua a primeira entrada DNS do gateway pelo endereço IP do resolvedor de entrada.

Para obter informações sobre como usar uma conexão do Site-to-Site VPN, consulte [Introdução ao Client VPN](#).

Conecte-se aos endpoints da VPC do LNS e do CUPS

A opção a seguir mostra como você pode testar a conexão com os endpoints da VPC do LNS e do CUPS.

Testar o endpoint do CUPS

Para testar a conexão do AWS PrivateLink com o endpoint do CUPS a partir do gateway LoRa, execute o seguinte comando:

```
curl -k -v -X POST https://xxxx.cups.region.iotwireless.iot:443/update-info
  --cacert cups.trust --cert cups.crt --key cups.key --header "Content-Type:
application/json"
  --data '{
    "router": "xxxxxxxxxxxxxx",
    "cupsUri": "https://xxxx.cups.lorawan.region.amazonaws.com:443",
    "cupsCredCrc":1234, "tcCredCrc":552384314
  }'
  -output cups.out
```

Testar o endpoint do LNS

Para testar o endpoint do LNS, primeiro provisione um dispositivo LoRaWAN que funcionará com o gateway sem fio. Em seguida, você pode adicionar o dispositivo e executar o procedimento de junção, após o qual você pode começar a enviar mensagens de uplink.

# AWS IoT Core para Amazon Sidewalk

O AWS IoT Core para Amazon Sidewalk fornece os serviços de nuvem que podem ser utilizados para conectar os dispositivos finais do Sidewalk à Nuvem AWS e utilizar outro AWS service (Serviço da AWS).

O Amazon Sidewalk é uma rede segura e compartilhada que permite que dispositivos em sua comunidade se conectem e permaneçam conectados. O Amazon Sidewalk transfere dados entre os dispositivos finais do Sidewalk e os gateways do Sidewalk e entre os gateways do Sidewalk e a nuvem do Sidewalk.

## Acessar o AWS IoT Core para Amazon Sidewalk

É possível integrar os dispositivos finais do Sidewalk ao AWS IoT utilizando o console ou as operações de API do AWS IoT Wireless. Depois que seus dispositivos são integrados, suas mensagens são enviadas para AWS IoT Core. Em seguida, você pode começar a desenvolver seus aplicativos de negócios na nuvem da AWS, que usa os dados dos seus dispositivos finais do Amazon Sidewalk.

### Usar o console

Para integrar seus dispositivos finais do Sidewalk, faça login no Console de gerenciamento da AWS e navegue até a página [Dispositivos](#) no console de AWS IoT. Depois que seus dispositivos estiverem integrados, você poderá visualizá-los e gerenciá-los nesta página do console de IoT.

### Como usar a API ou a CLI

É possível integrar dispositivos Sidewalk e LoRaWAN utilizando as [operações de API do AWS IoT Wireless](#). A API do AWS IoT Wireless em que o AWS IoT Core se baseia é compatível com o SDK da AWS. Para obter mais informações, consulte [SDKs da AWS e toolkits](#).

Você pode usar a AWS CLI para executar comandos para integrar e gerenciar seus dispositivos finais do Sidewalk. Para obter mais informações, consulte [referência de CLI de AWS IoT Wireless](#).

## AWS IoT Core para regiões e endpoints do Amazon Sidewalk

O Amazon Sidewalk está disponível apenas na Região da AWS us-east-1. O AWS IoT Core para Amazon Sidewalk é compatível com endpoints da API do ambiente de gerenciamento e do plano

de dados nessa região. Os endpoints da API do plano de dados são específicos para sua Conta da AWS. Para obter mais informações, consulte [AWS IoT Wireless Service endpoints](#) na Referência geral da AWS.

O AWS IoT Core para Amazon Sidewalk tem cotas que se aplicam aos dados do dispositivo que são transmitidos entre o dispositivo e a Nuvem AWS e o TPS máximo para as operações da API do AWS IoT Wireless. Para obter mais informações, consulte [AWS IoT Wireless quotas](#), na Referência geral da AWS.

## Preços do AWS IoT Core para Amazon Sidewalk

Ao se cadastrar na AWS, você poderá começar a utilizar o AWS IoT Core gratuitamente utilizando o [nível gratuito da AWS](#).

Para obter informações sobre visão geral do produto e definição de preços, consulte [Preços do AWS IoT Core](#).

## O que é o AWS IoT Core para Amazon Sidewalk?

Com o AWS IoT Core para Amazon Sidewalk, é possível integrar os dispositivos finais do Amazon Sidewalk ao AWS IoT, gerenciá-los e monitorá-los. Ele também gerencia os destinos que enviam dados do dispositivo a outros Serviços da AWS.

## Recursos do AWS IoT Core para Amazon Sidewalk

Ao utilizar o AWS IoT Core para Amazon Sidewalk, é possível:

- Integrar os dispositivos finais do Sidewalk ao AWS IoT utilizando o console do AWS IoT, as operações de API do AWS IoT Core para Amazon Sidewalk ou os comandos da AWS CLI.
- Aproveite os recursos oferecidos pela Nuvem AWS.
- Crie um destino que use regras de AWS IoT para processar mensagens de payload recebidas e interagir com outros Serviços da AWS.
- Ative as notificações de eventos para receber mensagens sobre eventos, como quando seu dispositivo final do Sidewalk foi provisionado ou registrado, ou se uma mensagem de downlink foi entregue com sucesso ao seu dispositivo.
- Registre e monitore seus dispositivos finais do Sidewalk em tempo real, obtenha informações úteis e identifique e solucione erros.

- Associe seus dispositivos finais do Sidewalk a um objeto de AWS IoT, que ajude você a armazenar uma representação do seu dispositivo na nuvem. Os objetos no AWS IoT facilitam a pesquisa e o gerenciamento de seus atributos e o acesso a outros atributos AWS IoT Core.

Os tópicos a seguir ajudarão você a conhecer o Amazon Sidewalk e o AWS IoT Core para Amazon Sidewalk.

## Tópicos

- [O que é o Amazon Sidewalk?](#)
- [Como funciona o AWS IoT Core para Amazon Sidewalk](#)

## O que é o Amazon Sidewalk?

O Amazon Sidewalk é uma rede comunitária segura que usa o Amazon Sidewalk Bridges, como dispositivos Amazon Echo e Ring compatíveis, para fornecer conectividade em nuvem para dispositivos de IoT. O Amazon Sidewalk permite conectividade de baixa largura de banda e longo alcance em casa e fora dela usando Bluetooth LE para comunicação de curta distância e protocolos de rádio LoRa e FSK em frequências de 900 MHz para cobrir distâncias maiores.

Quando o Amazon Sidewalk está ativado, essa rede é compatível com outros dispositivos finais do Sidewalk em sua comunidade e pode ser usada para aplicações como detectar seu ambiente. O Amazon Sidewalk ajuda seus dispositivos a se conectarem e permanecerem conectados.

## Atributos do Amazon Sidewalk

Estes são os atributos do Amazon Sidewalk.

- O Amazon Sidewalk cria uma rede de baixa largura de banda usando gateways do Sidewalk que incluem dispositivos Ring e alguns dispositivos Echo. Usando gateways, você pode compartilhar uma parte da largura de banda da Internet, que é usada para conectar seus dispositivos finais à rede.
- O Amazon Sidewalk oferece um mecanismo de rede seguro com várias camadas de criptografia e segurança.
- O Amazon Sidewalk oferece um mecanismo simples para ativar ou desativar a participação no Sidewalk.

## Conceitos do Amazon Sidewalk

Veja a seguir alguns dos principais conceitos do Amazon Sidewalk.

### Gateways do Sidewalk

Os gateways do Sidewalk, ou pontes do Amazon Sidewalk, roteiam os dados entre seus dispositivos finais do Sidewalk e a nuvem. Os gateways são dispositivos da Amazon, como o dispositivo Echo ou a Ring Floodlight Cam, compatíveis com subG-CSS (assíncrono, LDR), subG-FSK (síncrono, HDR) ou Bluetooth LE para comunicação no Sidewalk. Os gateways do Sidewalk compartilham uma parte da largura de banda da Internet com a comunidade do Sidewalk para fornecer conectividade a um grupo de dispositivos compatíveis com o Sidewalk.

### Dispositivos finais do Sidewalk

Os dispositivos finais do Sidewalk usam o roaming do Amazon Sidewalk conectando-se aos gateways do Sidewalk. Os dispositivos finais são produtos inteligentes de baixa largura de banda e baixo consumo de energia, como luzes habilitadas para Sidewalk ou fechaduras de portas.

#### Note

Certos gateways do Sidewalk também podem atuar como dispositivos finais.

### Servidor de rede do Sidewalk

O servidor de rede do Sidewalk, operado pela Amazon, verifica os pacotes recebidos e encaminha as mensagens de uplink e downlink para o destino desejado, mantendo o horário da rede Sidewalk sincronizado.

## Saiba mais sobre o Amazon Sidewalk

Para obter mais informações sobre o Amazon Sidewalk, consulte as seguintes páginas da web:

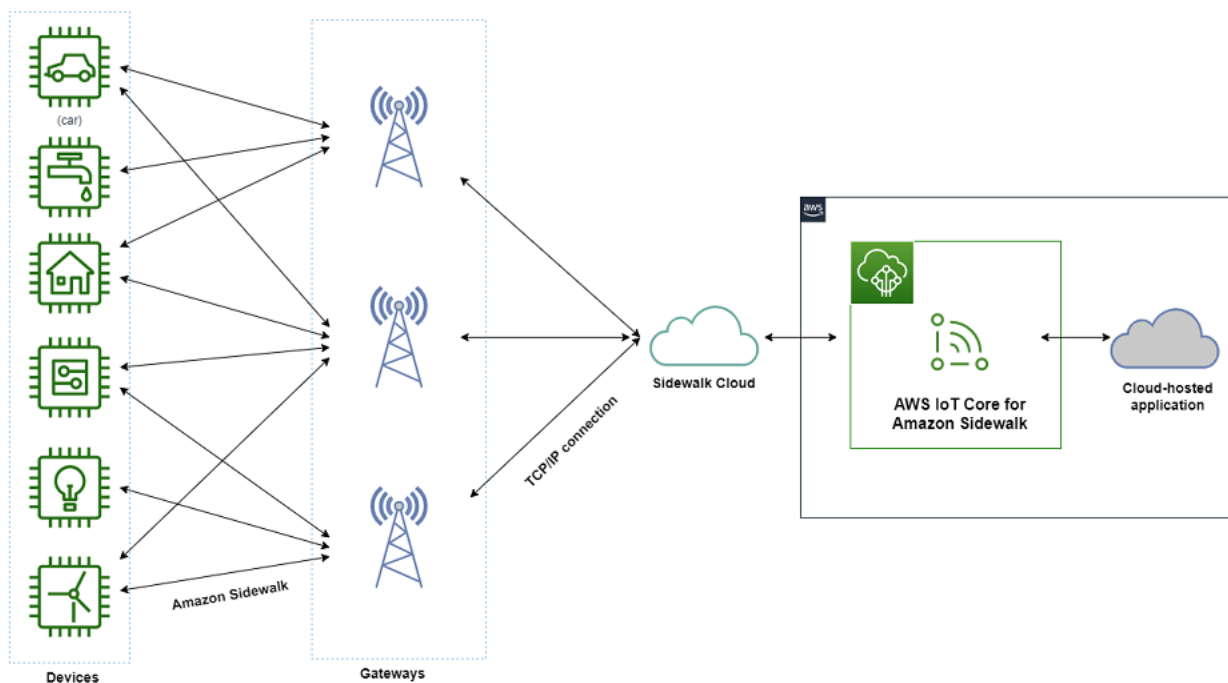
- [Amazon Sidewalk](#)
- [Documentação do Amazon Sidewalk](#)
- [AWS IoT Core para Amazon Sidewalk](#)

## Como funciona o AWS IoT Core para Amazon Sidewalk

Com o AWS IoT Core para Amazon Sidewalk, é possível integrar os dispositivos finais do Amazon Sidewalk ao AWS IoT, gerenciá-los e monitorá-los. Ele também gerencia os destinos que enviam dados do dispositivo para outros AWS service (Serviço da AWS)

O AWS IoT Core para Amazon Sidewalk fornece os serviços de nuvem que podem ser utilizados para conectar os dispositivos finais do Sidewalk à Nuvem AWS e utilizar outro AWS service (Serviço da AWS). Também é possível utilizar o AWS IoT Core para Amazon Sidewalk para gerenciar dispositivos Sidewalk, monitorar e criar aplicações neles.

Os dispositivos finais do Sidewalk se comunicam com o AWS IoT Core por meio de gateways do Sidewalk. O AWS IoT Core para Amazon Sidewalk gerencia as políticas de serviços e de dispositivos que o AWS IoT Core exige para gerenciar e se comunicar com os dispositivos finais e gateways do Sidewalk. Ele também gerencia os destinos que enviam dados do dispositivo para outros AWS service (Serviço da AWS).



## Como começar a utilizar o AWS IoT Core para Amazon Sidewalk

É possível utilizar o console do AWS IoT, a API do AWS IoT Core para Amazon Sidewalk ou a AWS CLI para criar e integrar dispositivos finais do Sidewalk e conectá-los à rede do Sidewalk. Para obter informações sobre os conceitos básicos do Amazon Sidewalk e a integração de dispositivos finais ao AWS IoT, consulte os seguintes tópicos.

- [Conceitos básicos do AWS IoT Core para Amazon Sidewalk](#)

Este tópico aborda os pré-requisitos para integrar seus dispositivos finais do Sidewalk, ilustra o fluxo de trabalho usando um aplicativo de monitoramento de sensores e fornece uma visão geral de como integrar seu dispositivo usando comandos da AWS CLI.

- [Conectar-se ao AWS IoT Core para Amazon Sidewalk](#)

Esta seção descreve as diferentes etapas na introdução do fluxo de trabalho de integração e explica a integração de seus dispositivos finais usando o console e as operações de API. Também será possível conectar o dispositivo e visualizar as mensagens trocadas entre o dispositivo e o AWS IoT Core para Amazon Sidewalk.

- [Provisionamento em massa de dispositivos com o AWS IoT Core para Amazon Sidewalk](#)

Esta seção fornece um tutorial detalhado e gradual para o provisionamento em massa dos dispositivos finais do Sidewalk utilizando o AWS IoT Core para Amazon Sidewalk. Você aprenderá o fluxo de trabalho de provisionamento em massa e como integrar um grande número de dispositivos do Sidewalk.

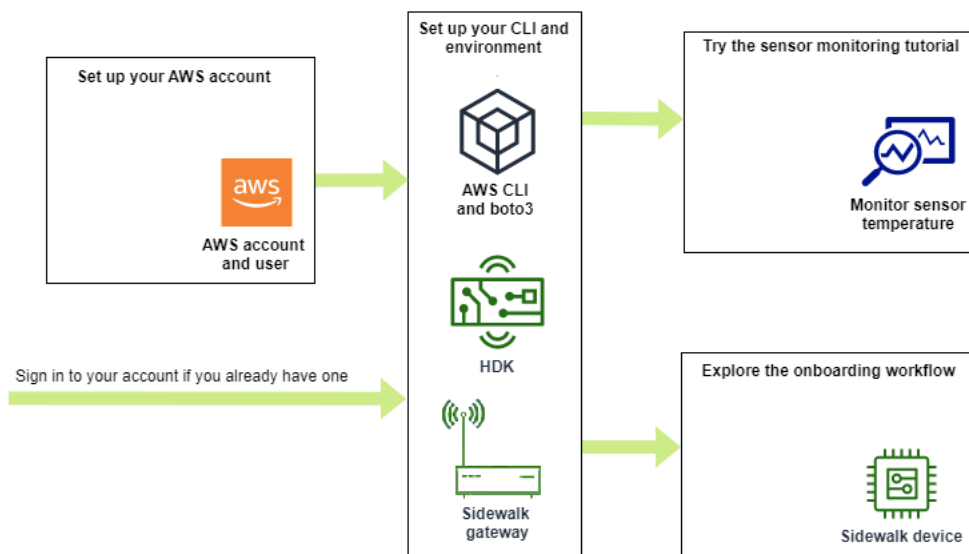
## Saiba mais sobre o AWS IoT Core para Amazon Sidewalk

Para obter mais informações sobre o AWS IoT Core para Amazon Sidewalk, consulte as seguintes páginas da web:

- [Amazon Sidewalk](#)
- [Documentação do Amazon Sidewalk](#)
- [AWS IoT Core para Amazon Sidewalk](#)

## Conceitos básicos do AWS IoT Core para Amazon Sidewalk

Esta seção mostra como começar a conectar os dispositivos finais do Sidewalk ao AWS IoT Core para Amazon Sidewalk. Ele explica como você pode conectar um dispositivo final ao Amazon Sidewalk e passar mensagens entre eles. Você também aprenderá sobre a aplicação de exemplo do Sidewalk e uma visão geral de como executar o monitoramento de sensores utilizando o AWS IoT Core para Amazon Sidewalk. O aplicativo de amostra fornece um painel para visualizar e monitorar as alterações na temperatura do sensor.



Os tópicos a seguir ajudarão você a começar a usar o AWS IoT Core para Amazon Sidewalk.

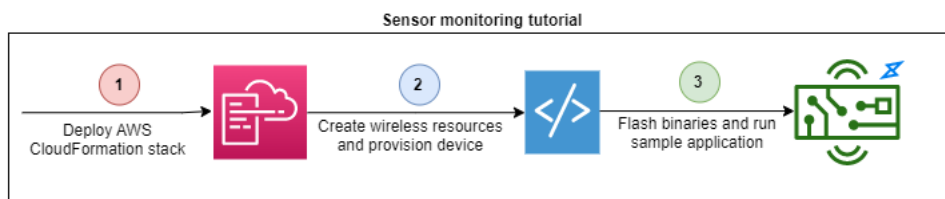
## Tópicos

- [Experimente o tutorial de monitoramento de sensores](#)
- [Introdução à integração de seus dispositivos do Sidewalk](#)

## Experimente o tutorial de monitoramento de sensores

Esta seção fornece uma visão geral do aplicativo de amostra do Amazon Sidewalk no GitHub que mostra como monitorar a temperatura de um sensor. Neste tutorial, você usa scripts que criam programaticamente os recursos sem fio necessários, provisionam o dispositivo final e instalam os binários e, em seguida, conectam seu dispositivo final ao aplicativo. Os scripts que usam os comandos AWS CLI e Python criam recursos sem fio e uma pilha AWS CloudFormation e, em seguida, atualizam os binários e implantam o aplicativo em seu kit de desenvolvimento de hardware (HDK).

O diagrama a seguir mostra as etapas envolvidas quando você executa o [aplicativo de amostra](#) e conecta seu dispositivo final Sidewalk ao aplicativo. Para obter instruções detalhadas, incluindo pré-requisitos e configuração para este tutorial, consulte o [documento README](#) no GitHub.



## Introdução à integração de seus dispositivos do Sidewalk

Esta seção mostra como integrar os dispositivos finais do Sidewalk ao AWS IoT Core para Amazon Sidewalk. Para integrar seus dispositivos, primeiro adicione seu dispositivo do Sidewalk, depois provisione e registre seu dispositivo e, em seguida, conecte seu hardware ao aplicativo em nuvem. Antes de executar este tutorial, revise e conclua [Instalar o Python e a AWS CLI](#).

As etapas a seguir mostram como integrar e conectar os dispositivos finais do Sidewalk ao AWS IoT Core para Amazon Sidewalk. Se você quiser integrar dispositivos usando a AWS CLI, consulte os exemplos de comandos fornecidos nesta seção. Para obter informações sobre a integração de dispositivos usando o console de AWS IoT, consulte [Conectar-se ao AWS IoT Core para Amazon Sidewalk](#).

### Important

Para realizar todo o fluxo de trabalho de integração, você também provisiona e registra seu dispositivo final e conecta seu kit de desenvolvimento de hardware (HDK). Para obter mais informações, consulte [Provisionamento e registro do seu dispositivo final](#) na documentação do Amazon Sidewalk.

### Tópicos

- [Etapa 1: Adicionar o dispositivo Sidewalk ao AWS IoT Core para Amazon Sidewalk](#)
- [Etapa 2: Criar um destino para seu dispositivo final do Sidewalk](#)
- [Etapa 3: Provisionar e registrar o dispositivo final](#)
- [Etapa 4: Conectar-se ao dispositivo final do Sidewalk e trocar mensagens](#)

### Etapa 1: Adicionar o dispositivo Sidewalk ao AWS IoT Core para Amazon Sidewalk

Veja a seguir uma visão geral das etapas que você executará para adicionar o dispositivo final do Sidewalk ao AWS IoT Core para Amazon Sidewalk. Armazene as informações obtidas sobre o perfil do dispositivo e o dispositivo sem fio que você cria. Você usará essas informações para provisionar e registrar o dispositivo final. Para mais informações sobre essas etapas, consulte [Adicionar o dispositivo ao AWS IoT Core para Amazon Sidewalk](#).

## 1. Criar um perfil do dispositivo

Crie um perfil de dispositivo que contenha as configurações compartilhadas para seus dispositivos do Sidewalk. Ao criar o perfil, especifique um *name* para o perfil como uma sequência alfanumérica. Para criar um perfil, vá até a [guia Sidewalk do hub Perfis](#) no console de AWS IoT e escolha Criar perfil, ou use a operação da API [CreateDeviceProfile](#) ou o comando da CLI [create-device-profile](#), conforme mostrado neste exemplo.

```
// Add your device profile using a name and the sidewalk object.  
aws iotwireless create-device-profile --name sidewalk_profile --sidewalk {}
```

## 2. Crie seu dispositivo final do Sidewalk

Crie o dispositivo final do Sidewalk com o AWS IoT Core para Amazon Sidewalk. Especifique um nome de destino e a ID do perfil do dispositivo obtido na etapa anterior. Para adicionar um dispositivo, vá até a [guia Sidewalk do hub Dispositivos](#) no console de AWS IoT e escolha Provisionar dispositivo, ou use a operação da API [CreateWirelessDevice](#) ou o comando da CLI [create-wireless-device](#), conforme mostrado neste exemplo.

### Note

Especifique um nome para seu destino que seja exclusivo para sua Conta da AWS e Região da AWS. Você utilizará o mesmo nome de destino ao adicionar seu destino ao AWS IoT Core para Amazon Sidewalk.

```
// Add your Sidewalk device by using the device profile ID.  
aws iotwireless create-wireless-device --type "Sidewalk" --name sidewalk_device \  
  --destination-name SidewalkDestination \  
  --sidewalk DeviceProfileId="12345678-234a-45bc-67de-e8901234f0a1"
```

## 3. Obtenha informações sobre o perfil do dispositivo e o dispositivo sem fio

Obtenha as informações sobre o perfil do dispositivo e o dispositivo sem fio como um JSON. O JSON conterá informações sobre os detalhes do dispositivo, certificados do dispositivo, chaves privadas DeviceTypeId e o número de série de fabricação do Sidewalk (SMSN).

- Se estiver usando o console de AWS IoT, você pode usar a [guia Sidewalk do hub de dispositivos](#) para baixar um arquivo JSON combinado para seu dispositivo final do Sidewalk.

- Se você estiver usando as operações da API, armazene as respostas obtidas das operações da API [GetDeviceProfile](#) e [GetWirelessDevice](#) como arquivos JSON separados, como *device\_profile.json* e *wireless\_device.json*.

```
// Store device profile information as a JSON file.
aws iotwireless get-device-profile \
  --id "12345678-a1b2-3c45-67d8-e90fa1b2c34d" > device_profile.json

// Store wireless device information as a JSON file.
aws iotwireless get-wireless-device --identifier-type WirelessDeviceId \
  --identifier "23456789-abcd-0123-bcde-fabc012345678" > wireless_device.json
```

## Etapa 2: Criar um destino para seu dispositivo final do Sidewalk

Veja a seguir uma visão geral das etapas que você executará para adicionar o destino ao AWS IoT Core para Amazon Sidewalk. Utilizando o Console de gerenciamento da AWS ou as operações de API do AWS IoT Wireless ou a AWS CLI, execute as etapas a seguir para criar uma regra e um destino do AWS IoT. Em seguida, você pode se conectar à plataforma de hardware e visualizar e trocar mensagens. Para ver um exemplo de perfil do IAM e regra de AWS IoT usado nos exemplos da AWS CLI desta seção, consulte [Criar um perfil do IAM e regra de IoT para o destino](#).

### 1. Crie o perfil do IAM

Crie um perfil do IAM que conceda permissão ao AWS IoT Core para Amazon Sidewalk para enviar dados à regra do AWS IoT. Para criar o perfil, use a operação de API [CreateRole](#) ou o comando de CLI [create-role](#). Você pode nomear o perfil como *SidewalkRole*.

```
aws iam create-role --role-name lambda-ex \
  --assume-role-policy-document file://lambda-trust-policy.json
```

### 2. Crie uma regra para o destino

Crie uma regra de AWS IoT que processe os dados do dispositivo e especifique o tópico no qual as mensagens são publicadas. Você observará mensagens sobre esse tópico depois de se conectar à plataforma de hardware. Use a operação da API AWS IoT Core, [CreateTopicRule](#), ou o comando da AWS CLI, [create-topic-rule](#), para criar uma regra para o destino.

```
aws iot create-topic-rule --rule-name Sidewalkrule \
```

```
--topic-rule-payload file://myrule.json
```

### 3. Crie um destino

Crie um destino que associe seu dispositivo Sidewalk à regra de IoT que o processa para uso com outros Serviços da AWS. Você pode adicionar um destino usando o [hub Destinos](#) do console de AWS IoT, a operação da API [CreateDestination](#) ou o comando da CLI [create-destination](#).

```
aws iotwireless create-destination --name SidewalkDestination \  
  --expression-type RuleName --expression SidewalkRule \  
  --role-arn arn:aws:iam::123456789012:role/SidewalkRole
```

## Etapa 3: Provisionar e registrar o dispositivo final

Usando comandos do Python, você pode provisionar e registrar seu dispositivo final. O script de provisionamento usa os dados JSON do dispositivo que você obteve para gerar uma imagem binária de fabricação, que é então instalada na placa de hardware. Em seguida, você registra seu dispositivo final para se conectar à plataforma de hardware. Para obter mais informações, consulte [Provisionamento e registro do seu dispositivo final](#) na documentação do Amazon Sidewalk.

### Note

Ao registrar seu dispositivo final do Sidewalk, seu gateway deve estar conectado ao Amazon Sidewalk, e o gateway e o dispositivo devem estar ao alcance um do outro.

## Etapa 4: Conectar-se ao dispositivo final do Sidewalk e trocar mensagens

Depois de registrar seu dispositivo final, você poderá conectá-lo e começar a trocar mensagens e dados do dispositivo.

### 1. Conecte seu dispositivo final do Sidewalk

Conecte o HDK ao seu computador e siga as instruções fornecidas pela documentação do fornecedor para conectar-se ao seu HDK. Para obter mais informações, consulte [Provisionamento e registro do seu dispositivo final](#) na documentação do Amazon Sidewalk.

## 2. Ver e trocar mensagens

Use o cliente MQTT para assinar o tópico especificado na regra e visualizar a mensagem recebida. Você também pode usar a operação da API [SendDataToWirelessDevice](#) ou o comando da CLI [send-data-to-wireless-device](#) para enviar uma mensagem de downlink para o seu dispositivo e verificar o status da conectividade.

(Opcional) Você pode ativar o evento de status de entrega da mensagem para verificar se a mensagem de downlink foi recebida com sucesso.

```
aws iotwireless send-data-to-wireless-device \  
  --id "<Wireless_Device_ID>" \  
  --payload-data "SGVsbG8gVG8gRGV2c2lt" \  
  --wireless-metadata Sidewalk={Seq=1,AckModeRetryDurationSecs=10}
```

## Conectar-se ao AWS IoT Core para Amazon Sidewalk

Esta seção mostra como integrar seu dispositivo final do Sidewalk e depois conectá-lo à rede Sidewalk. Ela descreve as etapas executadas no tutorial de integração, conforme mencionado em [Introdução à integração de seus dispositivos do Sidewalk](#). Você aprenderá a integrar dispositivos utilizando o console do AWS IoT e as operações de API do AWS IoT Core para Amazon Sidewalk. Você também aprenderá sobre os comandos da AWS CLI que realizam essas operações.

### Pré-requisitos

Para adicionar um destino e um dispositivo final ao AWS IoT Core para Amazon Sidewalk, configure a sua Conta da AWS. Para executar essas operações utilizando a API do AWS IoT Wireless ou os comandos da AWS CLI, configure a AWS CLI também. Para obter mais informações sobre os pré-requisitos e configuração, consulte [Instalar o Python e a AWS CLI](#).

#### Note

Para realizar todo o fluxo de trabalho de integração para provisionamento e registro do dispositivo final e conexão com seu kit de desenvolvimento de hardware (HDK), você precisa configurar também o gateway do Sidewalk e HDK. Para obter mais informações, consulte [Configuração do kit de desenvolvimento de hardware \(HDK\)](#) e [Configuração de um gateway do Sidewalk](#) na documentação do Amazon Sidewalk.

## Descrição de recursos do Sidewalk

Antes de começar a usar e a criar os recursos, é recomendável considerar a convenção de nomenclatura dos dispositivos finais, dos perfis dos dispositivos e dos destinos do Sidewalk. O AWS IoT Core para Amazon Sidewalk atribui um identificador exclusivo aos recursos criados. No entanto, você pode dar a eles nomes mais descritivos, adicionar uma descrição ou adicionar tags opcionais para ajudar a identificá-los e gerenciá-los.

### Note

O nome do destino não pode ser alterado depois de criado. Use um nome exclusivo para sua Conta da AWS e Região da AWS.

Para ter mais informações, consulte [Descrever os recursos do AWS IoT Wireless](#).

### Tópicos

- [Adicionar o dispositivo ao AWS IoT Core para Amazon Sidewalk](#)
- [Adicionar um destino para o dispositivo final do Sidewalk](#)
- [Conecte seu dispositivo do Sidewalk e visualize o formato dos metadados de uplink](#)

## Adicionar o dispositivo ao AWS IoT Core para Amazon Sidewalk

Antes de criar um dispositivo sem fio, primeiro crie um perfil de dispositivo. Os perfis definem os recursos e outros parâmetros para seus dispositivos do Sidewalk. Um único perfil pode ser associado a vários dispositivos.

Depois de criado, quando você recupera informações sobre o perfil de dispositivo, ele retorna um DeviceTypeId. Ao provisionar o dispositivo final, você utilizará o ID, os certificados do dispositivo, a chave pública do servidor de aplicações e o SMSN.

### Como criar e adicionar seu dispositivo

1. Crie um perfil para seus dispositivos finais do Sidewalk. Especifique um nome para o perfil a ser utilizado com os dispositivos do Sidewalk como uma sequência de caracteres alfanuméricos. O perfil ajudará a identificar os dispositivos aos quais associá-lo.

- (Console) Ao adicionar seu dispositivo do Sidewalk, você também pode criar um novo perfil. Isso ajuda a adicionar rapidamente o dispositivo ao AWS IoT Core para Amazon Sidewalk e associá-lo a um perfil.
  - (API) Use a operação da API `CreateDeviceProfile` especificando um nome de perfil e o objeto do Sidewalk, `sidewalk { }`. A resposta da API conterá um ID de perfil e um nome do recurso da Amazon (ARN).
2. Adicione o dispositivo sem fio ao AWS IoT Core para Amazon Sidewalk. Especifique um nome de destino e escolha o perfil de dispositivo que você criou na etapa anterior.
- (Console) Ao adicionar seu dispositivo do Sidewalk, insira um nome de destino e escolha o perfil que você criou.
  - (API) Use a operação da API `CreateWirelessDevice`. Especifique um nome de destino e ID do perfil do dispositivo obtido anteriormente.

#### Parâmetros do dispositivo sem fio

Parâmetro	Descrição	Observações
Nome do destino	O nome do destino que descreve as regras de AWS IoT para processar os dados do dispositivo que outros AWS service (Serviço da AWS) utilizarão.	Se ainda não tiver criado um destino, você poderá fornecer qualquer valor de string. O AWS IoT Core para Amazon Sidewalk criará um destino vazio ao criar o dispositivo, que você poderá atualizar ao adicionar o destino.
Perfil do dispositivo	O perfil de dispositivo que você criou anteriormente.	–

3. Obtenha o arquivo JSON que contém as informações necessárias para provisionar seu dispositivo final.
- (Console) Faça download desse arquivo na página de detalhes do dispositivo do Sidewalk que você criou.
  - (API) Use as operações da API `GetDeviceProfile` e `GetWirelessDevice` para recuperar informações sobre o perfil do seu dispositivo e o dispositivo sem fio. Armazene as informações de resposta da API como arquivos JSON, como *device\_profile.json* e *wireless\_device.json*.

## Adicione o perfil do seu dispositivo e o dispositivo final do Sidewalk

Esta seção mostra como criar um perfil de dispositivo. Também mostra como é possível utilizar o console do AWS IoT e a AWS CLI para adicionar o dispositivo final do Sidewalk ao AWS IoT Core para Amazon Sidewalk.

### Adicionar seu dispositivo do Sidewalk (console)

Para adicionar seu dispositivo do Sidewalk usando o console AWS IoT, acesse a [guia Sidewalk do hub de dispositivos](#), escolha Provisionar dispositivo e execute as etapas a seguir.

The screenshot shows the AWS IoT console interface for Sidewalk. At the top, there are tabs for 'LoRaWAN' and 'Sidewalk'. Below the tabs, there is a section titled 'How it works' with a sub-header 'How it works' and a brief description: 'With AWS IoT Core for Sidewalk, you can add your Sidewalk device fleet to the AWS Cloud. Use the following steps to get started.' The main content is divided into three columns, each with an icon and a step description:

- Step 1. Add your Sidewalk device**: First, create a device profile and retrieve the application server public key. Next, create your Sidewalk device and retrieve information about it, including device certificates and private keys.
- Step 2. Provision & register your Sidewalk device**: Provision your hardware as a Sidewalk endpoint by flashing the device certificates and the application server public key that you have generated. Register your device so that it can connect to AWS IoT Core for Amazon Sidewalk.
- Step 3. Connect your Sidewalk endpoint to the cloud**: Create a destination and use [AWS IoT Rules](#) to process and route data to other AWS services. Your endpoint can now exchange messages with your cloud application.

At the bottom of the console, there is a section titled 'Sidewalk devices (2) Info' with a sub-header 'Provision and manage all your Sidewalk devices.' Below this, there is a search bar with the placeholder text 'Find Sidewalk device'. To the right of the search bar, there are three buttons: 'Edit', 'Delete', and 'Provision device'. The 'Provision device' button is highlighted with a red border.

### 1. Especifique os detalhes do dispositivo

Especifique as informações de configuração do seu dispositivo do Sidewalk. Você também pode criar um novo perfil de dispositivo ou escolher um perfil existente para seu dispositivo do Sidewalk.

- Especifique um nome de dispositivo e uma descrição opcional. A descrição pode ter até 2.048 caracteres. Esses campos podem ser editados após a criação do dispositivo.
- Escolha um perfil de dispositivo para associar ao seu dispositivo do Sidewalk. Se você tiver algum perfil de dispositivo existente, poderá escolhê-lo. Se você criar um novo perfil, escolha Criar novo perfil e, em seguida, digite um nome para ele.

**Note**

Para anexar tags ao perfil de dispositivo depois de sua criação, acesse o [Hub de perfis](#) e edite o perfil para adicionar essas informações.

- c. Especifique o nome do destino que encaminhará as mensagens do seu dispositivo para outro Serviço da AWS. Se você ainda não criou um destino, acesse o [Hub de destinos](#) para criar seu destino. Em seguida, você pode escolher esse destino para o seu dispositivo do Sidewalk. Para ter mais informações, consulte [Adicionar um destino para o dispositivo final do Sidewalk](#).
  - d. Escolha Próximo para continuar o processo de adição do dispositivo do Sidewalk.
2. Associe o dispositivo do Sidewalk a alguma coisa da AWS IoT (opcional)

Opcionalmente, você pode associar o dispositivo do Sidewalk a qualquer coisa da AWS IoT. Coisas da IoT são entradas no registro do dispositivo do AWS IoT. Isso facilita a pesquisa e o gerenciamento de seus dispositivos. Associar alguma coisa ao dispositivo permite que ele acesse outros recursos do AWS IoT Core.

Para associar o dispositivo a alguma coisa, escolha Registro automático de coisas.

- a. Digite um nome exclusivo para a coisa da IoT a que você deseja associar o dispositivo do Sidewalk. Os nomes das coisas diferenciam maiúsculas de minúsculas na sua Conta da AWS e devem ser exclusivos na sua Região da AWS.
- b. Forneça qualquer configuração adicional para a coisa da IoT escolhida, por exemplo, use um tipo de coisa ou atributos pesquisáveis que possam ser usados para filtrar a partir de uma lista de itens.
- c. Escolha Próximo e verifique as informações sobre o dispositivo do Sidewalk e, em seguida, escolha Criar.

## Adicionar seu dispositivo do Sidewalk (CLI)

Para adicionar o dispositivo do Sidewalk e baixar os arquivos JSON que serão usados para provisioná-lo, execute as seguintes operações da API.

### Tópicos

- [Etapa 1: Criar um perfil do dispositivo](#)

- [Etapa 2: Adicionar o dispositivo do Sidewalk](#)

### Etapa 1: Criar um perfil do dispositivo

Para criar um perfil de dispositivo na sua Conta da AWS, use a operação da API [CreateDeviceProfile](#) ou o comando da CLI [create-device-profile](#). Ao criar seu perfil de dispositivo, especifique o nome e forneça quaisquer tags opcionais como pares nome-valor.

Por exemplo, o comando a seguir cria um perfil de dispositivo para os dispositivos do Sidewalk:

```
aws iotwireless create-device-profile \  
  --name sidewalk_profile --sidewalk {}
```

A execução desse comando retorna o nome do recurso da Amazon (ARN) e o ID do perfil do dispositivo como saída.

```
{  
  "DeviceProfileArn": "arn:aws:iotwireless:us-  
east-1:123456789012:DeviceProfile/12345678-a1b2-3c45-67d8-e90fa1b2c34d",  
  "DeviceProfileId": "12345678-a1b2-3c45-67d8-e90fa1b2c34d"  
}
```

### Etapa 2: Adicionar o dispositivo do Sidewalk

Para adicionar o dispositivo do Sidewalk à sua conta para o AWS IoT Core para Amazon Sidewalk, utilize a operação de API [CreateWirelessDevice](#) ou o comando [create-wireless-device](#) da CLI. Ao criar seu dispositivo, especifique os seguintes parâmetros, além de um nome e uma descrição opcionais para o dispositivo do Sidewalk.

#### Note

Para associar o dispositivo Sidewalk a alguma coisa do AWS IoT, utilize a operação de API [AssociateWirelessDeviceWithThing](#) ou o comando [associate-wireless-device-with-thing](#) da CLI.

O comando a seguir mostra um exemplo de criação de um dispositivo do Sidewalk:

```
aws iotwireless create-wireless-device \  
  --name sidewalk_device --description sidewalk device
```

```
--cli-input-json "file://device.json"
```

O exemplo a seguir mostra o conteúdo do arquivo `device.json`.

Conteúdo de `device.json`

```
{
  "Type": "Sidewalk",
  "Name": "SidewalkDevice",
  "DestinationName": "SidewalkDestination",
  "Sidewalk": {
    "DeviceProfileId": "12345678-a1b2-3c45-67d8-e90fa1b2c34d"
  }
}
```

A execução desse comando retorna o ID do dispositivo e o nome do recurso da Amazon (ARN) como saída.

```
{
  "Arn": "arn:aws:iotwireless:us-east-1:123456789012:WirelessDevice/23456789-
abcd-0123-bcde-fabc012345678",
  "Id": "23456789-abcd-0123-bcde-fabc012345678"
}
```

## Obtenha os arquivos JSON do dispositivo para provisionamento

Depois de adicionar o dispositivo Sidewalk ao AWS IoT Core para Amazon Sidewalk, baixe o arquivo JSON que contém as informações necessárias para provisionar o dispositivo final. Você pode recuperar essas informações usando o console de AWS IoT ou a AWS CLI. Para mais informações sobre como provisionar o dispositivo, consulte [Provisionamento e registro do seu dispositivo final](#) na documentação do Amazon Sidewalk.

Obter arquivo JSON (console)

Para obter o arquivo JSON para provisionar o dispositivo do Sidewalk:

1. Acesse o [Hub de dispositivos do Sidewalk](#).
2. Para visualizar detalhes, escolha o dispositivo adicionado ao AWS IoT Core para Amazon Sidewalk.

- Obtenha o arquivo JSON escolhendo Baixar arquivo JSON do dispositivo, na página de detalhes do dispositivo que você adicionou.

Um arquivo `certificate.json` que contém as informações necessárias para provisionar seu dispositivo final será baixado. A seguir, um arquivo JSON de amostra. Ele contém os certificados do dispositivo, chaves privadas, o número de série de fabricação do Sidewalk (SMSN) e o `DeviceTypeID`.

```
{
  "p256R1": "grg8izXoVvQ86cPvm0GMyWuZYHEBbbH ... DANKk0KoNT3bUGz+/f/pyTE
+xMRdIUBZ1Bw==",
  "eD25519": "grg8izXoVvQ86cPvm0GMyWuZYHEBbbHD ... UiZmntHiUr1GfkTOFMYqRB+Aw==",
  "metadata": {
    "devicetypeid": "fe98",
    "applicationDeviceArn": "arn:aws:iotwireless:us-
east-1:123456789012:WirelessDevice/897ce68e-3ca2-4ed0-85a2-30b0666c4052",
    "applicationDeviceId": "897ce68e-3ca2-4ed0-85a2-30b0666c4052",
    "smsn": "82B83C8B35E856F43CE9C3D59B418CC96B996071016DB1C3BE5901F0F3071A4A",
    "devicePrivKeyP256R1":
"3e704bf8d319b3a475179f1d68c60737b28c708f845d0198f2d00d00c88ee018",
    "devicePrivKeyEd25519":
"17dacb3a46ad9a42d5c520ca5f47f0167f59ce54d740aa13918465faf533b8d0"
  },
  "applicationServerPublicKey":
"5ce29b89c2e3ce6183b41e75fe54e45f61b8bb320efbdd2abd7aefa5957a316b"
}
```

Na página de detalhes do dispositivo Sidewalk, você também verá informações sobre:

- O ID do dispositivo, o nome do recurso da Amazon (ARN) e detalhes sobre qualquer coisa de AWS IoT a que o dispositivo esteja associado.
- O perfil do dispositivo e os detalhes do destino.
- A hora em que a última mensagem de uplink foi recebida do dispositivo.
- O status que indica se seu dispositivo foi provisionado ou registrado.

### Obter arquivo JSON (CLI)

Para obter os arquivos JSON para provisionar o dispositivo final do Sidewalk utilizando a API do AWS IoT Core para Amazon Sidewalk ou a AWS CLI, salve temporariamente a resposta da API

ao recuperar informações sobre o perfil do dispositivo e sobre o dispositivo sem fio como arquivos JSON, como *wireless\_device.json* e *device\_profile.json*. Eles serão utilizados para provisionar seu dispositivo do Sidewalk.

A seguir, é mostrado como recuperar os arquivos JSON.

## Tópicos

- [Etapa 1: Obter informações do perfil do dispositivo como arquivo JSON](#)
- [Etapa 2: Obter informações do dispositivo do Sidewalk como arquivo JSON](#)

### Etapa 1: Obter informações do perfil do dispositivo como arquivo JSON

Utilize a operação de API [GetDeviceProfile](#) ou o comando [get-device-profile](#) da CLI para obter informações sobre o perfil do dispositivo adicionado à sua conta para o AWS IoT Core para Amazon Sidewalk. Para recuperar informações sobre o perfil do dispositivo, especifique o ID do perfil.

A API retornará informações sobre o perfil do dispositivo que correspondem ao identificador especificado e ao ID do dispositivo. Você salva essas informações de resposta como um arquivo e as nomeia como *device\_profile.json*.

Um exemplo de um comando da CLI é mostrado a seguir:

```
aws iotwireless get-device-profile \  
  --id "12345678-a1b2-3c45-67d8-e90fa1b2c34d" > device_profile.json
```

A execução desse comando retorna os parâmetros do perfil do seu dispositivo, a chave pública do servidor de aplicativos e o DeviceTypeID. É apresentado a seguir um arquivo JSON contendo um exemplo de informações de resposta da API. Para obter mais informações sobre os parâmetros na resposta da API, consulte [GetDeviceProfile](#).

### Resposta da API **GetDeviceProfile** (Conteúdo de *device\_profile.json*)

```
{  
  "Arn": "arn:aws:iotwireless:us-east-1:123456789012:DeviceProfile/12345678-  
a1b2-3c45-67d8-e90fa1b2c34d",  
  "Id": "12345678-a1b2-3c45-67d8-e90fa1b2c34d",  
  "Name": "Sidewalk_profile",  
  "LoRaWAN": null,  
  "Sidewalk":
```

```

{
  "ApplicationServerPublicKey":
  "a123b45c6d78e9f012a34cd5e6a7890b12c3d45e6f78a1b234c56d7e890a1234",
  "DAKCertificateMetadata": [
    {
      "DeviceTypeId": "fe98",
      "CertificateId": "43564A6D2D50524F544F54595045",
      "FactorySupport": false,
      "MaxAllowedSignature": 1000
    }
  ],
  "QualificationStatus": false
}

```

## Etapa 2: Obter informações do dispositivo do Sidewalk como arquivo JSON

Utilize a operação de API [GetWirelessDevice](#) ou o comando [get-wireless-device](#) da CLI para obter informações sobre o dispositivo Sidewalk adicionado à sua conta para o AWS IoT Core para Amazon Sidewalk. Para obter informações sobre o dispositivo final, forneça o identificador do dispositivo sem fio obtido ao adicionar seu dispositivo.

A API retornará informações sobre o dispositivo que correspondem ao identificador especificado e ao ID do dispositivo. Salve essas informações de resposta como um arquivo JSON. Dê ao arquivo um nome significativo, como *wireless\_device.json*.

O exemplo a seguir mostra a execução do comando usando a CLI:

```

aws iotwireless get-wireless-device --identifier-type WirelessDeviceId \
  --identifier "23456789-abcd-0123-bcde-fabc012345678" > wireless_device.json

```

A execução desse comando retorna os detalhes do dispositivo, certificados do dispositivo, chaves privadas e o número de série de fabricação do Sidewalk (SMSN). O exemplo a seguir mostra a saída de execução desse comando. Para obter mais informações sobre os parâmetros na resposta da API, consulte [GetWirelessDevice](#).

## Resposta da API **GetWirelessDevice** (Conteúdo de *wireless\_device.json*)

```

{
  "Arn": "arn:aws:iotwireless:us-east-1:123456789012:WirelessDevice/23456789-
abcd-0123-bcde-fabc012345678",
  "Id": "23456789-abcd-0123-bcde-fabc012345678",

```

```

"DestinationName": "SidewalkDestination",
"Type": "Sidewalk",
"Sidewalk": {
  "CertificateId": "4C7438772D50524F544F54595045",
  "DeviceCertificates": [
    {
      "SigningAlg": "Ed25519",

      "Value": "hDdkJw9L2uMCORjImjMHqzNR6nYYh6QKncS15GthQNL7NKe4ounb5UMQtLjnm7z0UPY0qghCeVOLCBUiQe2Z
F+GelTcafZcFKhS+05NPcVNR/fHYaf/cn5iUbRwLz/T
+ODXvGdwkBkgDyFgoUJgn7JdzFjaneE5qzTWXUbl79i1sXToGGjP8hiD9jJhidPWhIswLeydAWg010ZGA4CjzIaSGVM1Vta
uMMBfgAeL8Tdv5LkFIPIB3ZX9zt8zzmAuFRzI4MuNjWfIDn0F6AKu37WU6/
QYhZoQrW9D/wndiCcsRGl+ANn367r/HE02Re4D0iCfs9f2rjc4LT1LKt7g/KW2ii+W
+9HYvvY0bBAI+AHx6Cx4j+djabTsvrgW2k6NU2zUSM7bdDP3z2a2+Z4WzBji/jYwt/
OP8rpsy5Ee4ywXUfCsfQ0rK0r0zay6yh27p3I3MZ1e2oC04JIlqK0VbIQqsXzSSyp6XXS0lhmuGugZ1AAADGz
+gFBex/ZNN8VJwnsNfgzj4me1HgVJdUo4W9kvx9cr2jHwKc30j/bdBTh1+yBj0C53yHLQK/
l1GhrEWiWPPnE434LRxnWkwr8EHD4oieJxC8fkIxxQfj+gHhU79Z
+oAAYAAAsnF9SDIZPoDXf0Tdc9P0qTglD0oXD12XPavD4CvVLearr0SlFv+lsNbc4rgZn23MtIBM/7YQmJwmQ
+FXRup6Tkubg1hgz04J/09dxg8UiZmntHiUr1GfkTOFMYqRB+Aw=="
    },
    {
      "SigningAlg": "P256r1",
      "Value": "hDdkJw9L2uMCORjImjMHqzNR6nYYh6QKncS15GthQNmHmGU8a
+S0qDXWwDnt3VSntpbTTQl7cMIusqweQo+JPXXWE1bGh7eaxPGz4ZeF5yM2cqVNUrQr1LX/6LZ
+0LuycrFrLzzB9APi0NIMLqV/Rt7XJssHQs2RPaT1uL/2XVpa6ztULJeQi2JwhTb/k48wbh/EvafG/
ibrIBIx9v7/
dwGRAPKHq7Uwb9hHnhpa8qN0UtjeUdIwJNh9vCBFX9s22t4PdortoFxbXo9C149PDDD4wqUHJGYlCsVX/
Sqqjf7Aug3h5dwdYN6cDgsuui0m0+aBcXBGpkh70xVxLwXkIP
+11dt23TkrSUKd0B01sc9Mc/0yEBCzx5RutKBwsefzy0l4vQX3AHgV7oD/XV73THMgGiDxQ55CPaaxN/
pm791VkQ76BSZaBeF+Su6tg0k/
eQnek1t8Du5uqkyBHVxy8MvxsBIMZ73vIFwUrLHjDeq3+n00yQqSBMnrHKU2mAwN3zb2LoLwjPkKN0h1+NNnv99L2pBcNCn
+BgewzYndWrxYkKp403ZDa4f+5SVWvbY5eyDDXcohvz/
OcCtuRjAkzKBCvIjBDnCV1McjVdC03+utizGntfhAo1RZstn0oRkgVF2WuMT9IrUmzYximuTXUmWtjyFSTqgNBZwHWUTlMm
csC4HPTKr3dazdvEkhwGAAAIFFByCjSp/5WHc4AhsyjMvKCsZQikgiI8ECwjfXBaSZdY4zYsRl03FC428H1atrFChFCZT0Bq
+vAUJiP8XqiEdXeqf2mYMJ5ykoDpwkve/cUQfPpjzFQlQfvwjBwiJDANKk0KoNT3bUGz+/f/pyTE
+xMRdIUBZ1Bw=="
    }
  ],
  "DeviceProfileId": "0ff5b0c6-f149-4498-af34-21993acd52a7",
  "PrivateKeys": [
    {
      "SigningAlg": "Ed25519",

      "Value": "2c24d4572327f23b9bef38097137c29224a9e979081b3d90124ac9dfa477934e"
    }
  ]
}

```

```
    },
    {
      "SigningAlg": "P256r1",

      "Value": "38d526f29cfaf142f596deca187bd809ef71bc13435eedc885b63bb825d63def"
    }
  ],

  "SidewalkManufacturingSn": "843764270F4BDAE3023918C89A3307AB3351EA761887A40A9DC4A5E46B6140D9",
  "Status": "PROVISIONED"
},
...
}
```

## Próximas etapas

Armazene temporariamente os arquivos JSON, *wireless\_device.json* e *device\_profile.json*, porque eles serão utilizados na próxima etapa de provisionamento e registro do seu dispositivo final para a conexão com a plataforma de hardware. Para obter mais informações, consulte [Provisionamento e registro do seu dispositivo final](#) na documentação do Amazon Sidewalk.

## Adicionar um destino para o dispositivo final do Sidewalk

Use as regras de AWS IoT para processar os dados e as mensagens do dispositivo e encaminhá-los para outros serviços. Você também pode definir regras para processar as mensagens binárias recebidas de um dispositivo e convertê-las em outros formatos que facilitem o uso de outros serviços. Os destinos associam seu dispositivo final do Sidewalk à regra que processa os dados do dispositivo para enviá-los para outros AWS service (Serviço da AWS).

### Como criar e usar um destino

1. Crie uma regra AWS IoT e um perfil do IAM para o destino. A regra de AWS IoT especifica as regras que processarão os dados do dispositivo e os encaminha para uso por outros AWS service (Serviço da AWS) e seus aplicativos. O perfil do IAM concede permissões para o acesso à regra.
2. Crie um destino para seus dispositivos do Sidewalk usando a operação da API `CreateDestination`. Especifique o nome do destino, da regra, da função e quaisquer

parâmetros opcionais. A API retornará um identificador exclusivo para o destino, que você pode especificar ao adicionar o dispositivo final ao AWS IoT Core para Amazon Sidewalk.

Veja a seguir como criar um destino, uma regra de AWS IoT e um perfil do IAM para o destino.

## Tópicos

- [Criar um destino para seu dispositivo do Sidewalk](#)
- [Criar um perfil do IAM e regra de IoT para o destino](#)

## Criar um destino para seu dispositivo do Sidewalk

É possível adicionar um destino à sua conta para o AWS IoT Core para Amazon Sidewalk utilizando o [Hub de destinos](#) ou `CreateDestination`. Ao criar seu destino, especifique:

- Um nome exclusivo para o destino a ser usado no dispositivo final do Sidewalk.

### Note

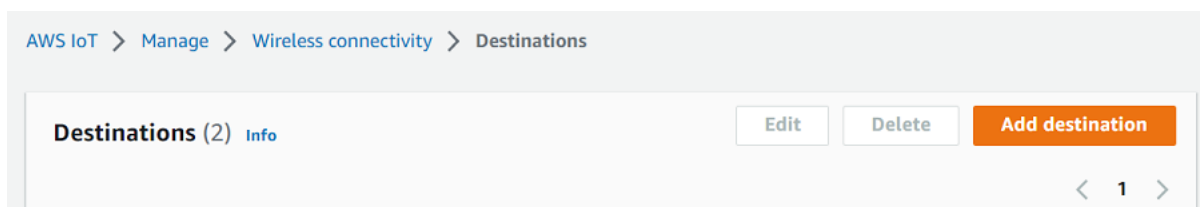
Se você já adicionou o dispositivo usando um nome de destino, será preciso usar esse nome ao criar seu destino. Para ter mais informações, consulte [Etapa 2: Adicionar o dispositivo do Sidewalk](#).

- O nome da regra de AWS IoT que processará os dados do dispositivo e o tópico no qual as mensagens serão publicadas.
- Um perfil do IAM que conceda permissões de dados do dispositivo para o acesso à regra.

As seções a seguir descrevem como criar a regra de AWS IoT e um perfil do IAM para o destino.

## Criar um destino (console)

Para criar um destino usando o console de AWS IoT, acesse o [Hub de destinos](#) e escolha Adicionar destino.



Para processar os dados de um dispositivo, especifique os seguintes campos ao criar um destino e escolha Adicionar destino.

- Detalhes do destino

Insira um Nome de destino e uma descrição opcional para o destino.

- Nome da regra

A regra de AWS IoT configurada para avaliar as mensagens enviadas pelo seu dispositivo e processar os dados do dispositivo. O nome da regra será mapeado para o seu destino. O destino exige que a regra processe as mensagens recebidas. Você pode escolher que as mensagens sejam processadas invocando uma regra de AWS IoT ou publicando no agente de mensagens de AWS IoT.

- Se você escolher Inserir um nome de regra, digite um nome e escolha Copiar para copiar o nome da regra que você inserirá ao criar a regra de AWS IoT. Você pode escolher Criar regra para criar a regra agora ou navegar até o Hub de [regras](#) do console de AWS IoT e criar uma regra com esse nome.

Você também pode inserir uma regra e usar a configuração Avançada para especificar um nome de tópico. O nome do tópico é fornecido durante a invocação da regra e é acessado usando a expressão `topic` dentro da regra. Para obter mais informações sobre as regras de AWS IoT, consulte [regras de AWS IoT](#).

- Se você escolher Publicar no agente de mensagens de AWS IoT, insira um nome de tópico. Em seguida, você pode copiar o nome do tópico de MQTT e vários assinantes podem se inscrever nesse tópico para receber mensagens publicadas nesse tópico. Para ver mais informações, consulte [tópicos de MQTT](#).

Para obter mais informações sobre as regras de AWS IoT para destinos, consulte [Criar regras para processar mensagens do dispositivo LoRaWAN](#).

- Nome do perfil

O perfil do IAM que concede permissões de dados do dispositivo para o acesso à regra, nomeada em Nome da regra. No console, é possível criar um novo perfil de serviço ou selecionar um já existente. Se você estiver criando um novo perfil de serviço, poderá inserir um nome de perfil (por exemplo, **SidewalkDestinationRole**) ou deixá-lo em branco para AWS IoT Core for LoRaWAN para gerar um novo nome de perfil. O AWS IoT Core for LoRaWAN, então, criará automaticamente o perfil do IAM com as devidas permissões em seu nome.

## Criar um destino (CLI)

Para criar um destino, use a operação da API [CreateDestination](#) ou o comando da CLI [create-destination](#). Por exemplo, o comando a seguir cria um destino para o dispositivo final do Sidewalk:

```
aws iotwireless create-destination --name SidewalkDestination \  
  --expression-type RuleName --expression SidewalkRule \  
  --role-arn arn:aws:iam::123456789012:role/SidewalkRole
```

A execução desse comando retorna os detalhes do destino, que incluem o nome do recurso da Amazon (ARN) e o nome do destino.

```
{  
  "Arn": "arn:aws:iotwireless:us-east-1:123456789012:Destination/SidewalkDestination",  
  "Name": "SidewalkDestination"  
}
```

Para obter mais informações sobre a criação de um destino, consulte [Criar regras para processar mensagens do dispositivo LoRaWAN](#).

## Criar um perfil do IAM e regra de IoT para o destino

As regras do AWS IoT enviam mensagens de dispositivos a outros serviços. As regras do AWS IoT também podem processar as mensagens binárias recebidas de um dispositivo final do Sidewalk para utilização de outros serviços. Os destinos do AWS IoT Core para Amazon Sidewalk associam um dispositivo sem fio à regra que processa os dados da mensagem do dispositivo para envio a outros serviços. A regra atua nos dados do dispositivo assim que o AWS IoT Core para Amazon Sidewalk os recebe. Para todos os dispositivos que enviam seus dados para o mesmo serviço, você pode criar um destino que possa ser compartilhado por todos eles. É preciso criar um perfil do IAM que conceda permissão para enviar dados para a regra.

### Criar um perfil do IAM para o destino

Crie um perfil do IAM que conceda permissão ao AWS IoT Core para Amazon Sidewalk para enviar dados à regra do AWS IoT. Para criar o perfil, use a operação de API [CreateRole](#) ou o comando de CLI [create-role](#). Você pode nomear a função como *SidewalkRole*.

```
aws iam create-role --role-name SidewalkRole \  
  --policy-name SidewalkPolicy
```

```
--assume-role-policy-document '{"Version": "2012-10-17", "Statement":
[{"Effect": "Allow", "Principal": {"Service": "lambda.amazonaws.com"}, "Action":
"sts:AssumeRole"}]}'
```

Também é possível definir a política de confiança para a função usando um arquivo JSON.

```
aws iam create-role --role-name SidewalkRole \
--assume-role-policy-document file://trust-policy.json
```

O exemplo a seguir mostra o conteúdo do arquivo JSON.

Conteúdo do trust-policy.json

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

### Criar uma regra para o destino

Use a operação da API AWS IoT Core, [CreateTopicRule](#), ou o comando da AWS CLI, [create-topic-rule](#), para criar uma regra. A regra do tópico será usada pelo destino para direcionar os dados recebidos do seu dispositivo final do Sidewalk para outros Serviços da AWS. Por exemplo, você pode criar uma ação de regra que envia uma mensagem para uma função do Lambda.

Você pode definir a função do Lambda de maneira que ela receba os dados do aplicativo do seu dispositivo e use base64 para decodificar os dados da carga útil para que possam ser usados por outros aplicativos.

As etapas a seguir mostram como criar a função do Lambda e, em seguida, uma regra de tópico que envie uma mensagem para essa função.

## 1. Criar uma função e uma política de execução

Crie um perfil do IAM que dá à sua função permissão para acessar recursos da AWS. Também é possível definir a política de confiança para a função usando um arquivo JSON.

```
aws iam create-role --role-name lambda-ex \  
  --assume-role-policy-document file://lambda-trust-policy.json
```

O exemplo a seguir mostra o conteúdo do arquivo JSON.

Conteúdo do `lambda-trust-policy.json`

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "Service": "lambda.amazonaws.com"  
      },  
      "Action": "sts:AssumeRole"  
    }  
  ]  
}
```

## 2. Criar e testar a função do Lambda

Execute as etapas a seguir para criar uma função do AWS Lambda que permita que base64 decodifique os dados da carga útil.

- a. Escreva o código para decodificar os dados da carga útil. Você pode usar o exemplo de código Python a seguir. Especifique um nome para o script, como *base64\_decode.py*.

Conteúdo do `base64_decode.py`

```
// -----  
// ----- Python script to decode incoming binary payload -----  
// -----  
import json  
import base64  
  
def lambda_handler(event, context):
```

```

message = json.dumps(event)
print (message)

payload_data = base64.b64decode(event["PayloadData"])
print(payload_data)
print(int(payload_data,16))

```

- b. Criar um pacote de implantação como um arquivo zip que contenha o arquivo Python e nomeá-lo como *base64\_decode.zip*. Use a API CreateFunction ou o comando da CLI `create-function` para criar uma função do Lambda para o código de amostra, *base64\_decode.py*.

- c.
- ```

aws lambda create-function --function-name my-function \
--zip-file fileb://base64_decode.zip --handler index.handler \
--runtime python3.9 --role arn:aws:iam::123456789012:role/lambda-ex

```

Você verá a saída a seguir. Você usará o valor do nome do recurso da Amazon (ARN) da saída, `FunctionArn`, ao criar a regra de tópico.

```

{
  "FunctionName": "my-function",
  "FunctionArn": "arn:aws:lambda:us-east-1:123456789012:function:my-function",
  "Runtime": "python3.9",
  "Role": "arn:aws:iam::123456789012:role/lambda-ex",
  "Handler": "index.handler",
  "CodeSha256": "FpFMvUhayLk0oVBpNuNiIVML/tuGv2iJQ7t0yWVTU8c=",
  "Version": "$LATEST",
  "TracingConfig": {
    "Mode": "PassThrough"
  },
  "RevisionId": "88ebe1e1-bfdf-4dc3-84de-3017268fa1ff",
  ...
}

```

- d. Para obter logs para uma invocação a partir da linha de comando, use a opção `--log-type` com o comando `invoke`. A resposta inclui um campo `LogResult` que contém até 4 KB de logs codificados em base64 da invocação.

```

aws lambda invoke --function-name my-function out --log-type Tail

```

Você receberá uma resposta com um `StatusCode` de 200. Para obter mais informações sobre como criar e usar as funções do Lambda com a AWS CLI, consulte [Como usar o Lambda com a AWS CLI](#).

### 3. Criar uma regra de tópico

Use a API `CreateTopicRule` ou o comando da CLI `create-topic-rule` para criar uma regra de tópico que envia uma mensagem para essa função do Lambda. Você também pode adicionar uma segunda ação de regra que republica em um tópico de AWS IoT. Nomeie essa regra de tópico como *Sidewalkrule*.

```
aws iot create-topic-rule --rule-name Sidewalkrule \  
  --topic-rule-payload file://myrule.json
```

Você pode usar o arquivo `myrule.json` para especificar mais detalhes sobre a regra. Por exemplo, o arquivo JSON a seguir mostra como republicar em um tópico de AWS IoT e enviar uma mensagem para uma função do Lambda.

```
{  
  "sql": "SELECT * ",  
  "actions": [  
    {  
      // You obtained this functionArn when creating the Lambda function  
      using the  
      // create-function command.  
      "lambda": {  
        "functionArn": "arn:aws:lambda:us-east-1:123456789012:function:my-  
function"  
      }  
    },  
    {  
      // This topic can be used to observe messages exchanged between the  
      device and  
      // AWS IoT Core for Amazon Sidewalk after the device is connected.  
      "republish": {  
        "roleArn": "arn:aws:iam::123456789012:role/service-  
role/SidewalkRepublishRole",  
        "topic": "project/sensor/observed"  
      }  
    }  
  ],  
}
```

```
}
```

## Conecte seu dispositivo do Sidewalk e visualize o formato dos metadados de uplink

Neste tutorial, você usará o cliente de teste MQTT para testar a conectividade e ver as mensagens trocadas entre seu dispositivo final e a Nuvem AWS. Para receber mensagens, no cliente de teste MQTT, assine o tópico especificado ao criar a regra de IoT para o destino. Também é possível enviar uma mensagem de downlink do AWS IoT Core para Amazon Sidewalk ao dispositivo utilizando a operação de API `SendDataToWirelessDevice`. Você pode verificar se a mensagem foi entregue ativando a notificação de evento de status de entrega da mensagem.

### Note

Para obter informações sobre como conectar sua plataforma de hardware e configurá-la, consulte [Provisionamento e registro do seu dispositivo final](#) e [Configuração do kit de desenvolvimento de hardware \(HDK\)](#) na documentação do Amazon Sidewalk.

## Enviar mensagens de downlink para o dispositivo final

Utilize a operação de API [SendDataToWirelessDevice](#) ou o comando [send-data-to-wireless-device](#) da CLI para enviar mensagens de downlink do AWS IoT Core para Amazon Sidewalk ao dispositivo final do Sidewalk. O exemplo a seguir mostra como executar esse comando. Os dados da carga útil são o binário a ser enviado, codificado em base64.

```
aws iotwireless send-data-to-wireless-device \  
  --id "<Wireless_Device_ID>" \  
  --payload-data "SGVsbG8gVG8gRGV2c2lt" \  
  --wireless-metadata Sidewalk={Seq=1,AckModeRetryDurationSecs=10}
```

O exemplo a seguir mostra uma saída da execução desse comando, que é um ID da mensagem de downlink enviada ao dispositivo.

```
{  
  MessageId: "6011dd36-0043d6eb-0072-0008"  
}
```

**Note**

A API `SendDataToWirelessDevice` pode retornar um ID de mensagem, mas a mensagem talvez não seja entregue com sucesso. Para verificar o status da mensagem que foi enviada ao dispositivo, você pode ativar eventos de status de entrega de mensagens para suas contas e dispositivos do Sidewalk. Para obter mais informações sobre como ativar esse evento, consulte [Notificações de eventos para recursos do Sidewalk](#). Para obter mais informações sobre esse tipo de evento, consulte [Eventos de entrega de mensagens](#).

## Visualizar o formato das mensagens de uplink do dispositivo

Depois de conectar seu dispositivo, você pode se inscrever no tópico (por exemplo, *project/sensor/observed*) que especificou ao criar a regra de destino e observar as mensagens de uplink vindas do dispositivo.

Se você especificou um nome de tópico ao criar o destino, você pode se inscrever no tópico para monitorar mensagens de uplink vindas do dispositivo final. Acesse o [cliente de teste MQTT](#) na página Teste do console AWS IoT, insira o nome do tópico (por exemplo, *project/sensor/observed*) e escolha Inscrição.

O exemplo a seguir mostra o formato das mensagens de uplink enviadas dos dispositivos do Sidewalk para a AWS IoT. O `WirelessMetadata` contém metadados sobre a solicitação de mensagem.

```
{
  "PayloadData": "ZjRlNjY1ZWw1Nw==",
  "WirelessDeviceId": "wireless_device_id",
  "WirelessMetadata": {
    "Sidewalk": {
      "CmdExStatus": "Cmd",
      "SidewalkId": "device_id",
      "Seq": 0,
      "MessageType": "messageType"
    }
  }
}
```

A tabela a seguir mostra uma definição dos diferentes parâmetros nos metadados do uplink. O *device-id* é o ID do dispositivo sem fio, como *ABCDEF1234*, e *messageType* é o tipo de mensagem de uplink recebida do dispositivo.

#### Parâmetros de metadados de uplink do Sidewalk

| Parâmetro             | Descrição                                                                                                                                                                                                      | Tipo              | Obrigatório |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|-------------|
| PayloadData           | A carga útil da mensagem enviada do dispositivo sem fio.                                                                                                                                                       | String            | Sim         |
| WirelessDeviceID      | O identificador do dispositivo sem fio que está enviando os dados                                                                                                                                              | String            | Sim         |
| Sidewalk.CmdExStatus  | Status do runtime do comando. As mensagens do tipo de resposta devem incluir o código de status, <code>COMMAND_EXEC_STATUS_SUCCESS</code> . No entanto, as notificações talvez não incluam o código de status. | Enumeração        | Não         |
| Sidewalk.NackExStatus | Status nack da resposta, que pode ser <code>RADIO_TX_ERROR</code> ou <code>MEMORY_ERROR</code> .                                                                                                               | Matriz de strings | Não         |

## Provisionamento em massa de dispositivos com o AWS IoT Core para Amazon Sidewalk

É possível utilizar o provisionamento em massa para integrar uma grande quantidade de dispositivos finais em massa ao AWS IoT Core para Amazon Sidewalk. O provisionamento em massa é útil principalmente quando você produz um grande número de dispositivos em uma fábrica e deseja integrá-los ao AWS IoT. Para obter mais informações sobre a fabricação de dispositivos, consulte [Fabricação de dispositivos Amazon Sidewalk](#) na documentação do Amazon Sidewalk.

Os tópicos a seguir mostram como o provisionamento em massa funciona.

- [Fluxo de trabalho de provisionamento em massa do Amazon Sidewalk](#)

Este tópico mostra alguns conceitos-chave do provisionamento em massa e como ele funciona. As etapas a serem executadas para que os dispositivos Sidewalk possam ser importados para o AWS IoT Core para Amazon Sidewalk também são descritas.

- [Criação de perfis de dispositivos com suporte de fábrica](#)

Este tópico explica como criar um perfil de dispositivo e obter suporte de fábrica para ele. Você também aprenderá como recuperar a chave YubiHSM e enviá-la ao fabricante para obter o log de controle após a fabricação dos dispositivos.

- [Provisionamento de dispositivos do Sidewalk usando tarefas de importação](#)

Este tópico mostra como provisionar em massa seus dispositivos do Sidewalk criando e usando tarefas de importação. Você também aprenderá a atualizar ou excluir as tarefas de importação e a visualizar o status delas e dos dispositivos na tarefa.

## Tópicos

- [Fluxo de trabalho de provisionamento em massa do Amazon Sidewalk](#)
- [Criação de perfis de dispositivos com suporte de fábrica](#)
- [Provisionamento de dispositivos do Sidewalk usando tarefas de importação](#)

## Fluxo de trabalho de provisionamento em massa do Amazon Sidewalk

As seções a seguir mostram os conceitos-chave do provisionamento em massa e como ele funciona. As etapas envolvidas no provisionamento em massa incluem:

1. Criar um perfil de dispositivo utilizando o AWS IoT Core para Amazon Sidewalk.
2. Solicitar à equipe do Amazon Sidewalk uma chave YubiHSM e atualizar o perfil do dispositivo com o suporte de fábrica.
3. Enviar a chave YubiHSM ao fabricante para que o AWS IoT Core para Amazon Sidewalk possa obter o log de controle após a fabricação dos dispositivos.
4. Criar uma tarefa de importação e fornecer os números de série (SMSN) dos dispositivos que serão integrados ao AWS IoT Core.

## Componentes do provisionamento em massa

Os conceitos a seguir mostram alguns componentes principais do provisionamento em massa e como usá-los como parte do provisionamento em massa de seus dispositivos do Sidewalk.

### Chave YubiHSM

A Amazon cria um ou mais HSMs (módulos de segurança de hardware) para cada um dos seus produtos Sidewalk. Cada HSM tem um número de série exclusivo, chamado chave YubiHSM, impresso no módulo de hardware. Essa chave pode ser comprada na [página da Yubico](#).

A chave é exclusiva para cada HSM e vinculada a cada perfil de dispositivo criado com o AWS IoT Core para Amazon Sidewalk. Para obter a chave YubiHSM, entre em contato com a equipe do Amazon Sidewalk. Se você enviar a chave YubiHSM ao fabricante, depois que os dispositivos Sidewalk forem produzidos na fábrica, o AWS IoT Core para Amazon Sidewalk receberá um arquivo de log de controle que contém os números de série dos dispositivos. Em seguida, ele compara essas informações com o arquivo CSV de entrada para integrar os dispositivos à AWS IoT.

### Chave de atestado do dispositivo (DAK)

Quando um dispositivo final do Sidewalk se junta à rede do Sidewalk, ele deve ser provisionado com um certificado de dispositivo do Sidewalk. Os certificados usados para configurar seu dispositivo incluem um certificado privado específico do dispositivo e os certificados públicos, que correspondem à cadeia de certificados do Sidewalk. Quando os dispositivos do Sidewalk são fabricados, o YubiHSM assina os certificados de dispositivo.

Veja a seguir um exemplo de um arquivo JSON que contém os certificados do dispositivo e as chaves privadas. Para ter mais informações, consulte [Obtenha os arquivos JSON do dispositivo para provisionamento](#).

```
{
  "p256R1": "grg8izXoVvQ86cPvm0GMyWuZYHEBbbH ... DANKk0KoNT3bUGz+/f/pyTE
+xMRdIUBZ1Bw==",
  "eD25519": "grg8izXoVvQ86cPvm0GMyWuZYHEBbbHD ... UiZmntHiUr1GfkTOFMYqRB+Aw==",
  "metadata": {
    "devicetypeid": "fe98",
    ...
  }
  "devicePrivKeyP256R1":
  "3e704bf8d319b3a475179f1d68c60737b28c708f845d0198f2d00d00c88ee018",
```

```
"devicePrivKeyEd25519":  
  "17dacb3a46ad9a42d5c520ca5f47f0167f59ce54d740aa13918465faf533b8d0"  
  },  
  "applicationServerPublicKey":  
  "5ce29b89c2e3ce6183b41e75fe54e45f61b8bb320efbdd2abd7aefa5957a316b"  
}
```

A chave de atestado do dispositivo (DAK) é uma chave privada obtida ao criar seu perfil de dispositivo. Ela corresponde ao certificado do produto, que é um certificado exclusivo emitido para cada produto Sidewalk. Ao entrar em contato com a equipe do Amazon Sidewalk, você receberá a cadeia de certificados do Sidewalk, a chave YubiHSM e um HSM provisionado com a chave de atestado de dispositivo do produto (DAK).

O perfil do seu dispositivo também é atualizado com a nova chave de atestado do dispositivo (DAK) e com o suporte de fábrica ativado. As informações de metadados do DAK do perfil do dispositivo fornecem detalhes como o nome do DAK, o ID do certificado, o APID (ID de produto anunciado), se o suporte de fábrica está ativado e o número máximo de assinaturas que o DAK pode assinar.

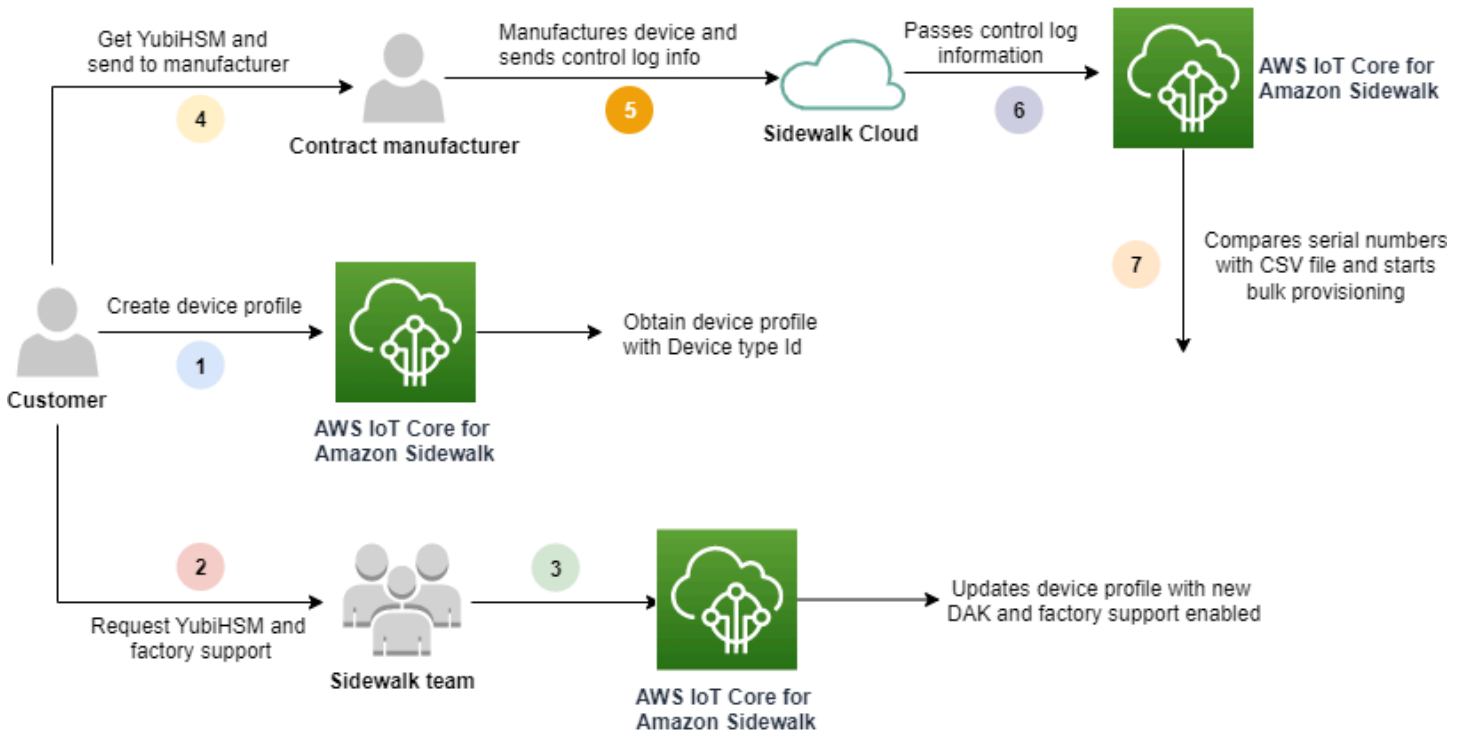
### ID de produto anunciado (**ApId**)

O parâmetro ApId é uma sequência alfanumérica que identifica o produto anunciado. Especifique esse campo caso queira utilizar determinado perfil de dispositivo Sidewalk provisionado em massa. O AWS IoT Core para Amazon Sidewalk gera o DAK e o fornece a você por meio da chave YubiHSM. As informações do DAK relacionadas serão apresentadas no perfil do dispositivo.

Para obter o ApId, depois de recuperar as informações sobre o perfil de dispositivo criado, entre em contato com a equipe de suporte do Amazon Sidewalk. Você pode obter as informações do perfil do dispositivo no console de AWS IoT, usando a operação da API [GetDeviceProfile](#) ou o comando da CLI [get-device-profile](#).

### Como funciona o provisionamento em massa

Este fluxograma mostra como funciona o provisionamento em massa com o AWS IoT Core para Amazon Sidewalk.



O procedimento a seguir ilustra as diferentes etapas do processo de provisionamento em massa.

### 1. Criar um perfil para seus dispositivos do Sidewalk

Antes de levar seu dispositivo final para a fábrica, primeiro crie um perfil de dispositivo. Você pode usar esse perfil para provisionar dispositivos individuais conforme descrito em [Adicione o perfil do seu dispositivo e o dispositivo final do Sidewalk](#).

### 2. Solicitar o suporte de fábrica para seu perfil

Quando você estiver pronto para levar seu dispositivo final para a fábrica, peça à equipe do Amazon Sidewalk a chave YubiHSM e o suporte de fábrica para o perfil do dispositivo.

### 3. Obter o DAK e o perfil com suporte de fábrica

Em seguida, a equipe de suporte do Amazon Sidewalk atualizará o perfil do dispositivo com a chave de atestado de dispositivo (DAK) do produto e o suporte de fábrica. O perfil do dispositivo será atualizado automaticamente com um ID do produto (APID) anunciado, um novo DAK e informações do certificado, como o seu ID. Os dispositivos do Sidewalk que usam esse perfil são qualificados para uso com provisionamento em massa.

#### 4. Enviar a chave YubiHSM ao fabricante (CM)

Seu dispositivo final agora está qualificado, então você pode enviar sua chave YubiHSM ao fabricante contratado (CM) para iniciar o processo de fabricação. Para obter mais informações, consulte [Fabricação de dispositivos Amazon Sidewalk](#) na documentação do Amazon Sidewalk.

#### 5. Fabricar dispositivos e enviar logs de controle e números de série

O CM fabrica os dispositivos e gera logs de controle. O CM também fornece um arquivo CSV que contém uma lista de dispositivos a serem fabricados e seus números de série de fabricação do Sidewalk (SMSN). O código a seguir mostra um exemplo de log de controle. Ele contém os números de série do dispositivo, o APID e os certificados públicos do dispositivo.

```
{
  "controlLogs": [
    {
      "version": "4-0-1",
      "device": {
        "serialNumber": "device1",
        "productIdentifier": {
          "advertisedProductId": "abCD"
        },
        "sidewalkData": {
          "SidewalkED25519CertificateChain": "...",
          "SidewalkP256R1CertificateChain": "..."
        }
      }
    }
  ]
}
```

#### 6. Passar as informações do log de controle para o AWS IoT Core para Amazon Sidewalk

A nuvem do Amazon Sidewalk recupera as informações do log de controle do fabricante e as transfere para o AWS IoT Core para Amazon Sidewalk. Os dispositivos podem então ser criados junto com seus números de série.

#### 7. Verifique a correspondência do número de série e inicie o provisionamento em massa

Ao utilizar o console do AWS IoT ou a operação de API `StartWirelessDeviceImportTask` do AWS IoT Core para Amazon Sidewalk, o AWS IoT Core para Amazon Sidewalk compara o número de série de fabricação do Sidewalk (SMSN) de cada dispositivo obtido do Amazon

Sidewalk com os correspondentes em seu arquivo CSV. Se essas informações corresponderem, o processo de provisionamento em massa será iniciado e criará os dispositivos a serem importados para o AWS IoT Core para Amazon Sidewalk.

## Criação de perfis de dispositivos com suporte de fábrica

Antes de provisionar em massa seus dispositivos do Amazon Sidewalk, você precisa criar um perfil de dispositivo e entrar em contato com a equipe de suporte do Amazon Sidewalk para solicitar suporte de fábrica para ele. Em seguida, a equipe do Amazon Sidewalk atualizará o perfil do dispositivo com a chave de atestado de dispositivo (DAK) e adicionará o suporte de fábrica a ele. Os dispositivos Sidewalk que utilizam esse perfil são qualificados para serem usados com o AWS IoT Core para Amazon Sidewalk e poderão ser integrados para provisionamento em massa.

As etapas a seguir mostram como criar um perfil de dispositivo com suporte de fábrica.

### 1. Criar um perfil do dispositivo

Primeiro, crie um perfil do dispositivo. Ao criar um perfil, especifique o nome e tags opcionais como pares nome-valor. Para obter mais informações sobre os parâmetros necessários e sobre como criar e usar perfis, consulte [Como criar e adicionar seu dispositivo](#).

### 2. Obter suporte de fábrica para o perfil

Obtenha o suporte de fábrica para o perfil de dispositivo para que os dispositivos que o utilizam possam ser qualificados. Para se qualificar, crie um tíquete com a equipe do Amazon Sidewalk. Depois de confirmado pela equipe, você receberá um APID (ID de produto anunciado) e seu perfil será atualizado com um DAK emitido pela fábrica. Os dispositivos finais do Sidewalk que usam esse perfil serão qualificados.

É possível criar um perfil de dispositivo utilizando o console do AWS IoT, as operações de API do AWS IoT Core para Amazon Sidewalk ou a AWS CLI.

### Tópicos

- [Criar um perfil \(console\)](#)
- [Criar um perfil \(CLI\)](#)
- [Próximas etapas](#)

## Criar um perfil (console)

Para criar um perfil de dispositivo usando o console de AWS IoT, acesse a [guia Sidewalk do hub de Perfis](#) e escolha Criar perfil.

The screenshot shows the AWS IoT console interface for Sidewalk. At the top, there are two tabs: 'LoRaWAN' and 'Sidewalk'. The 'Sidewalk' tab is active. Below the tabs, there is a header for 'Device profiles (1) Info' with a 'Delete' button and an 'Add device profile' button. A search bar is present with the placeholder text 'Find device profile'. Below the search bar is a table with the following columns: 'Name', 'Profile ID', and 'Qualification status'. The table contains one row with the following data: 'New\_profile3', 'b627bc56-97c3-475e-90b7-b...', and 'Not Qualified'.

Para criar um perfil, especifique os campos a seguir e escolha Enviar.

- Nome

Insira um Nome para o perfil.

- Tags

Insira tags opcionais como pares de nome-valor para ajudar você a identificar seu perfil com mais facilidade. As tags também facilitam o rastreamento de cobranças.

### Ver informações e qualificar perfis

Você verá o perfil criado em [hub de Perfis](#). Escolha o perfil para visualizar os detalhes. Você verá informações sobre:

- O nome do perfil e o identificador exclusivo do dispositivo e quaisquer tags opcionais especificadas como pares de nome-valor.
- A chave pública do servidor de aplicativos e o ID do tipo de dispositivo do perfil.
- O status de qualificação, que indica que você está usando um perfil de dispositivo não compatível com a fábrica. Para qualificar o perfil de dispositivo para o suporte de fábrica, entre em contato com o Suporte do Amazon Sidewalk.

- As informações da chave de atestado de dispositivo (DAK). Depois que o perfil do dispositivo for qualificado, um novo DAK será emitido e seu perfil será atualizado automaticamente com as novas informações do DAK.

## Criar um perfil (CLI)

Para criar um perfil de dispositivo, use a operação da API [CreateDeviceProfile](#) ou o comando da CLI [create-device-profile](#). Por exemplo, o comando a seguir cria um perfil para o dispositivo final do Sidewalk:

```
aws iotwireless create-device-profile \  
  --name sidewalk_device_profile --sidewalk {}
```

A execução desse comando retorna os detalhes do perfil, que incluem o nome do recurso da Amazon (ARN) e o ID do perfil.

```
{  
  "DeviceProfileArn": "arn:aws:iotwireless:us-  
east-1:123456789012:DeviceProfile/12345678-a1b2-3c45-67d8-e90fa1b2c34d",  
  "DeviceProfileId": "12345678-a1b2-3c45-67d8-e90fa1b2c34d"  
}
```

## Ver informações e qualificar perfis

Utilize a operação de API [GetDeviceProfile](#) ou o comando [get-device-profile](#) da CLI para obter informações sobre o perfil do dispositivo adicionado à sua conta para o AWS IoT Core para Amazon Sidewalk. Para recuperar informações sobre o perfil do dispositivo, especifique o ID do perfil. A API retornará informações sobre o perfil do dispositivo que correspondem ao identificador especificado.

Um exemplo de um comando da CLI é mostrado a seguir:

```
aws iotwireless get-device-profile \  
  --id "12345678-234a-45bc-67de-e8901234f0a1" > device_profile.json
```

A execução desse comando retorna os parâmetros do perfil do seu dispositivo, a chave pública do servidor de aplicativos, DeviceTypeId, ApId, status de qualificação e informações do DAKCertificate.

Nesse exemplo, o status de qualificação e as informações do DAK indicam que o perfil do dispositivo não está qualificado. Para qualificar seu perfil, entre em contato com o suporte do Amazon Sidewalk e seu perfil receberá um novo DAK sem limite de dispositivos.

```
{
  "Arn": "arn:aws:iotwireless:us-east-1:123456789012:DeviceProfile/12345678-
a1b2-3c45-67d8-e90fa1b2c34d",
  "Id": "12345678-a1b2-3c45-67d8-e90fa1b2c34d",
  "Name": "Sidewalk_profile",
  "LoRaWAN": null,
  "Sidewalk":
  {
    "ApplicationServerPublicKey":
    "a123b45c6d78e9f012a34cd5e6a7890b12c3d45e6f78a1b234c56d7e890a1234",
    "DAKCertificateMetadata": [
      {
        "DeviceTypeId": "fe98",
        "CertificateId": "43564A6D2D50524F544F54595045",
        "FactorySupport": false,
        "MaxAllowedSignature": 1000
      }
    ],
    "QualificationStatus": false
  }
}
```

Depois que a equipe de suporte do Amazon Sidewalk confirmar essas informações, você receberá o APID e um DAK com suporte da fábrica, conforme mostrado no exemplo a seguir.

#### Note

O MaxAllowedSignature de -1 indica que o DAK não tem limite de dispositivos. Para obter informações sobre os parâmetros do DAK, consulte [DAKCertificateMetadata](#).

```
{
  "Arn": "arn:aws:iotwireless:us-east-1:123456789012:DeviceProfile/12345678-
a1b2-3c45-67d8-e90fa1b2c34d",
  "Id": "12345678-a1b2-3c45-67d8-e90fa1b2c34d",
  "Name": "Sidewalk_profile",
  "LoRaWAN": null,
```

```
"Sidewalk":
{
  "ApplicationServerPublicKey":
  "a123b45c6d78e9f012a34cd5e6a7890b12c3d45e6f78a1b234c56d7e890a1234",
  "DAKCertificateMetadata": [
    {
      "ApId": "GZBd",
      "CertificateId": "43564A6D2D50524F544F54595045",
      "FactorySupport": true,
      "MaxAllowedSignature": -1
    }
  ],
  "QualificationStatus": true
}
```

## Próximas etapas

Agora que você criou um perfil de dispositivo que tem um DAK com suporte de fábrica, forneça ao fabricante a chave YubiHSM obtida com a equipe. Desse modo, seus dispositivos serão produzidos na fábrica e as informações do log de controle serão passadas para o Amazon Sidewalk, que contém os números de série (SMSN) dos dispositivos. Para obter mais informações sobre esse fluxo de trabalho, consulte [Fabricação de dispositivos Amazon Sidewalk](#) na documentação do Amazon Sidewalk.

É possível provisionar dispositivos Sidewalk em massa fornecendo os números de série dos dispositivos a serem integrados ao AWS IoT Core para Amazon Sidewalk. Quando o AWS IoT Core para Amazon Sidewalk recebe o log de controle, ele compara os números de série no log de controle com os números de série fornecidos. Se os números de série corresponderem, a tarefa de importação começará a integrar os dispositivos ao AWS IoT Core para Amazon Sidewalk. Para ter mais informações, consulte [Provisionamento de dispositivos do Sidewalk usando tarefas de importação](#).

## Provisionamento de dispositivos do Sidewalk usando tarefas de importação

Esta seção mostra como provisionar dispositivos Sidewalk em massa utilizando o console do AWS IoT, as operações de API do AWS IoT Core para Amazon Sidewalk ou a AWS CLI. As seções a seguir explicam como provisionar seus dispositivos do Sidewalk em massa.

### Tópicos

- [Como funciona o provisionamento em massa do Sidewalk](#)
- [Principais considerações sobre o provisionamento em massa do Sidewalk](#)
- [Formato de arquivo CSV](#)
- [Como utilizar o provisionamento em massa do Sidewalk](#)
- [Provisionar dispositivos do Sidewalk em massa](#)
- [Visualizar o status de integração da tarefa de importação e do dispositivo](#)

## Como funciona o provisionamento em massa do Sidewalk

As etapas a seguir ilustram como funciona o provisionamento em massa.

### 1. Iniciar a tarefa de importação de dispositivos sem fio

Para provisionar dispositivos Sidewalk em massa, crie uma tarefa de importação e forneça o número de série de fabricação do Sidewalk (SMSN) dos dispositivos a serem integrados ao AWS IoT Core para Amazon Sidewalk. Você obteve o número de série de fabricação do Sidewalk (SMSN) dos dispositivos como um arquivo CSV em seu e-mail depois que o fabricante fez o upload dos logs de controle para o Amazon Sidewalk. Para obter mais informações sobre o fluxo de trabalho e como obter o log de controle, consulte [Fabricação de dispositivos Amazon Sidewalk](#) na documentação do Amazon Sidewalk.

### 2. Executar o processo de importação em segundo plano

Quando o AWS IoT Core para Amazon Sidewalk recebe a solicitação da tarefa de importação, ele inicia a configuração de coisas e um processo em segundo plano que pesquisa o sistema com frequência. Depois que o processo em segundo plano recebe a instrução da tarefa de importação, ele começa a ler o arquivo CSV. Ao mesmo tempo, o AWS IoT Core para Amazon Sidewalk verifica se os logs de controle foram recebidos do Amazon Sidewalk.

### 3. Criar registros de dispositivos sem fio

Quando o log de controle é recebido do Amazon Sidewalk, o AWS IoT Core para Amazon Sidewalk verifica se os números de série no log de controle correspondem aos valores SMSN no arquivo CSV. Se os números de série corresponderem, o AWS IoT Core para Amazon Sidewalk começará a criar registros de dispositivos sem fio para os dispositivos Sidewalk que corresponderem a esses números de série. Depois que todos os dispositivos estiverem integrados, a tarefa de importação será marcada como Concluída.

## Principais considerações sobre o provisionamento em massa do Sidewalk

Ao provisionar os dispositivos Sidewalk em massa para o AWS IoT Core para Amazon Sidewalk, observe algumas considerações importantes a seguir.

- Execute o provisionamento em massa utilizando o console do AWS IoT ou as operações de API do AWS IoT Core para Amazon Sidewalk na mesma Conta da AWS em que o perfil do dispositivo foi criado.
- Antes de provisionar em massa seus dispositivos do Sidewalk, seu perfil de dispositivo já deve conter informações do DAK que indiquem o suporte de fábrica. Caso contrário, o provisionamento em massa usando o console de AWS IoT ou as operações da API de provisionamento em massa podem falhar.
- Depois que você inicia a tarefa de importação, são necessários 10 minutos ou mais para processar o arquivo CSV, importar os dispositivos sem fio e integrá-los ao AWS IoT Core para Amazon Sidewalk.
- Quando iniciada, a tarefa de importação do dispositivo sem fio será executada por 90 dias. Durante esse período, ela verifica se os logs de controle foram recebidos do Amazon Sidewalk. Se o log de controle não for recebido do Amazon Sidewalk antes de 90 dias, a tarefa será marcada como Concluída, com uma mensagem indicando que ela expirou, quando você visualizar os detalhes da tarefa. O status de integração dos dispositivos na tarefa de importação que estavam aguardando o log de controle será marcado como Falha.
- Ao tentar atualizar uma tarefa de importação criada, você só pode incluir dispositivos adicionais à tarefa. Você pode adicionar novos dispositivos a qualquer momento após criar uma tarefa de importação e antes do início dela em dispositivos que já foram adicionados à tarefa de importação. Se o arquivo de atualização contiver números de série de dispositivos que já existem na tarefa de importação original, esses números de série serão ignorados.
- Quando você solicita uma operação de atualização, o mesmo perfil do IAM utilizado ao criar a tarefa de importação será considerado para acessar o arquivo CSV no bucket do Amazon S3.
- Uma tarefa de importação só poderá ser excluída se a tarefa já tiver sido concluída com êxito ou se houver uma falha em sua atualização. A atualização de uma tarefa pode falhar em casos em que um perfil do IAM incorreto é fornecido ou quando um arquivo de bucket do Amazon S3 não é encontrado. Uma tarefa de importação não poderá ser atualizada ou excluída se estiver no estado PENDING.
- O arquivo CSV que você importa para a tarefa deve usar o formato descrito na seção a seguir.

## Formato de arquivo CSV

O arquivo CSV contido em um bucket do Amazon S3 que você especificar para a tarefa de importação deve usar o seguinte formato:

- A linha 1 deve usar a palavra-chave `smsn`, que indica que o arquivo CSV sendo importado contém o SMSN dos dispositivos a serem importados.
- As linhas 2 e posteriores devem conter o SMSN dos dispositivos a serem integrados. O SMSN do dispositivo deve estar no formato de 64 caracteres hexadecimais.

Esse arquivo JSON mostra um exemplo de formato de arquivo CSV.

```
smsn
1C1A10B0AC0A200C012BBAC2CBB1B21CB12C0CA2AC1C1BB22CAA01C1B0B01122
B122C2B1121BACA2221001AC1B22012AAC11112C11C2A100C1C2B012A1100C10
02B222C110B0A210B0A0C2C112CCCAC21C1C0B0AA1221AB1022A2CC11B1B1122
C2C021CA1C111CCAB1221C0021C1C2AAA0AA1A2A01ABC10CBAACCA2A0121022A
0CB22C01BBC2CA2C0B11001121ACB2ABB0BB0121C2BA101C012CC2B20C011AC0
```

## Como utilizar o provisionamento em massa do Sidewalk

As etapas a seguir mostram como usar o provisionamento em massa do Amazon Sidewalk.

### 1. Forneça os números de série do dispositivo

Para provisionar os dispositivos do Sidewalk, é preciso fornecer os números de série dos dispositivos a serem integrados. Você pode provisionar seus dispositivos usando qualquer um dos métodos a seguir.

- Provisione cada dispositivo individualmente usando o número de série de fabricação do Sidewalk (SMSN). Esse método é útil quando você quer testar o fluxo de trabalho e integrar seu dispositivo mais rapidamente sem precisar carregar um arquivo CSV com o perfil do IAM apropriado ou esperar que os dispositivos estejam prontos para serem integrados à tarefa.
- Provisione os dispositivos em massa fornecendo um URL do bucket do Amazon S3 que contenha o SMSN dos dispositivos a serem provisionados, em um arquivo CSV. Esse método é especialmente útil quando você tem um grande número de dispositivos a serem integrados. Nesse caso, integrar cada dispositivo individualmente pode ser um trabalho maçante. Em vez disso, basta fornecer o caminho para o arquivo CSV que foi carregado em um bucket do Amazon S3 e o perfil do IAM para acessar o arquivo.

## 2. Obter o status de integração da tarefa de importação e do dispositivo

Para cada tarefa de importação criada, você pode recuperar informações sobre o status de integração da tarefa e o status de integração dos dispositivos adicionados a ela. Você também pode ver informações adicionais de status, como o motivo pelo qual a integração de uma tarefa ou dispositivo falharam. Para obter mais informações, consulte

## 3. (Opcional) Atualizar ou excluir uma tarefa de importação

Você pode atualizar ou excluir uma tarefa de importação criada.

- É possível atualizar uma tarefa de importação e adicionar outros dispositivos à tarefa a qualquer momento antes de iniciá-la com os dispositivos já adicionados. O AWS IoT Core para Amazon Sidewalk presume que o perfil do IAM é o mesmo utilizado ao criar a tarefa de importação. Ao criar a tarefa, especifique o novo arquivo CSV que contém os números de série dos dispositivos que você deseja adicionar à tarefa.

### Note

Ao atualizar uma tarefa de importação, só é possível adicionar dispositivos. O AWS IoT Core para Amazon Sidewalk executa uma operação de união entre os dispositivos que já estão na tarefa de importação e aqueles que você está tentando adicionar a ela. Se o novo arquivo contiver números de série de dispositivos que já existem na tarefa de importação, esses números de série serão ignorados.

- Você pode excluir uma tarefa de importação que já foi concluída com êxito ou uma tarefa de importação cuja atualização falhou, em casos como quando as informações do perfil do IAM estão incorretas ou quando um arquivo do bucket do S3 não está disponível quando a tarefa é criada ou atualizada.

## Tópicos

- [Provisionar dispositivos do Sidewalk em massa](#)
- [Visualizar o status de integração da tarefa de importação e do dispositivo](#)

## Provisionar dispositivos do Sidewalk em massa

Esta seção mostra como é possível provisionar dispositivos Sidewalk em massa para o AWS IoT Core para Amazon Sidewalk utilizando o console do AWS IoT e a AWS CLI.

## Provisionar dispositivos do Sidewalk em massa (console)

Para adicionar seu dispositivo do Sidewalk usando o console de AWS IoT, acesse a [guia Sidewalk do hub de dispositivos](#), escolha Provisionar dispositivos em massa e execute as etapas a seguir.

The screenshot shows the AWS IoT console interface for Sidewalk. At the top, there are tabs for 'LoRaWAN' and 'Sidewalk'. Below this is a 'How it works' section with three steps:

- Step 1. Add your Sidewalk device:** First, create a device profile and retrieve the application server public key. Next, create your Sidewalk device and retrieve information about it, including device certificates and private keys.
- Step 2. Provision & register your Sidewalk device:** Provision your hardware as a Sidewalk endpoint by flashing the device certificates and the application server public key that you have generated. Register your device so that it can connect to AWS IoT Core for Amazon Sidewalk.
- Step 3. Connect your Sidewalk endpoint to the cloud:** Create a destination and use [AWS IoT Rules](#) to process and route data to other AWS services. Your endpoint can now exchange messages with your cloud application.

Below the steps is the 'Bulk provision (0) Info' section. It includes a 'Bulk provision devices' button, a search bar labeled 'Find task', and a table with the following headers: Task ID, Creation date, S3 bucket, Success count, Pending count, and Failed count. The table content is currently empty, displaying the message: 'No bulk provisioning tasks are currently running at this time.'

### 1. Escolher o método de importação

Especifique como você deseja importar os dispositivos a serem integrados em massa ao AWS IoT Core para Amazon Sidewalk.

- Para provisionar dispositivos individuais usando o SMSN deles, escolha Provisionar dispositivo individual com suporte de fábrica.
- Para provisionar dispositivos em massa fornecendo um arquivo CSV que contenha uma lista de dispositivos e seus SMS, escolha Usar o bucket do S3.

### 2. Especificar os dispositivos a serem integrados

Dependendo do método escolhido para integrar seus dispositivos, adicione as informações do dispositivo e seus números de série.

- a. Se você escolher Provisionar um dispositivo individual com suporte de fábrica, especifique as seguintes informações:
  - i. Um Nome para cada dispositivo a ser integrado. O nome deve ser exclusivo na sua Conta da AWS e Região da AWS.
  - ii. O número de série de fabricação do Sidewalk (SMSN) no campo Inserir SMSN.
  - iii. Um Destino que descreva a regra de IoT para encaminhar mensagens do dispositivo para outros Serviços da AWS.
- b. Se você escolher Usar bucket do S3:
  - i. Forneça as informações de Destino do S3 Bucket, que consistem nas informações de URL do S3. Para fornecer o arquivo CSV, escolha Procurar no S3 e, em seguida, escolha o arquivo CSV que deseja usar.

O AWS IoT Core para Amazon Sidewalk preenche automaticamente o URL do S3, que é o caminho para o arquivo CSV no bucket do S3. O formato do caminho é `s3://bucket_name/file_name`. Para visualizar o arquivo no console do [Amazon Simple Storage Service](#), selecione Exibir.

- ii. Forneça a Função de provisionamento do S3, que permite que o AWS IoT Core para Amazon Sidewalk acesse o arquivo CSV no bucket do S3 em seu nome. É possível criar um novo perfil de serviço ou escolher um existente.

Para criar um novo perfil, você pode fornecer um Nome de perfil ou deixar em branco, para que um nome aleatório seja gerado automaticamente.

- iii. Forneça um Destino que descreva a regra de IoT para encaminhar mensagens do dispositivo para outros Serviços da AWS.

### 3. Iniciar tarefa de importação

Forneça tags opcionais como pares de nome-valor e escolha Enviar para iniciar a tarefa de importação do dispositivo sem fio.

### Provisionar dispositivos do Sidewalk em massa (CLI)

Para integrar os dispositivos Sidewalk à sua conta para o AWS IoT Core para Amazon Sidewalk, utilize qualquer uma das operações de API a seguir, dependendo do que você deseja fazer: adicionar dispositivos individualmente ou fornecer o arquivo CSV contido em um bucket do S3.

- Fazer upload de dispositivos em massa usando um arquivo CSV do S3

Para fazer upload de dispositivos em massa fornecendo o arquivo CSV em um bucket do S3, use a operação da API [StartWirelessDeviceImportTask](#) ou o comando [start-wireless-device-import-task](#) da AWS CLI. Ao criar a tarefa, especifique o caminho para o arquivo CSV no bucket do Amazon S3 e o perfil do IAM que concede ao AWS IoT Core para Amazon Sidewalk permissões para acessar o arquivo CSV.

Quando a tarefa começar a ser executada, o AWS IoT Core para Amazon Sidewalk começará a ler o arquivo CSV e comparará os números de série (SMSN) no arquivo com as informações correspondentes no log de controle recebido do Amazon Sidewalk. Quando os números de série corresponderem, ele começará a criar registros de dispositivos sem fio que corresponderem a esses números de série.

O comando a seguir mostra um exemplo de criação de uma tarefa de importação:

```
aws iotwireless start-wireless-device-import-task \  
  --cli-input-json "file://task.json"
```

O exemplo a seguir mostra o conteúdo do arquivo `task.json`.

Conteúdo do `task.json`

```
{  
  "DestinationName": "Sidewalk_Destination",  
  "Sidewalk": {  
    "DeviceCreationFile": "s3://import_task_bucket/import_file1",  
    "Role": "arn:aws:iam:123456789012:role/service-role/ACF1zBEI"  
  }  
}
```

A execução desse comando retorna um ID e um ARN para a tarefa de importação.

```
{  
  "Arn": "arn:aws:iotwireless:us-east-1:123456789012:ImportTask/a1b234c5-67ef-21a2-  
a1b2-3cd4e5f6789a"  
  "Id": "a1b234c5-67ef-21a2-a1b2-3cd4e5f6789a"  
}
```

- Provisionar dispositivos individualmente usando o SMSN deles

Para provisionar dispositivos individualmente usando o SMSN deles, use a operação da API [StartSingleWirelessDeviceImportTask](#) ou o comando [start-single-wireless-device-import-task](#) da AWS CLI. Ao criar a tarefa, especifique o destino do Sidewalk e o número de série do dispositivo que você deseja integrar.

Quando o número de série corresponder às informações no log de controle recebido do Amazon Sidewalk, a tarefa será executada e criará o registro do dispositivo sem fio.

O comando a seguir mostra um exemplo de criação de uma tarefa de importação:

```
aws iotwireless start-single-wireless-device-import-task \  
  --destination-name sidewalk_destination \  
  --sidewalk  
'{"SidewalkManufacturingSn": "82B83C8B35E856F43CE9C3D59B418CC96B996071016DB1C3BE5901F0F3071A"
```

A execução desse comando retorna um ID e um ARN para a tarefa de importação.

```
{  
  "Arn": "arn:aws:iotwireless:us-east-1:123456789012:ImportTask/e2a5995e-743b-41f2-a1e4-3ca6a5c5249f"  
  "Id": "e2a5995e-743b-41f2-a1e4-3ca6a5c5249f"  
}
```

## Atualizar ou excluir tarefas de importação

Se quiser adicionar mais dispositivos a uma tarefa de importação, você poderá atualizá-la. Você também pode excluir uma tarefa se não precisar mais dela ou se ela falhar. Para obter informações sobre quando atualizar ou excluir uma tarefa, consulte [Como utilizar o provisionamento em massa do Sidewalk](#).

### Warning

Uma ação de exclusão é permanente e não pode ser desfeita. A exclusão de uma tarefa de importação que já tinha sido concluída com êxito não removerá os dispositivos finais que a utilizaram para a integração.

## Atualizar ou excluir tarefas de importação:

- Usar o console de AWS IoT

As etapas a seguir explicam como atualizar ou excluir suas tarefas de importação usando o console de AWS IoT.

Atualizar uma tarefa de importação:

1. Acesse o [hub de dispositivos do Sidewalk](#) no console de AWS IoT.
2. Escolha a tarefa de importação que você deseja atualizar e, em seguida, escolha Editar.
3. Forneça outro arquivo S3 que contenha os números de série dos dispositivos que você deseja adicionar à tarefa e escolha Enviar.

Excluir uma tarefa de importação:

1. Acesse o [hub de dispositivos do Sidewalk](#) no console de AWS IoT.
2. Escolha a tarefa que você deseja excluir e, em seguida, escolha Excluir.

- Utilizar a API do AWS IoT Wireless ou a AWS CLI

Utilize as operações de API do AWS IoT Wireless ou os comandos da CLI a seguir para atualizar ou excluir a tarefa de importação.

- API [UpdateWirelessDeviceImportTask](#) ou CLI [update-wireless-device-import-task](#)

Essa operação da API anexa o conteúdo de um arquivo CSV do Amazon S3 a uma tarefa de importação existente. Você só pode adicionar números de série de dispositivos que não foram incluídos anteriormente na tarefa.

- API [DeleteWirelessDeviceImportTask](#) ou CLI [delete-wireless-device-import-task](#)

Essa operação da API exclui a tarefa de importação que foi marcada para exclusão usando o ID da tarefa de importação.

## Visualizar o status de integração da tarefa de importação e do dispositivo

As tarefas de importação do seu dispositivo sem fio e dispositivos do Sidewalk que você adicionou à tarefa podem apresentar uma das seguintes mensagens de status. Você verá essas mensagens exibidas no console do AWS IoT ou ao utilizar qualquer uma das operações de API do AWS IoT

Wireless ou qualquer um dos comandos da AWS CLI para recuperar informações sobre essas tarefas e os respectivos dispositivos.

Visualizar informações sobre o status da tarefa de importação

Depois de criar uma tarefa de importação, você pode visualizá-la, juntamente com o status de integração dos dispositivos adicionados a ela. O status de integração indica o número de dispositivos com integração pendente, o número de dispositivos integrados com sucesso e os cuja integração falhou.

Quando a criação de uma tarefa de importação tiver sido concluída, a Contagem de pendentes exibirá um valor correspondente ao número de dispositivos adicionados. Depois que a tarefa for iniciada e ler o arquivo CSV para criar os registros do dispositivo sem fio, a Contagem de pendentes diminuirá e a Contagem de com sucesso aumentará à medida que os dispositivos forem integrados com sucesso. Se a integração de algum dispositivo falhar, a Contagem de falhas aumentará.

Visualizar o status de integração da tarefa de importação e do dispositivo:

- Usar o console de AWS IoT

No [hub de dispositivos do Sidewalk](#) do console de AWS IoT, você conseguirá ver as tarefas de importação criadas e uma contagem do resumo das informações de status de integração de seus dispositivos. Se você visualizar os detalhes de qualquer uma das tarefas de importação criadas, poderá ver informações adicionais sobre o status de integração do dispositivo.

- Utilizar a API do AWS IoT Wireless ou a AWS CLI

Para visualiza o status da integração de um dispositivo, utilize qualquer uma das seguintes operações de API do AWS IoT Wireless ou o comando correspondente da AWS CLI.

- API [ListWirelessDeviceImportTasks](#) ou CLI [list-wireless-device-import-tasks](#)

Essa operação de API retorna informações sobre todas as tarefas de importação adicionadas à sua conta do AWS IoT Wireless e o respectivo status. Ele também retorna uma contagem do resumo do status da integração dos dispositivos do Sidewalk nessas tarefas.

- API [ListDevicesForWirelessDeviceImportTask](#) ou CLI [list-devices-for-wireless-device-import-task](#)

Essa operação da API retorna informações sobre a tarefa de importação especificada e seu status, além de informações sobre todos os dispositivos do Sidewalk adicionados à tarefa de importação e suas informações de status da integração.

- API [GetWirelessDeviceImportTask](#) ou CLI [get-wireless-device-import-task](#)

Essa operação da API retorna informações sobre a tarefa de importação especificada e seu status, além de uma contagem de resumo do status da integração dos dispositivos do Sidewalk nessa tarefa.

## Status da tarefa de importação

As tarefas de importação que você criou em sua Conta da AWS podem apresentar uma das seguintes mensagens de status. O status indica se sua tarefa de importação teve o processamento iniciado, foi concluída ou falhou. Também é possível utilizar o console do AWS IoT ou o parâmetro `StatusReason` de qualquer operação de API do AWS IoT Wireless para recuperar detalhes adicionais de status.

- INICIALIZANDO

O AWS IoT Core para Amazon Sidewalk recebeu a solicitação da tarefa de importação do dispositivo sem fio e está configurando a tarefa.

- INICIALIZADA

O AWS IoT Core para Amazon Sidewalk concluiu a configuração da tarefa de importação e está aguardando a chegada do log de controle para poder importar os dispositivos utilizando os respectivos números de série (SMSN) e continuar a processar a tarefa.

- PENDENTE

A tarefa de importação está esperando na fila para ser processada. O AWS IoT Core para Amazon Sidewalk está avaliando outras tarefas que estão na fila de processamento.

- COMPLETA

A tarefa de importação foi processada e concluída.

- COM FALHA

Falha na tarefa de importação ou do dispositivo. Você pode usar o parâmetro `StatusReason` para identificar por que a tarefa de importação falhou, como uma exceção de validação.

- EXCLUINDO

A tarefa de importação foi marcada para exclusão e está em processo de exclusão.

## Status de integração do dispositivo

Os dispositivos do Sidewalk que você adicionou à tarefa de importação podem apresentar uma das seguintes mensagens de status. O status indica se seus dispositivos estão prontos para serem integrados, foram integrados ou falharam na integração. Também é possível utilizar o console do AWS IoT ou o parâmetro `OnboardingStatusReason` da operação de API `ListDevicesForWirelessDeviceImportTask` do AWS IoT Wireless para recuperar detalhes adicionais de status.

- INICIALIZADA

O AWS IoT Core para Amazon Sidewalk concluiu a configuração da tarefa de importação e está aguardando a chegada do log de controle para poder importar os dispositivos utilizando os respectivos números de série (SMSN) e continuar a processar a tarefa.

- PENDENTE

A tarefa de importação está esperando na fila para ser processada e para iniciar a integração dos dispositivos à tarefa. O AWS IoT Core para Amazon Sidewalk está avaliando outras tarefas que estão na fila de processamento.

- INTEGRADA

O dispositivo do Sidewalk foi integrado com sucesso à tarefa de importação.

- COM FALHA

A tarefa de importação ou tarefa do dispositivo falhou e o dispositivo do Sidewalk falhou ao se integrar à tarefa. Você pode usar o parâmetro `OnboardingStatusReason` para recuperar detalhes adicionais sobre por que a integração do dispositivo falhou.

# Segurança no AWS IoT Wireless

A segurança na nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você contará com um datacenter e uma arquitetura de rede criados para atender aos requisitos das organizações com as maiores exigências de segurança.

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

- **Segurança da nuvem:** AWS é responsável pela proteção da infraestrutura que executa serviços da AWS na Nuvem AWS. A AWS também fornece serviços que podem ser usados com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos [AWS Programas de Conformidade](#). Para saber mais sobre os programas de conformidade que se aplicam ao AWS IoT Wireless, consulte [Serviços da AWS em escopo por programa de conformidade](#).
- **Segurança na nuvem:** sua responsabilidade é determinada pelo serviço da AWS que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a compreender como aplicar o Modelo de Responsabilidade Compartilhada ao utilizar o AWS IoT Wireless. Ela mostra como configurar o AWS IoT Wireless para atender aos objetivos de segurança e conformidade. Você também aprenderá a utilizar outros serviços da AWS que ajudam a monitorar e proteger os recursos do AWS IoT Wireless.

## Conteúdo

- [Proteção de dados no AWS IoT Wireless](#)
- [Gerenciamento de identidades e acesso do AWS IoT Wireless](#)
- [Validação de conformidade do AWS IoT Wireless](#)
- [Resiliência no AWS IoT Wireless](#)
- [Segurança da infraestrutura no AWS IoT Wireless](#)

# Proteção de dados no AWS IoT Wireless

O [Modelo de Responsabilidade Compartilhada](#) da AWS se aplica à proteção de dados no AWS IoT Wireless. Conforme descrito nesse modelo, a AWS é responsável por proteger a infraestrutura global que executa toda a 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 Serviços da AWS que usa. Para ter mais informações sobre a privacidade de dados, consulte as [Perguntas frequentes sobre privacidade de dados](#). Para ter 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 as credenciais da Conta da AWS e configure as contas de usuário individuais com o Centro de Identidade do AWS IAM ou o 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 da AWS. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure o registro em log das atividades da API e do usuário com o AWS CloudTrail.
- Use as soluções de criptografia da AWS, juntamente com todos os controles de segurança padrão dos Serviços da AWS.
- 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 a AWS por meio de uma interface de linha de comando ou uma API, use um endpoint do FIPS. Para ter mais informações sobre endpoints do FIPS, 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 trabalhar com o AWS IoT Wireless ou outros Serviços da AWS utilizando o console, a API, a AWS CLI ou os SDKs da AWS. 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 de dados no AWS IoT Wireless

Por padrão, todos os dados em trânsito e em repouso do AWS IoT Wireless são criptografados. O AWS IoT Wireless não é compatível com as chaves do AWS KMS gerenciadas pelo cliente do AWS KMS key. Para criptografar os dados, o AWS IoT Wireless utiliza apenas uma Chave pertencente à AWS.

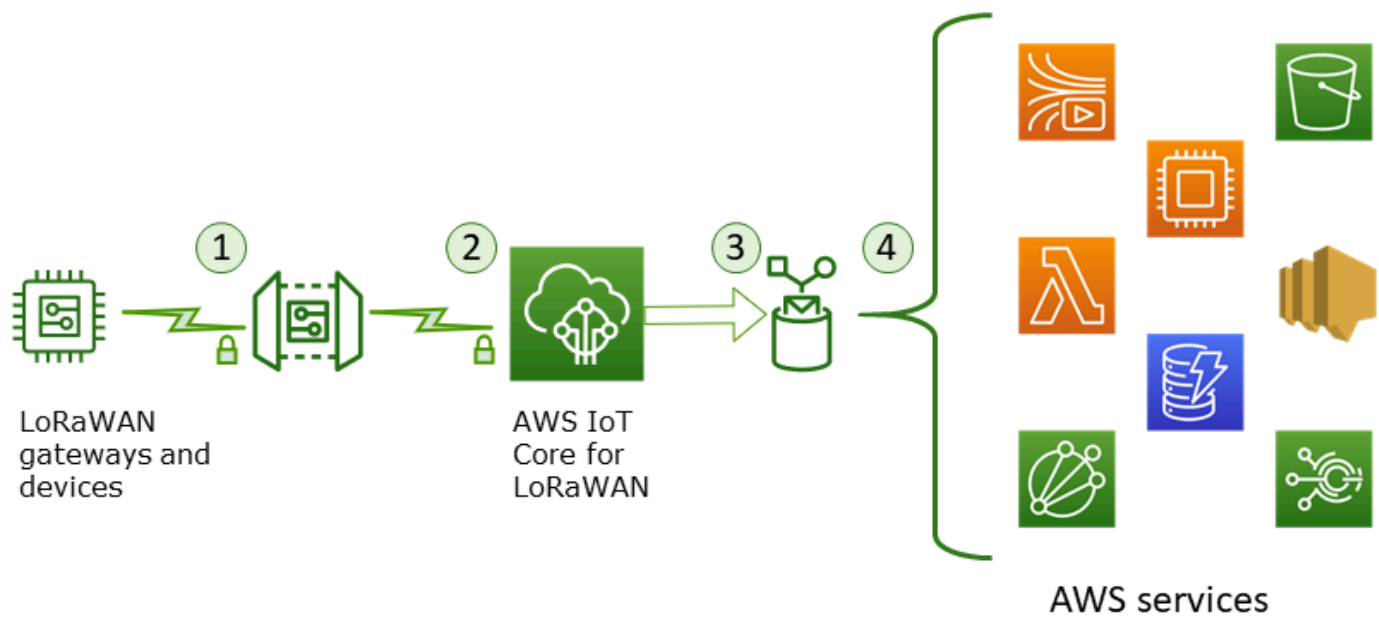
## Segurança de dados e de transporte com o AWS IoT Core for LoRaWAN

O AWS IoT Core for LoRaWAN utiliza os seguintes métodos para proteger os dados e a comunicação entre dispositivos e gateways LoRaWAN e o AWS IoT Core for LoRaWAN:

- As práticas recomendadas de segurança que os dispositivos seguem ao se comunicarem com os gateways LoRaWAN, conforme descrito no whitepaper [LoRaWAN Security](#).
- A segurança que o AWS IoT Core utiliza para conectar gateways ao AWS IoT Core for LoRaWAN e enviar os dados a outros serviços da AWS. Para obter mais informações, consulte [Data protection in AWS IoT Core](#).

### Como os dados são protegidos em todo o sistema

Este diagrama identifica os principais elementos em um sistema LoRaWAN conectado ao AWS IoT Core for LoRaWAN para identificar como os dados são protegidos como um todo.



1. O dispositivo sem fio LoRaWAN criptografa as mensagens binárias usando o modo AES128 CTR antes de transmiti-las.
2. As conexões de gateway ao AWS IoT Core for LoRaWAN são protegidas por TLS, conforme descrito em [Transport security in AWS IoT](#). O AWS IoT Core for LoRaWAN descriptografa a mensagem binária e codifica a carga útil da mensagem binária descriptografada como uma string base64.
3. A mensagem codificada em base64 resultante é enviada como carga útil da mensagem para a regra AWS IoT descrita no destino atribuído ao dispositivo. Os dados na AWS são criptografados usando as chaves pertencentes à AWS.
4. A regra de AWS IoT direciona os dados da mensagem para os serviços descritos na configuração da regra. Os dados na AWS são criptografados usando as chaves pertencentes à AWS.

## Segurança de transporte de dispositivos e gateways LoRaWAN

Os dispositivos LoRaWAN e o AWS IoT Core for LoRaWAN armazenam chaves raiz pré-compartilhadas. As chaves de sessão são derivadas dos dispositivos LoRaWAN e do AWS IoT Core for LoRaWAN de acordo com os protocolos. As chaves de sessão simétricas são usadas para criptografia e descriptografia em um modo CTR AES-128 padrão. Um código de integridade de mensagem (MIC) de 4 bytes também é usado para verificar a integridade dos dados seguindo um algoritmo CMAC AES-128 padrão. As chaves de sessão podem ser atualizadas usando o processo Join/Rejoin.

A prática de segurança para gateways LoRa é descrita nas especificações do LoRaWAN. Os gateways LoRa se conectam ao AWS IoT Core for LoRaWAN por meio de um soquete da web utilizando [Basics Station](#). O AWS IoT Core for LoRaWAN é compatível somente com o Basics Station versão 2.0.4 e posterior.

Para que a conexão do soquete da web seja estabelecida, o AWS IoT Core for LoRaWAN utiliza o [Modo de autenticação de servidor e cliente TLS](#) para autenticar o gateway. Para garantir a confidencialidade do protocolo LoRaWAN, o [TLS versão 1.2](#) é utilizado. O suporte ao TLS está disponível em várias de linguagens de programação e sistemas operacionais. Os dados na AWS são criptografados pelo serviço da AWS específico. Para obter mais informações sobre criptografia de dados em outros serviços da AWS, consulte a documentação de segurança desse serviço.

Por padrão, o AWS IoT Core for LoRaWAN também mantém um Servidor de Configuração e Atualização (CUPS) para configurar e atualizar os certificados e chaves utilizados para a autenticação TLS.

## Gerenciamento de identidades e acesso do AWS IoT Wireless

O AWS Identity and Access Management (IAM) é um AWS service (Serviço da AWS) que ajuda a controlar o acesso aos recursos da AWS de forma segura. Os administradores do IAM controlam quem pode ser autenticado (fazer login) e autorizado (ter permissões) para utilizar os recursos do AWS IoT Wireless. O IAM é um AWS service (Serviço da AWS) que pode ser usado sem custo adicional.

### Tópicos

- [Público](#)
- [Autenticando com identidades](#)
- [Gerenciamento do acesso usando políticas](#)
- [Como funciona o AWS IoT Wireless com o IAM](#)
- [Exemplos de políticas baseadas em identidade do AWS IoT Wireless](#)
- [Políticas gerenciadas pela AWS do AWS IoT Wireless](#)
- [Solução de problemas de identidade e acesso do AWS IoT Wireless](#)

## Público

O uso do AWS Identity and Access Management (IAM) varia de acordo com o trabalho realizado no AWS IoT Wireless.

Usuário do serviço: se você utilizar o serviço AWS IoT Wireless para fazer seu trabalho, o administrador fornecerá as credenciais e as permissões necessárias. À medida que utilizar mais recursos do AWS IoT Wireless para fazer seu trabalho, você poderá precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudá-lo a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um recurso no AWS IoT Wireless, consulte [Solução de problemas de identidade e acesso do AWS IoT Wireless](#).

Administrador do serviço: se você for o responsável pelos recursos do AWS IoT Wireless na empresa, provavelmente terá acesso total ao AWS IoT Wireless. Cabe a você determinar quais funcionalidades e recursos do AWS IoT Wireless 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 sua empresa pode utilizar o IAM com o AWS IoT Wireless, consulte [Como funciona o AWS IoT Wireless com o IAM](#).

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

## Autenticando com identidades

A autenticação é a forma como você faz login na AWS usando suas credenciais de identidade. É necessário ser autenticado (fazer login na AWS) como o usuário raiz da Usuário raiz da conta da AWS, como usuário do IAM ou assumindo um perfil do IAM.

Você pode fazer login na AWS como uma identidade federada usando credenciais fornecidas por uma fonte de identidades. Centro de Identidade do AWS IAM Os usuários do IAM Identity Center, a autenticação única da empresa e as suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como uma identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Quando você acessa a AWS usando a federação, está indiretamente assumindo um perfil.

É possível fazer login no Console de gerenciamento da AWS ou no portal de acesso da AWS dependendo do tipo de usuário que você é. Para obter mais informações sobre como fazer login na

AWS, consulte [Como fazer login na conta da Conta da AWS](#) no Guia do usuário do Início de Sessão da AWS.

Se você acessar a AWS programaticamente, a AWS fornecerá um kit de desenvolvimento de software (SDK) e uma interface da linha de comando (CLI) para você assinar criptograficamente as solicitações usando as suas credenciais. Se você não utilizar as ferramentas da AWS, deverá assinar as solicitações por conta própria. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte [Assinar solicitações de API da AWS](#) no Guia do usuário do IAM.

Independentemente do método de autenticação usado, também pode ser exigido que você forneça mais informações de segurança. Por exemplo, a AWS recomenda o uso da autenticação multifator (MFA) para aumentar a segurança de sua conta. Para saber mais, consulte [Autenticação multifator](#) no Guia Centro de Identidade do AWS IAM do usuário. [Usar a autenticação multifator \(MFA\) na AWS](#) no Guia do usuário do IAM.

## Usuário root da Conta da AWS

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos os recursos e Serviços da AWS na conta. Essa identidade, denominada usuário raiz da Conta da AWS, e é acessada por 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 pode 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.

## Grupos e usuários do IAM

Um [usuário do IAM](#) é uma identidade dentro da Conta da AWS que tem permissões específicas para uma única pessoa ou aplicação. Sempre que possível, recomendamos depender de 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 atribuir a esse grupo permissões para administrar recursos do IAM.

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

## Funções do IAM

### Note

O AWS IoT Wireless não é compatível com perfis de serviço e perfis vinculados a serviço.

Um [perfil do IAM](#) é uma identidade dentro da Conta da AWS que tem permissões específicas. Ela é semelhante a um usuário do IAM, mas não está associada a uma pessoa específica. É possível assumir temporariamente um perfil do IAM no Console de gerenciamento da AWS [alternando perfis](#). É possível assumir um perfil chamando uma operação de API da AWS CLI ou da AWS, ou usando um URL personalizado. Para obter mais informações sobre métodos para o uso de perfis, consulte [Usar perfis do IAM](#) no Guia do usuário do IAM.

Os perfis 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 IAM Identity Center, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte [Conjuntos de permissões](#) no Guia do usuário do Centro de Identidade do AWS IAM.
- **Permissões temporárias para usuários do IAM:** um usuário ou um perfil do IAM pode assumir 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. As funções são a principal

forma de conceder acesso entre contas. No entanto, alguns Serviços da AWS permitem que você anexe uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recurso para acesso entre contas, consulte [Como as funções do IAM diferem das políticas baseadas em recurso](#) no Guia do usuário do IAM.

- Acesso entre serviços: alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações 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 ao serviço.
- Encaminhamento de sessões de acesso (FAS): qualquer pessoa que utilizar uma função ou usuário do IAM para realizar ações na AWS é considerada uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O recurso FAS utiliza as permissões da entidade principal que chama um AWS service (Serviço da AWS), combinadas às permissões do AWS service (Serviço da AWS) solicitante, para realizar solicitações para serviços downstream. As solicitações de FAS só são feitas quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. 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: 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 \(Serviço da AWS\)](#) no Guia do usuário do IAM.
- Perfil vinculado ao serviço: um perfil vinculado ao serviço é um tipo de perfil de serviço vinculado a um AWS service (Serviço da AWS). O serviço pode assumir o perfil para executar uma ação em seu nome. Os perfis vinculados ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados a serviço.
- Aplicações em execução no Amazon EC2: é possível usar um perfil do IAM para gerenciar credenciais temporárias para aplicações em execução em uma instância do EC2 e fazer solicitações da AWS CLI ou da AWS API. É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma função da AWS a uma instância do EC2 e disponibilizá-la para todas as suas aplicações, crie um perfil de instância que esteja anexado a ela. Um perfil de instância contém a função e permite que os programas em execução na instância do EC2

obtenham credenciais temporárias. Para mais informações, consulte [Usar 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 os perfis do IAM, consulte [Quando criar um perfil do IAM \(em vez de um usuário\)](#) no Guia do usuário do IAM.

## Gerenciamento do acesso usando políticas

Você controla o acesso na AWS criando políticas e anexando-as a identidades ou recursos da AWS. Uma política é um objeto na AWS que, quando associado a uma identidade ou recurso, define suas permissões. A AWS avalia essas políticas quando uma entidade 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 são armazenadas na 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 AWS as políticas JSON da para especificar quem tem acesso a 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 permissão para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM a perfis, e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação, independentemente 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 perfis do Console de gerenciamento da AWS, da AWS CLI ou da API da AWS.

### 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, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte [Criar políticas do IAM](#) no Guia do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda mais como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou função. As políticas gerenciadas são políticas independentes que podem ser anexadas a vários usuários, grupos e funções na Conta da AWS. As políticas gerenciadas incluem políticas gerenciadas pela AWS 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 recurso

Políticas baseadas em recurso são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recurso as políticas de confiança de função do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com 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 um principal](#) em uma política baseada em recursos. As entidades principais podem incluir contas, usuários, perfis, usuários federados ou Serviços da AWS.

Políticas baseadas em recursos são políticas em linha que estão localizadas nesse serviço. Não é possível usar as políticas gerenciadas da AWS 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 funções da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

Amazon S3, AWS WAF e Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. 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

A AWS aceita tipos de política 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 recurso 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 e dos seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou a função 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 (UO) no AWS Organizations. O AWS Organizations é um serviço para agrupar e gerenciar centralmente várias Contas da AWS pertencentes à sua empresa. Se você habilitar todos os recursos 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 em contas-membro, incluindo cada Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizations e SCPs, consulte [Como os SCPs funcionam](#) no Guia 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 uma função ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou da função e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recurso. 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 a AWS determina se deve permitir uma solicitação quando há vários tipos de política envolvidos, consulte [Lógica da avaliação](#) de políticas no Guia do usuário do IAM.

## Como funciona o AWS IoT Wireless com o IAM

Antes de utilizar o IAM para gerenciar o acesso ao AWS IoT Wireless, conheça os recursos do IAM que estão disponíveis para utilização com o AWS IoT Wireless. Para obter uma visão geral de como o AWS IoT Wireless e outros serviços da AWS funcionam com o IAM, consulte [Serviços da AWS que funcionam com o IAM](#) no Guia do usuário do IAM.

## atributos do IAM que você pode usar com o AWS IoT Wireless

| atributo do IAM                                  | Suporte a AWS IoT Wireless |
|--------------------------------------------------|----------------------------|
| <a href="#">Políticas baseadas em identidade</a> | Sim                        |
| <a href="#">Políticas baseadas em recursos</a>   | Não                        |
| <a href="#">Ações de políticas</a>               | Sim                        |
| <a href="#">Recursos 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>                | Não                        |
| <a href="#">Perfis vinculados ao serviço</a>     | Não                        |

## Tópicos

- [Políticas baseadas em identidade do AWS IoT Wireless](#)
- [Políticas baseadas em recursos no AWS IoT Wireless](#)
- [Ações de políticas](#)
- [atributos de políticas](#)
- [Chaves de condição](#)
- [Listas de controle de acesso \(ACLs\)](#)
- [ABAC com AWS IoT Wireless](#)
- [Usar credenciais temporárias com o AWS IoT Wireless](#)
- [Permissões de entidade principal entre serviços para o AWS IoT Wireless](#)
- [Perfis de serviço](#)

- [Funções vinculadas ao serviço para o AWS IoT Wireless](#)

## Políticas baseadas em identidade do AWS IoT Wireless

|                                                   |     |
|---------------------------------------------------|-----|
| É 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 funções podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte [Criar 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, bem 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 função à qual ela está anexado. 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

Para visualizar exemplos de políticas baseadas em identidade do AWS IoT Wireless, consulte [Exemplos de políticas baseadas em identidade do AWS IoT Wireless](#).

## Políticas baseadas em recursos no AWS IoT Wireless

|                                                  |     |
|--------------------------------------------------|-----|
| Oferece suporte a políticas baseadas em recursos | Não |
|--------------------------------------------------|-----|

Políticas baseadas em recurso são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recurso as políticas de confiança de função do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com 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 um principal](#) em uma política baseada em recursos. As entidades principais podem incluir contas, usuários, funções, usuários federados ou Serviços da AWS.

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 recurso. Adicionar um principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando a entidade principal e o recurso estão em diferentes Contas da AWS, um administrador do IAM da conta confiável também deve conceder à entidade principal (usuário ou função) permissão 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 um principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte [Como os perfis do IAM diferem de políticas baseadas em recursos](#) no Guia do usuário do IAM.

## Ações de políticas

|                                      |     |
|--------------------------------------|-----|
| Oferece suporte a ações de políticas | Sim |
|--------------------------------------|-----|

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a 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 que a operação de API da AWS associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Há também algumas operações que 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.

As ações de política no AWS IoT Wireless utilizam o seguinte prefixo antes da ação: `iotwireless:`. Por exemplo, para conceder permissão a alguém para listar todos os dispositivos sem fio registrados na Conta da AWS com a operação de API `ListWirelessDevices`, inclua a ação `iotwireless:ListWirelessDevices` na política. As instruções de política devem incluir um elemento `Action` ou `NotAction`. O AWS IoT Wireless define seu próprio conjunto de ações que descrevem as tarefas que você pode executar com o serviço.

Para especificar várias ações em uma única instrução, separe-as com vírgulas, como segue:

```
"Action": [
  "iotwireless:ListMulticastGroups",
  "iotwireless:ListFuotaTasks"
]
```

Você também pode especificar várias ações usando caracteres curinga (\*). Por exemplo, para especificar todas as ações que começam com a palavra Get, inclua a seguinte ação:

```
"Action": "iotwireless:Get*"
```

Para ver uma lista de ações do AWS IoT Wireless, consulte [Actions Defined by AWS IoT Wireless](#) no Guia do usuário do IAM.

## atributos de políticas

|                                         |     |
|-----------------------------------------|-----|
| Oferece suporte a recursos de políticas | Sim |
|-----------------------------------------|-----|

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

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

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

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

O serviço AWS IoT Wireless tem o seguinte ARN:

```
arn:${Partition}:iotwireless:${Region}:${Account}:${Resource}/${Resource-id}
```

Para obter mais informações sobre o formato de ARNs, consulte [Nomes de recursos da Amazon \(ARNs\)AWS e namespaces de serviços da](#)

Por exemplo, para especificar a configuração NAConfig1 do analisador de rede na instrução, utilize o seguinte ARN:

```
"Resource": "arn:aws:iotwireless:us-east-1:123456789012:NetworkAnalyzerConfiguration/NAConfig1"
```

Para especificar todas as tarefas FUOTA que pertencem a uma conta específica, utilize o caractere curinga (\*):

```
"Resource": "arn:aws:iotwireless:us-east-1:123456789012:FuotaTask/*"
```

Algumas ações do AWS IoT Wireless, como para a listagem de recursos, não podem ser executadas em um recurso específico. Nesses casos, você deve utilizar o caractere curinga (\*).

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

Muitas ações da API do AWS IoT Wireless envolvem vários recursos. Por exemplo, AssociateWirelessDeviceWithThing associa um dispositivo sem fio a uma coisa do AWS IoT; portanto, um usuário do IAM deve ter permissões para utilizar o dispositivo e uma coisa de IoT. Para especificar vários recursos em uma única instrução, separe os ARNs com vírgulas.

```
"Resource": [
  "WirelessDevice",
  "thing"
```

Para ver uma lista de tipos dos recurso do AWS IoT Wireless e os respectivos ARNs, consulte [Resources Defined by AWS IoT Wireless](#) no Guia do usuário do IAM. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte [Actions Defined by AWS IoT Wireless](#).

## Chaves de condição

|                                                                      |     |
|----------------------------------------------------------------------|-----|
| Compatível com chaves de condição de política específicas do serviço | Sim |
|----------------------------------------------------------------------|-----|

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

O elemento `Condition` (ou bloco de `Condition`) permite que você especifique condições nas quais uma instrução está em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usam [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 elemento `Condition`, a AWS os avaliará usando uma operação lógica AND. Se você especificar vários valores para uma única chave de condição, a AWS avaliará a condição usando uma operação lógica OR. Todas as condições devem ser atendidas para que as permissões da instrução sejam concedidas.

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

A AWS oferece suporte a chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as AWS chaves de condição globais da , consulte [AWSChaves de contexto de condição globais da](#) no Guia do usuário do IAM.

O AWS IoT Wireless define seu próprio conjunto de chaves de condição e também permite a utilização de algumas chaves de condição globais. Para ver todas as chaves de condição globais da AWS, consulte [Chaves de contexto de condição globais da AWS](#) no Guia do usuário do IAM. Para ver uma lista de chaves de condição do AWS IoT Wireless, consulte [Condition Keys for AWS IoT Wireless](#) no Guia do usuário do IAM. Para saber com quais ações e recursos é possível utilizar uma chave de condição, consulte [Actions Defined by AWS IoT Wireless](#).

## Listas de controle de acesso (ACLs)

Oferece suporte a ACLs

Não

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

## ABAC com AWS IoT Wireless

|                                            |     |
|--------------------------------------------|-----|
| Oferece 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. Na AWS, esses atributos são chamados de tags. É possível anexar tags a entidades do IAM (usuários ou funções) e a muitos recursos da AWS. A marcação de entidades e recursos 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 está tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que 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 `aws:TagKeys` chaves de condição.

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 [Usar controle de acesso baseado em atributos \(ABAC\)](#) no Guia do usuário do IAM.

É possível anexar tags a recursos do AWS IoT Wireless ou transmitir tags em uma solicitação ao AWS IoT Wireless. Para controlar o acesso baseado em tags, forneça informações sobre as tags no [elemento de condição](#) de uma política usando as `YOUR-SERVICE-PREFIX:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys` chaves de condição. Para obter mais informações sobre como fazer a marcação de recursos do AWS IoT Wireless, consulte [Marcando seus Recursos AWS IoT Wireless](#).

## Usar credenciais temporárias com o AWS IoT Wireless

|                                           |     |
|-------------------------------------------|-----|
| Oferece suporte a credenciais temporárias | Sim |
|-------------------------------------------|-----|

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

Você está usando credenciais temporárias se faz login no Console de gerenciamento da AWS usando qualquer método, exceto um nome de usuário e uma senha. Por exemplo, quando você acessa a AWS usando o link de autenticação única (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 funções. Para obter mais informações sobre como alternar funções, consulte [Alternar para uma função \(console\)](#) no Guia do usuário do IAM.

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

## Permissões de entidade principal entre serviços para o AWS IoT Wireless

|                                                                  |     |
|------------------------------------------------------------------|-----|
| Suporte para o recurso Encaminhamento de sessões de acesso (FAS) | Sim |
|------------------------------------------------------------------|-----|

Quando você usa um usuário ou um perfil do IAM para executar ações na AWS, você é considerado uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O recurso FAS utiliza as permissões da entidade principal que chama um AWS service (Serviço da AWS), combinadas às permissões do AWS service (Serviço da AWS) solicitante, para realizar solicitações para serviços downstream. As solicitações de FAS só são feitas quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. 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](#).

## Perfis de serviço

|                                     |     |
|-------------------------------------|-----|
| Oferece suporte a perfis de serviço | Não |
|-------------------------------------|-----|

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 \(Serviço da AWS\)](#) no Guia do usuário do IAM.

## Funções vinculadas ao serviço para o AWS IoT Wireless

Oferece suporte a perfis vinculados ao serviço      Não

Um perfil vinculado ao serviço é um tipo de perfil de serviço vinculado a um AWS service (Serviço da AWS). O serviço pode assumir a função de executar uma ação em seu nome. Os perfis vinculados ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados a serviço.

## Exemplos de políticas baseadas em identidade do AWS IoT Wireless

Por padrão, os usuários e os perfis do IAM não têm permissão para criar ou modificar recursos do AWS IoT Wireless. Eles também não podem executar tarefas usando o Console de gerenciamento da AWS, a AWS CLI ou uma API da AWS. Um administrador do IAM deve criar políticas do IAM que concedam aos usuários e perfis permissão para executarem operações de API específicas nos recursos especificados de que precisam. O administrador deve anexar essas políticas aos usuários ou grupos do IAM que exigem essas permissões.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documentos de política JSON, consulte [Criar políticas na guia JSON](#) no Guia do usuário do IAM.

### Tópicos

- [Práticas recomendadas de políticas](#)
- [Utilizar o console AWS IoT Wireless](#)
- [Permitir que os usuários visualizem suas próprias permissões](#)
- [Permissões necessárias para executar ações em dispositivos sem fio do AWS IoT Wireless](#)

## Práticas recomendadas de políticas

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

- Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo: para começar a conceder permissões a seus usuários e workloads, use as políticas gerenciadas pela AWS que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis na sua Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da AWS 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 recursos 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 escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso a ações de serviço, se elas forem usadas por meio de um AWS service (Serviço da AWS) específico, como o CloudFormation. Para obter mais informações, consulte [Elementos de política JSON do IAM: Condition](#) no Manual 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 ajudar você 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 houver um cenário que exija usuários do IAM ou um usuário raiz em sua Conta da AWS, ative a MFA para obter segurança adicional. Para exigir a 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.

## Utilizar o console AWS IoT Wireless

Para acessar o console do AWS IoT Wireless, é necessário ter um conjunto mínimo de permissões. Essas permissões devem permitir listar e visualizar os detalhes sobre os recursos do AWS IoT Wireless na sua conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis do IAM) com essa política.

Para garantir que essas entidades ainda possam utilizar o console do AWS IoT Wireless, anexe também às entidades a política gerenciada pela AWS a seguir. Para obter mais informações, consulte [Adição de permissões a um usuário](#) no Manual do usuário do IAM:

```
AWSIoTWirelessFullAccess
```

Não é necessário conceder permissões mínimas do console para usuários que fazem chamadas somente à AWS CLI ou à API do AWS. Em vez disso, permita o acesso somente às ações que correspondem à operação da API que você está tentando executar.

## Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permite 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 de forma programática usando a AWS CLI ou a AWS API.

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

```

## Permissões necessárias para executar ações em dispositivos sem fio do AWS IoT Wireless

É possível utilizar condições na política baseada em identidade para controlar o acesso às ações do AWS IoT Wireless. Este exemplo mostra como é possível criar uma política que permite criar e gerenciar dispositivos. No entanto, a permissão é concedida somente se a tag do objeto `Owner` tiver o valor do nome de usuário desse usuário. Essa política também concede as permissões necessárias concluir essa ação no console.

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "VisualEditor0",
    "Effect": "Allow",
    "Action": [
      "iotwireless:CreateWirelessDevice",
      "iotwireless:GetWirelessDevice",
      "iotwireless:ListWirelessDevices",
      "iotwireless:UpdateWirelessDevice",
      "iotwireless>DeleteWirelessDevice"
    ],
    "Resource": "*"
  }
]

```

```
}
```

A política tem uma declaração que concede permissão para utilizar as ações `CreateWirelessDevice`, `GetWirelessDevice`, `ListWirelessDevices`, `UpdateWirelessDevice` e `DeleteWirelessDevice`. O AWS IoT Wireless chama esses métodos para criar e gerenciar os dispositivos sem fio.

A política não especifica o elemento da entidade principal porque você não especifica a entidade principal que obtém a permissão em uma política baseada em identidade. Quando você anexar uma política a um usuário, o usuário será a entidade principal implícita. Quando você anexa uma política de permissões a um perfil do IAM, a entidade principal identificada na política de confiança do perfil obtém as permissões.

## Políticas gerenciadas pela AWS do AWS IoT Wireless

Para adicionar permissões a usuários, grupos e perfis, é mais fácil usar políticas gerenciadas pela AWS do que gravar políticas por conta própria. 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 gerenciadas pela AWS. Essas políticas abrangem casos de uso comuns e estão disponíveis na sua Conta da AWS. Para obter mais informações sobre as políticas gerenciadas da AWS, consulte [Políticas gerenciadas da AWS](#) no IAM User Guide.

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

Além disso, a AWS oferece suporte a políticas gerenciadas para perfis de trabalho que abrangem vários serviços. Por exemplo, a política gerenciada pela AWS denominada `ReadOnlyAccess` fornece acesso somente leitura a todos os serviços e recursos da AWS. Quando um serviço executa um novo atributo, a AWS adiciona permissões somente leitura para novas operações e recursos. Para

obter uma lista e descrições das políticas de perfis de trabalho, consulte [Políticas gerenciadas pela AWS para perfis de trabalho](#) no Guia do usuário do IAM.

## Política gerenciada da AWS: AWSIoTWirelessDataAccess

É possível anexar a política `AWSIoTWirelessDataAccess` a suas identidades do IAM.

Essa política concede as permissões de identidade associadas que permitem acesso para enviar dados a dispositivos LoRaWAN e Sidewalk utilizando a API `SendDataToWirelessDevice`.

Para visualizar essa política no Console de gerenciamento da AWS, consulte [AWSIoTWirelessDataAccess](#).

### Detalhes das permissões

Esta política inclui as seguintes permissões.

- `iotwireless`: recuperar dados do AWS IoT Wireless.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iotwireless:SendDataToWirelessDevice"
      ],
      "Resource": "*"
    }
  ]
}
```

## Política gerenciada da AWS: AWSIoTWirelessFullAccess

É possível anexar a política `AWSIoTWirelessFullAccess` a suas identidades do IAM.

Essa política concede as permissões de identidade associadas que permitem acesso a todas as operações de dados do AWS IoT Wireless. Para visualizar essa política no Console de gerenciamento da AWS, consulte [AWSIoTWirelessFullAccess](#).

### Detalhes das permissões

Esta política inclui as seguintes permissões.

- `iotwireless`: recuperar dados do AWS IoT Wireless e executar todas as operações do AWS IoT Wireless.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iotwireless:*"
      ],
      "Resource": "*"
    }
  ]
}
```

### Política gerenciada da AWS: `AWSIoTWirelessFullPublishAccess`

É possível anexar a política `AWSIoTWirelessFullPublishAccess` a suas identidades do IAM.

Essa política concede as permissões de identidade associadas que permitem acesso limitado para publicar as regras do AWS IoT em seu nome. Para visualizar essa política no Console de gerenciamento da AWS, consulte [AWSIoTWirelessFullPublishAccess](#).

## Detalhes das permissões

Esta política inclui as seguintes permissões.

- `iot`: executar operações que obtêm o URL do endpoint e publicam no mecanismo de regras do AWS IoT.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:DescribeEndpoint",
        "iot:Publish"
      ],
      "Resource": "*"
    }
  ]
}
```

## Política gerenciada da AWS: AWSIoTWirelessLogging

É possível anexar a política `AWSIoTWirelessLogging` a suas identidades do IAM.

Essa política concede as permissões de identidades associadas que permitem a criação de grupos de log do Amazon CloudWatch Logs e de logs de fluxo para os grupos. Essa política está anexada ao seu perfil de registro em log do CloudWatch. Para visualizar essa política no Console de gerenciamento da AWS, consulte [AWSIoTWirelessLogging](#).

## Detalhes das permissões

Esta política inclui as seguintes permissões.

- logs – Recuperar os logs do CloudWatch. Também permite a criação de grupos de logs do CloudWatch e transmissão de logs para os grupos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/iotwireless*"
    }
  ]
}
```

## Política gerenciada da AWS: AWSIoTWirelessReadOnlyAccess

É possível anexar a política AWSIoTLogging a suas identidades do IAM.

Essa política concede as permissões de identidade associada que permitem acesso somente leitura a todas as operações do AWS IoT Wireless. Para visualizar essa política no Console de gerenciamento da AWS, consulte [AWSIoTWirelessReadOnlyAccess](#).

### Detalhes das permissões

Esta política inclui as seguintes permissões.

- logs: executar as operações de API AWS IoT Wireless, List e Get.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iotwireless:List*",
        "iotwireless:Get*"
      ],
      "Resource": "*"
    }
  ]
}
```

## Política gerenciada da AWS: AWSIoTWirelessGatewayCertManager

É possível anexar a política `AWSIoTWirelessGatewayCertManager` a suas identidades do IAM.

Essa política concede permissões de identidade associadas que permitem acesso para criar, listar e descrever certificados do AWS IoT. Para visualizar essa política no Console de gerenciamento da AWS, consulte [AWSIoTWirelessGatewayCertManager](#).

### Detalhes das permissões

Esta política inclui as seguintes permissões.

- `iot`: executar ações que criam, descrevem e listam certificados.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IoTWirelessGatewayCertManager",
      "Effect": "Allow",
```

```
    "Action": [  
      "iot:CreateKeysAndCertificate",  
      "iot:DescribeCertificate",  
      "iot:ListCertificates"  
    ],  
    "Resource": "*"    
  }  
]  
}
```

## AWS IoT Wireless: atualizações em políticas gerenciadas pela AWS.

Visualizar detalhes sobre atualizações em políticas gerenciadas pela AWS para o AWS IoT Wireless desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações realizadas nesta página, assine o feed RSS na [página de histórico do documento do AWS IoT Wireless](#).

| Alteração                                                | Descrição                                                                                  | Data               |
|----------------------------------------------------------|--------------------------------------------------------------------------------------------|--------------------|
| O AWS IoT Wireless iniciou o rastreamento das alterações | O AWS IoT Wireless começou a monitorar as alterações para as políticas gerenciadas da AWS. | 18 de maio de 2022 |

## Solução de problemas de identidade e acesso do AWS IoT Wireless

Utilize as informações a seguir para ajudar a diagnosticar e corrigir problemas comuns que podem ser encontrados ao trabalhar com o AWS IoT Wireless e o IAM.

### Tópicos

- [Não tenho autorização para executar uma ação no AWS IoT Wireless](#)
- [Quero visualizar minhas chaves de acesso](#)
- [Sou administrador e desejo conceder acesso ao AWS IoT Wireless a outros usuários.](#)
- [Desejo permitir que pessoas fora da minha conta da AWS acessem meus recursos do AWS IoT Wireless](#)

## Não tenho autorização para executar uma ação no AWS IoT Wireless

Se o Console de gerenciamento da AWS informar que você não foi autorizado a executar uma ação, você deve entrar em contato com o administrador para obter assistência. O administrador é a pessoa que forneceu o seu nome de usuário e senha.

O exemplo de erro a seguir ocorre quando o usuário do IAM mateojackson tenta utilizar o console para visualizar detalhes sobre um *WirelessDevice* e não tem as permissões YOUR-SERVICE-PREFIX:*GetWirelessDevice*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: YOUR-SERVICE-PREFIX:GetWirelessDevice on resource: my-LoRaWAN-device
```

Neste caso, Mateo pede ao administrador para atualizar suas políticas para permitir a ele o acesso ao recurso *my-LoRaWAN-device* usando a ação YOUR-SERVICE-PREFIX:*GetWirelessDevice*.

## Quero visualizar minhas chaves de acesso

Depois de criar suas chaves de acesso de usuário do IAM, é possível visualizar seu ID da chave de acesso a qualquer momento. No entanto, você não pode visualizar sua chave de acesso secreta novamente. Se você perder sua chave secreta, crie um novo par de chaves de acesso.

As chaves de acesso consistem em duas partes: um ID de chave de acesso (por exemplo, AKIAIOSFODNN7EXAMPLE) e uma chave de acesso secreta (por exemplo, wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY). Como um nome de usuário e uma senha, você deve usar o ID da chave de acesso e a chave de acesso secreta em conjunto para autenticar suas solicitações. Gerencie suas chaves de acesso de forma tão segura quanto você gerencia seu nome de usuário e sua senha.

### Important

Não forneça as chaves de acesso a terceiros, mesmo que seja para ajudar a [encontrar o ID de usuário canônico](#). Ao fazer isso, você pode dar a alguém acesso permanente a sua Conta da AWS.

Ao criar um par de chaves de acesso, você é solicitado a guardar o ID da chave de acesso e a chave de acesso secreta em um local seguro. A chave de acesso secreta só está disponível no momento em que é criada. Se você perder sua chave de acesso secreta, será necessário adicionar novas

chaves de acesso para seu usuário do IAM. Você pode ter no máximo duas chaves de acesso. Se você já tiver duas, você deverá excluir um par de chaves para poder criar um novo. Para visualizar as instruções, consulte [Gerenciar chaves de acesso](#) no Guia do usuário do IAM.

Sou administrador e desejo conceder acesso ao AWS IoT Wireless a outros usuários.

Para permitir que outros usuários acessem o AWS IoT Wireless, é necessário criar uma entidade do IAM (usuário ou perfil) para a pessoa ou a aplicação que precisa do acesso. Elas usarão as credenciais dessa entidade para acessar a AWS. Você deve anexar uma política à entidade que conceda as permissões corretas no AWS IoT Wireless.

Para começar a usar imediatamente, consulte [Criar os primeiros usuário e grupo delegados pelo IAM](#) no Guia do usuário do IAM.

## Desejo permitir que pessoas fora da minha conta da AWS acessem meus recursos do AWS IoT Wireless

É possível criar um perfil que os usuários de outras contas ou pessoas fora da sua organização possam utilizar para acessar seus recursos. Você pode especificar quem é confiável para assumir a função. Para serviços que oferecem suporte a 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 AWS IoT Wireless é compatível com esses recursos, consulte [Como funciona o AWS IoT Wireless com o IAM](#).
- Para saber como conceder acesso a seus atributos em todas as Contas da AWS pertencentes a você, consulte [Fornecimento de acesso a um usuário do IAM em outra Conta da AWS pertencente a você](#) no Guia de usuário do IAM.
- Para saber como conceder acesso a seus recursos para terceiros Contas da AWS, consulte [Fornecimento de acesso a Contas da AWS pertencentes 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 usar perfis e políticas baseadas em recursos para acesso entre contas, consulte [Como os perfis do IAM diferem de políticas baseadas em recursos](#) no Guia do usuário do IAM.

## Validação de conformidade do AWS IoT Wireless

Audidores de terceiros avaliam a segurança e a conformidade do AWS IoT Wireless como parte de vários programas de conformidade da AWS. Isso inclui SOC, PCI, FedRAMP, HIPAA e outros.

Para obter uma lista de serviços da AWS no escopo de programas de conformidade específicos, consulte [Serviços da AWS no escopo pelo programa de conformidade](#). Para obter informações gerais, consulte [Programas de conformidade da AWS](#).

É possível fazer download de relatórios de auditoria de terceiros usando o AWS Artifact. Para obter mais informações, consulte [Downloading Reports in AWS Artifact](#).

Sua responsabilidade pela conformidade ao utilizar o AWS IoT Wireless é determinada pela confidencialidade dos dados, pelos objetivos de conformidade da empresa e pelos regulamentos e leis aplicáveis. A AWS oferece os seguintes recursos para contribuir para a conformidade:

- [Guias de início rápido de segurança e compatibilidade](#): estes guias de implantação abordam as considerações de arquitetura e fornecem etapas para implantação de ambientes de linha de base focados em compatibilidade e segurança na AWS.
- [Whitepaper Architecting for HIPAA Security and Compliance](#): este whitepaper descreve como as empresas podem usar a AWS para criar aplicações em conformidade com a HIPAA.
- [Recursos de conformidade da AWS](#): essa coleção de manuais e guias pode ser aplicada a seu setor e local.
- [Avaliar recursos com regras](#) no AWS Config Guia do desenvolvedor: AWS Config; avalia como suas configurações de recursos estão em conformidade com práticas internas, diretrizes do setor e regulamentos.
- [AWS Security Hub CSPM](#): esse serviço da AWS fornece uma visão abrangente do estado da segurança na AWS que ajuda verificar a conformidade com os padrões e as práticas recomendadas de segurança do setor.

## Resiliência no AWS IoT Wireless

A infraestrutura global da AWS é criada com base em regiões e zonas de disponibilidade da AWS. As regiões fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, que são conectadas com baixa latência, alta throughput e redes altamente redundantes. Com as zonas de disponibilidade, é possível projetar e operar aplicações 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 datacenter tradicionais.

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

## Segurança da infraestrutura no AWS IoT Wireless

Como serviço gerenciado, o AWS IoT Wireless é protegido pelos procedimentos de segurança da rede global da AWS descritos no whitepaper [Amazon Web Services: Overview of Security Processes](#).

Utilize as chamadas de API publicadas pela AWS para acessar o AWS IoT Wireless por meio da rede. Os clientes devem oferecer suporte a Transport Layer Security (TLS) 1.0 ou posterior. Recomendamos TLS 1.2 ou posterior. Os clientes também devem ter suporte a 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 suporte a 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.

# Monitorar os recursos do AWS IoT Wireless utilizando o Amazon CloudWatch Logs

O monitoramento é uma parte importante da manutenção da confiabilidade, da disponibilidade e do desempenho do AWS IoT Wireless e de outras soluções da AWS. É possível utilizar o monitoramento de dispositivos LoRaWAN e Sidewalk e obter mensagens informativas e erros referentes à integração com o AWS IoT Wireless.

É altamente recomendável que você colete dados de monitoramento de todas as partes da solução da AWS para facilitar a depuração de uma falha de vários pontos, caso ocorra. Comece criando um plano de monitoramento que responda às seguintes perguntas. Se não tiver certeza de como respondê-las, você ainda poderá continuar a habilitar o registro em log e estabelecer suas linhas de base de desempenho.

- Quais são seus objetivos de monitoramento?
- Quais recursos você vai monitorar?
- Com que frequência você vai monitorar esses recursos?
- Quais ferramentas de monitoramento você usará?
- Quem realizará o monitoramento das tarefas?
- Quem deve ser notificado quando algo der errado?

A próxima etapa é habilitar o registro em log e estabelecer um parâmetro de desempenho normal do AWS IoT Wireless no ambiente medindo o desempenho em vários momentos e em diferentes condições de carga. Ao monitorar o AWS IoT Wireless, mantenha os dados históricos de monitoramento para que você possa compará-los com os dados de desempenho atuais. Isso ajuda a identificar padrões normais e anomalias de desempenho e a criar métodos para tratar os problemas.

## Ferramentas de monitoramento

É possível utilizar as seguintes ferramentas de monitoramento para observar o AWS IoT Wireless, informar quando algo está errado e executar ações automáticas quando apropriado:

- O Amazon CloudWatch monitora os recursos da AWS e as aplicações que você executa na AWS em tempo real. É possível coletar e rastrear métricas, criar painéis personalizados e definir

alarmes que o notificam ou que realizam ações quando uma métrica especificada atinge um limite definido. Por exemplo, você pode fazer o CloudWatch acompanhar o uso da CPU ou outras métricas das instâncias do Amazon EC2 e iniciar automaticamente novas instâncias quando necessário. Para obter mais informações, consulte o [Guia do usuário do Amazon CloudWatch](#).

- O analisador de rede permite monitorar os recursos LoRaWAN, incluindo dispositivos e gateways LoRaWAN. Ele reduz o tempo necessário para configurar uma conexão para começar a receber mensagens de rastreamento, fornecendo informações de log no momento certo. Para ter mais informações, consulte [Monitorar sua frota de recursos sem fio em tempo real usando o analisador de rede](#).

## Como monitorar recursos utilizando o Amazon CloudWatch

É possível monitorar o AWS IoT Wireless utilizando o CloudWatch, que coleta dados brutos e os processa em métricas legíveis quase em tempo real. Essas estatísticas são mantidas por 15 meses, de maneira que você possa acessar informações históricas e ter uma perspectiva melhor de como o aplicativo web ou o serviço está se saindo. Você também pode definir alarmes que observam determinados limites e enviam notificações ou realizam ações quando esses limites são atingidos. Para obter mais informações, consulte o [Guia do usuário do Amazon CloudWatch](#).

Para registrar em log e monitorar seus recursos do AWS IoT Wireless, execute as seguintes etapas:

1. Crie um perfil de registro em log para registrar os recursos do AWS IoT Wireless em log, conforme descrito em [Criar um perfil e uma política de log para o AWS IoT Wireless](#).
2. As mensagens de log no console do CloudWatch Logs têm um nível de log padrão de ERROR, que é menos detalhado e contém apenas informações de erro. Se quiser ver mais mensagens detalhadas, recomendamos usar a CLI para configurar o registro em log primeiro, conforme descrito em [Configurar o registro em log para recursos do AWS IoT Wireless](#).
3. Depois, monitore seus recursos visualizando as entradas de log no console do CloudWatch Logs. Para ter mais informações, consulte [Visualizar entradas de log do AWS IoT Wireless no CloudWatch](#).
4. É possível criar expressões de filtro usando grupos de logs, mas recomendamos primeiro criar filtros simples e visualize entradas de log nos grupos de logs e, depois, acessar o CloudWatch Insights para criar consultas para filtrar as entradas de log, dependendo do recurso ou evento sendo monitorado. Para ter mais informações, consulte [Use o CloudWatch Insights para filtrar logs do AWS IoT Wireless](#).

# Configurar o registro em log para o AWS IoT Wireless

Antes de monitorar e registrar as atividades do AWS IoT em log, ative o registro em log de recursos do AWS IoT Wireless usando a CLI ou a API.

Ao considerar como configurar o registro em log do AWS IoT Wireless, a configuração padrão determina como a atividade do AWS IoT será registrada, a menos que você especifique de outra forma. No começo, você talvez queira obter logs detalhados com um nível de log padrão de INFO.

Após analisar os logs iniciais, você pode alterar o nível de log padrão para ERROR, que é um nível menos detalhado, e definir um nível de log mais detalhado específico do recurso em recursos que precisem de maior atenção. É possível alterar os níveis de log sempre que quiser.

Os seguintes tópicos demonstram como configurar o log para recursos do AWS IoT Wireless.

## Tópicos

- [Criar um perfil e uma política de log para o AWS IoT Wireless](#)
- [Configurar o registro em log para recursos do AWS IoT Wireless](#)

## Criar um perfil e uma política de log para o AWS IoT Wireless

Veja a seguir como criar um perfil de registro em log apenas para recursos do AWS IoT Wireless. Se também quiser criar um perfil de registro em log para o AWS IoT Core, consulte <https://docs.aws.amazon.com/iot/latest/developerguide/create-logging-role.html>.

### Criar um perfil de registro em log para o AWS IoT Wireless

Antes que possa habilitar o registro em log, é preciso criar um perfil do IAM e uma política que forneça à permissão AWS para monitorar a atividade do AWS IoT Wireless em seu nome.

Crie um perfil do IAM para registro em log

Para criar um perfil de registro em log para o AWS IoT Wireless, abra o [hub Perfis do console do IAM](#) e selecione Criar perfil.

1. Em Selecionar tipo de entidade confiável, selecione Outra conta da AWS.
2. Em ID da conta, informe seu ID da conta da AWS e selecione Próximo: permissões.
3. Na caixa de pesquisa, insira **AWSIoTWirelessLogging**.

4. Marque a caixa ao lado da política chamada `AWSIoTWirelessLogging` e selecione `Próximo: tags`.
5. Escolha `Próximo: revisar`.
6. Em `Nome do perfil`, insira `IoTWirelessLogsRole` e selecione `Criar perfil`.

### Edite a relação de confiança do perfil do IAM

Na mensagem de confirmação que é exibida após a execução da etapa anterior, selecione o nome do perfil criado, `IoTWirelessLogsRole`. Depois, você editará o perfil para adicionar a relação de confiança a seguir.

1. Na seção `Resumo` do perfil `IoTWirelessLogsRole`, selecione a guia `Relações de confiança` e, em seguida, selecione `Editar relação de confiança`.
2. Em `Documento de política`, altere a propriedade `Principal` para ficar parecida com o exemplo a seguir.

```
"Principal": {  
  "Service": "iotwireless.amazonaws.com"  
},
```

Depois de alterar a propriedade `Principal`, o documento de política completo deve ser semelhante a este exemplo.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "Service": "iotwireless.amazonaws.com"  
      },  
      "Action": "sts:AssumeRole",  
      "Condition": {}  
    }  
  ]  
}
```

3. Para salvar as alterações e sair, selecione `Atualizar política de confiança`.

## Política de registro em log do AWS IoT Wireless

O documento de política a seguir fornece as políticas de perfil e de confiança que permitem que o AWS IoT Wireless envie entradas de log ao CloudWatch em seu nome.

### Note

Esse documento de política gerenciada pela AWS foi criado automaticamente para você quando você criou o perfil de registro em log IoTWirelessLogsRole.

### Política de perfil

Veja a seguir o documento de política de perfil.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/iotwireless*"
    }
  ]
}
```

### Política de confiança para registrar em log somente atividades do AWS IoT Wireless

Veja a seguir a política de confiança para registrar em log apenas atividades do AWS IoT Wireless.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
```

```
    "Effect": "Allow",
    "Principal": {
      "Service": [
        "iotwireless.amazonaws.com"
      ]
    },
    "Action": "sts:AssumeRole"
  }
]
```

Caso tenha criado o perfil do IAM para também registrar em log atividades do AWS IoT Core, então os documentos de política permitem que você registre em log ambas as atividades. Para acessar mais informações sobre a criação de um perfil de registro em log para o AWS IoT Core, consulte <https://docs.aws.amazon.com/iot/latest/developerguide/create-logging-role.html>.

## Próximas etapas

Você aprendeu como criar um perfil de registro em log para registrar seus recursos do AWS IoT Wireless. Por padrão, os logs têm um nível de log de ERROR, portanto, se você quiser visualizar apenas as informações de erro, acesse [Visualizar entradas de log do AWS IoT Wireless no CloudWatch](#) para monitorar seus recursos sem fio visualizando as entradas de log.

Se desejar mais informações nas entradas de log, é possível configurar o nível de log padrão para seus recursos ou para tipos diferentes de eventos, como definir o nível de log como INFO. Para obter informações sobre como configurar o registro em log para seus recursos, consulte [Configurar o registro em log para recursos do AWS IoT Wireless](#).

## Configurar o registro em log para recursos do AWS IoT Wireless

Para configurar o registro em log de recursos do AWS IoT Wireless, use a API ou a CLI. Quando você começar a monitorar recursos do AWS IoT Wireless, é possível usar a configuração padrão. Para fazer isso, pule este tópico e avance para [Monitorar o AWS IoT Wireless com o CloudWatch Logs](#) para monitorar seus logs.

Depois de começar a monitorar os logs, é possível usar a CLI para alterar os níveis de log para uma opção mais detalhada, como fornecer informações de INFO e ERROR e ativar o registro em log para obter mais recursos.

## Recursos e níveis de log do AWS IoT Wireless

Antes de usar a API ou a CLI, use a tabela a seguir para saber mais sobre os diferentes níveis de log e os recursos para os quais você pode configurar o registro em log. A tabela exibe parâmetros que você vê nos logs do CloudWatch ao monitorar recursos. A forma como você configura o registro em log para seus recursos determinará os logs que presentes no console.

Para obter informações sobre a aparência de uma amostra de logs do CloudWatch e como você pode usar esses parâmetros para registrar em log informações úteis sobre os recursos do AWS IoT Wireless, consulte [Visualizar entradas de log do AWS IoT Wireless no CloudWatch](#).

### Recursos e níveis de log

| Nome                | Possíveis valores                 | Descrição                                                                                                                                                                                                                                                                                                                                     |
|---------------------|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| logLevel            | INFO, ERROR ou DISABLED           | <ul style="list-style-type: none"> <li>ERROR: exibe qualquer erro que cause a falha de uma operação. Os logs incluem somente informações de ERROR.</li> <li>INFO: oferece informações de alto nível sobre o fluxo das objetos. Os logs incluem informações de INFO e ERROR.</li> <li>DISABLED: desativa todos os registros em log.</li> </ul> |
| resource            | WirelessGateway ou WirelessDevice | O tipo do recurso, que pode ser WirelessGateway , ou WirelessDevice .                                                                                                                                                                                                                                                                         |
| wirelessGatewayType | LoRaWAN                           | O tipo de gateway sem fio, quando resource é WirelessGateway , que é sempre LoRaWAN.                                                                                                                                                                                                                                                          |
| wirelessDeviceType  | LoRaWAN ou Sidewalk               | O tipo do dispositivo sem fio, quando resource é WirelessDevice , que pode ser LoRaWAN ou Sidewalk.                                                                                                                                                                                                                                           |
| wirelessGatewayId   | -                                 | O identificador do gateway sem fio, quando resource é WirelessGateway .                                                                                                                                                                                                                                                                       |

| Nome             | Possíveis valores                                                                       | Descrição                                                                                                                                                                                                                                                                       |
|------------------|-----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wirelessDeviceId | -                                                                                       | O identificador do dispositivo sem fio, quando resource é WirelessDevice .                                                                                                                                                                                                      |
| event            | Join, Rejoin, Registration , Uplink_data , Downlink_data , CUPS_Request , e Certificate | O tipo de evento que está sendo registrado em log, que depende se o recurso que você está registrando em log é um dispositivo sem fio ou um gateway sem fio. Para ter mais informações, consulte <a href="#">Visualizar entradas de log do AWS IoT Wireless no CloudWatch</a> . |

## API de registro em log do AWS IoT Wireless


É possível usar as seguintes ações de API para configurar o registro em log de recursos. A tabela também exibe um exemplo de política do IAM que você precisa criar para usar as ações de API. A seção a seguir descreve como usar as APIs para configurar níveis de log de recursos.

### Ações de API de registro em log

| Nome da API                                 | Descrição                                                                                                                                                      | Exemplo de política do IAM                                                                                                                                                                                |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">GetLogLevelsByResourceTypes</a> | Retorna os níveis de log padrão atuais ou os níveis de log por tipo de recurso, que podem incluir opções de log para dispositivos sem fio ou gateways sem fio. | <pre> {   "Version":   "2012-10-17",   "Statement": [     {       "Effect":       "Allow",       "Action": [          "iotwireless:GetLogLevelsByResourceTypes"       ],       "Resource":       [ </pre> |

| Nome da API                         | Descrição                                                                                                                                                         | Exemplo de política do IAM                                                                                                                                                                                                                                                                                                         |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                     |                                                                                                                                                                   | <pre> "*" ] } ] } </pre>                                                                                                                                                                                                                                                                                                           |
| <a href="#">GetResourceLogLevel</a> | <p>Retorna a substituição em nível de log de um determinado identificador e tipo de recurso. O recurso pode ser um gateway sem fio ou um dispositivo sem fio.</p> | <pre> {   "Version":   "2012-10-17",   "Statement": [     {       "Effect":       "Allow",       "Action": [          "iotwireless:GetResourceLogLevel"        ],       "Resource":       [          "arn:aws:iotwireless:us-east-1:123456789012:WirelessDevice/012bc537-ab12-cd3a-d00e-1f0e20c1204a",        ]     }   ] } </pre> |

| Nome da API                         | Descrição                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Exemplo de política do IAM                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">PutResourceLogLevel</a> | <p>Define a substituição em nível de log de um determinado identificador e tipo de recurso. O recurso pode ser um gateway sem fio ou um dispositivo sem fio.</p> <div data-bbox="529 493 1029 760" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> <b>Note</b></p><p>Essa API tem um limite de 200 substituições em nível de log por conta.</p></div> | <pre data-bbox="1073 226 1507 1409">{   "Version":     "2012-10-17",   "Statement": [     {       "Effect":         "Allow",       "Action": [          "iotwireless:PutResourceLogLevel"        ],       "Resource":         [            "arn:aws:iotwireless:us-east-1:123456789012:WirelessDevice/012bc537-ab12-cd3a-d00e-1f0e20c1204a",          ]       }     ]   } }</pre> |

| Nome da API                               | Descrição                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Exemplo de política do IAM                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">ResetAllResourceLogLevels</a> | <p>Remove as substituições em nível de log de todos os recursos, o que inclui gateways sem fio e dispositivos sem fio.</p> <div data-bbox="529 445 1029 810" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>Essa API não afeta os níveis de log definidos através da API <code>UpdateLogLevelsByResourceTypes</code>.</p> </div> | <pre data-bbox="1071 226 1507 1528"> {   "Version":     "2012-10-17",   "Statement": [     {       "Effect":         "Allow",       "Action": [         "iotwireless:Reset         AllResourceLogLevels"       ],       "Resource":         [           "arn:aws:iotwireless:us-east-1:123456789012:WirelessDevice/*",           "arn:aws:iotwireless:us-east-1:123456789012:WirelessGateway/*"         ]     }   ] }</pre> |

| Nome da API                           | Descrição                                                                                                                                                 | Exemplo de política do IAM                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">ResetResourceLogLevel</a> | Remove a substituição em nível de log de um determinado identificador e tipo de recurso. O recurso pode ser um gateway sem fio ou um dispositivo sem fio. | <pre>{   "Version":     "2012-10-17",   "Statement": [     {       "Effect":         "Allow",       "Action": [          "iotwireless:Reset         ResourceLogLevel"        ],       "Resource":         [          "arn:aws:iotwirele         ss:us-east-1:12345         6789012:WirelessDe         vice/012bc537-ab12         -cd3a-d00e-1f0e20c         1204a",          ]       }     ]   } }</pre> |

| Nome da API                                    | Descrição                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Exemplo de política do IAM                                                                                                                                                                                                                                                 |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">UpdateLogLevelsByResourceTypes</a> | <p>Define o nível de log padrão ou níveis de log por tipo de recurso. É possível usar essa API para opções de log para dispositivos sem fio ou gateways sem fio e controlar as mensagens de log que serão exibidas no CloudWatch.</p> <div data-bbox="529 590 1029 1045" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p><b>Note</b></p> <p>Os eventos são opcionais e o tipo de evento está atrelado ao tipo de recurso. Para ter mais informações, consulte <a href="#">Tipos de eventos e recursos</a>.</p> </div> | <pre data-bbox="1068 226 1505 1213"> {   "Version":   "2012-10-17",   "Statement": [     {       "Effect":       "Allow",       "Action": [          "iotwireless:UpdateLogLevelsByResourceTypes"       ],       "Resource":       [         "*"       ]     }   ] }</pre> |

## Configurar níveis de log de recursos usando a CLI

Esta seção descreve como configurar níveis de log para recursos do AWS IoT Wireless usando a API ou a AWS CLI.

Antes de usar a CLI:

- Verifique se você criou a política do IAM para a API para a qual deseja executar o comando da CLI, conforme descrito anteriormente.
- É necessário o nome do recurso da Amazon (ARN) do perfil que você deseja usar. Se precisar criar um perfil a ser usado para o registro em log, consulte [Criar um perfil e uma política de log para o AWS IoT Wireless](#).

## Por que usar o AWS CLI

Por padrão, se criar um perfil do IAM, `IoTWirelessLogsRole`, como descrito em [Criar um perfil e uma política de log para o AWS IoT Wireless](#), você verá os logs do CloudWatch no Console de gerenciamento da AWS com nível de log padrão de `ERROR`. Para alterar o nível de log padrão para todos os recursos, ou para recursos específicos, use a API de registro em log AWS IoT Wireless ou a CLI.

## Como usar a AWS CLI

As ações de API podem ser categorizadas nos tipos a seguir, dependendo se você deseja configurar os níveis de log para todos os recursos ou para recursos específicos:

- As ações de API `GetLogLevelsByResourceTypes` e `UpdateLogLevelsByResourceTypes` podem recuperar e atualizar os níveis de log de todos os recursos da sua conta que sejam de um tipo específico, como um gateway sem fio ou um dispositivo LoRaWAN ou Sidewalk.
- As ações de API `GetResourceLogLevel`, `PutResourceLogLevel` e `ResetResourceLogLevel` podem recuperar, atualizar e redefinir os níveis de log de recursos individuais a serem especificados usando um identificador de recurso.
- A ação de API `ResetAllResourceLogLevels` redefine a substituição em nível de log para `null` para todos os recursos para os quais você especificou uma substituição em nível de log usando a API `PutResourceLogLevel`.

## Como usar a CLI para configurar o registro em log de recursos específicos para o AWS IoT

### Note

Também é possível executar esse procedimento com a API usando os métodos na API da AWS que correspondam aos comandos da CLI mostrados aqui.

1. Por padrão, todos os recursos têm o nível de log definido como `ERROR`. Para definir os níveis de log padrão ou os níveis de log por tipos de recursos para todos os recursos da sua conta, use o comando [update-log-levels-by-resource-types](#). O seguinte exemplo demonstra como você pode criar um arquivo JSON, `Input.json`, e usá-lo como uma entrada para o comando CLI. É possível usar esse comando para desativar seletivamente o registro em log ou substituir o nível de log padrão para tipos específicos de recursos e eventos.

```
{
  "DefaultLogLevel": "INFO",
  "WirelessDeviceLogOptions":
  [
    {
      "Type": "Sidewalk",
      "LogLevel": "INFO",
      "Events":
      [
        {
          "Event": "Registration",
          "LogLevel": "DISABLED"
        }
      ]
    },
    {
      "Type": "LoRaWAN",
      "LogLevel": "INFO",
      "Events":
      [
        {
          "Event": "Join",
          "LogLevel": "DISABLED"
        },
        {
          "Event": "Rejoin",
          "LogLevel": "ERROR"
        }
      ]
    }
  ]
  "WirelessGatewayLogOptions":
  [
    {
      "Type": "LoRaWAN",
      "LogLevel": "INFO",
      "Events":
      [
        {
          "Event": "CUPS_Request",
          "LogLevel": "DISABLED"
        },
        {
```

```
        "Event": "Certificate",
        "LogLevel": "ERROR"
    }
  ]
}
}
```

onde:

### WirelessDeviceLogOptions

A lista de opções de log de um dispositivo sem fio. Cada opção de log inclui o tipo de dispositivo sem fio (Sidewalk ou LoRaWAN) e uma lista de opções de log de eventos do dispositivo sem fio. Cada opção de log de eventos do dispositivo sem fio pode, opcionalmente, incluir o tipo de evento e seu nível de log.

### WirelessGatewayLogOptions

A lista de opções de log de um gateway sem fio. Cada opção de log inclui o tipo de gateway sem fio (LoRaWAN) e uma lista de opções de log de eventos do gateway sem fio. Cada opção de log de eventos do gateway sem fio pode, opcionalmente, incluir o tipo de evento e seu nível de log.

### DefaultLogLevel

O nível de log a ser usado para todos os seus recursos. Os valores válidos são: ERROR, INFO e DISABLED. O valor padrão é INFO.

### LogLevel

O nível de log que você deseja usar para tipos de recursos e eventos individuais. Esses níveis de log substituem o nível de log padrão, como o nível de log INFO para o gateway LoRaWAN, e os níveis de log DISABLED e ERROR para os dois tipos de eventos.

Execute o seguinte comando para fornecer o arquivo `Input.json` como entrada para o comando. Esse comando não retorna nenhuma saída.

```
aws iotwireless update-log-levels-by-resource-types \
  --cli-input-json Input.json
```

Se quiser remover as opções de log para dispositivos sem fio e gateways sem fio, execute o seguinte comando.

```
{
  "DefaultLogLevel": "DISABLED",
  "WirelessDeviceLogOptions": [],
  "WirelessGatewayLogOptions": []
}
```

2. O comando `update-log-levels-by-resource-types` não retorna nenhuma saída. Use o comando [get-log-levels-by-resource-types](#) para recuperar informações de registro em log específicas do recurso. O comando retorna o nível de log padrão e as opções de log do dispositivo sem fio e do gateway sem fio.

#### Note

O comando `get-log-levels-by-resource-types` não pode recuperar diretamente os níveis de log no console do CloudWatch. Você pode usar o comando `get-log-levels-by-resource-types` para obter as informações mais recentes de nível de log especificadas para seus recursos usando o comando `update-log-levels-by-resource-types`.

```
aws iotwireless get-log-levels-by-resource-types
```

Ao executar o comando a seguir, ele retorna as informações de registro em log mais recentes especificadas com `update-log-levels-by-resource-types`. Por exemplo, se você remover as opções de log do dispositivo sem fio, a execução de `get-log-levels-by-resource-types` retornará esse valor como `null`.

```
{
  "DefaultLogLevel": "INFO",
  "WirelessDeviceLogOptions": null,
  "WirelessGatewayLogOptions":
  [
    {
      "Type": "LoRaWAN",
      "LogLevel": "INFO",
      "Events":
      [
```

```
{
  "Event": "CUPS_Request",
  "LogLevel": "DISABLED"
},
{
  "Event": "Certificate",
  "LogLevel": "ERROR"
}
]
}
]
```

3. Para controlar níveis de log de gateways sem fio individuais ou recursos de dispositivos sem fio, utilize os seguintes comandos da CLI:

- [put-resource-log-level](#)
- [get-resource-log-level](#)
- [reset-resource-log-level](#)

Por exemplo, ao usar essas CLIs, digamos que você tenha um grande número de dispositivos ou gateways sem fio em sua conta que estão sendo registrados. Se quiser solucionar erros em apenas alguns dos dispositivos sem fio, você pode desativar o registro em log de todos os dispositivos sem fio definindo o `DefaultLogLevel` como `DISABLED` e usar o `put-resource-log-level` para definir `LogLevel` como `ERROR` somente nesses dispositivos da sua conta.

```
aws iotwireless put-resource-log-level \
  --resource-identifier
  --resource-type WirelessDevice
  --log-level ERROR
```

Neste exemplo, o comando define o nível de log como `ERROR` apenas para o recurso de dispositivo sem fio especificado e os logs de todos os outros recursos são desativados. Esse comando não retorna nenhuma saída. Para recuperar essas informações e verificar se os níveis de log foram definidos, use o comando `get-resource-log-level`.

4. Na etapa anterior, depois de depurar o problema e solucionar o erro, você pode executar o comando `reset-resource-log-level` para redefinir o nível de log desse recurso como `null`. Caso tenha usado o comando `put-resource-log-level` para definir a substituição de nível de log para mais de um recurso de gateway ou dispositivo sem fio, como para solucionar erros em

vários dispositivos, você poderá redefinir as substituições em nível de log como `null` para todos esses recursos usando o comando [reset-all-resource-log-levels](#).

```
aws iotwireless reset-all-resource-log-levels
```

Esse comando não retorna nenhuma saída. Para recuperar as informações de registro em log dos recursos, execute o comando `get-resource-log-level`.

## Próximos Passos

Você aprendeu a criar o perfil de registro em log e usar a API do AWS IoT Wireless para configurar o registro em log para seus recursos do AWS IoT Core for LoRaWAN. Em seguida, para aprender mais sobre como monitorar suas entradas de log, acesse [Monitorar o AWS IoT Wireless com o CloudWatch Logs](#).

## Monitorar o AWS IoT Wireless com o CloudWatch Logs

O AWS IoT Core for LoRaWAN tem mais de cinquenta entradas de log do CloudWatch que, por padrão, estão habilitadas. Cada entrada de log descreve o tipo de evento, o nível de log e o tipo de recurso. Para ter mais informações, consulte [Recursos e níveis de log do AWS IoT Wireless](#).

### Como monitorar seus recursos do AWS IoT Wireless

Quando o registro em log está habilitado para o AWS IoT Wireless, o AWS IoT Wireless envia eventos de progresso sobre cada mensagem conforme ela passa dos dispositivos pelo AWS IoT e volta. Por padrão, as entradas de log do AWS IoT Wireless têm um nível de erro de log padrão. Quando você habilita o registro em log conforme descrito em [Criar um perfil e uma política de log para o AWS IoT Wireless](#), você verá mensagens no console do CloudWatch com um nível de log padrão de ERROR. Ao usar esse nível de log, as mensagens mostrarão somente as informações de erro de todos os recursos de gateway ou dispositivos sem fio sendo usados.

Se quiser que os logs exibam informações adicionais, como sobre aqueles que têm um nível de log de INFO, ou desabilitar log para alguns de seus dispositivos e mostrem mensagens de log sobre apenas alguns de seus dispositivos, você pode usar a API de registro em log AWS IoT Wireless. Para ter mais informações, consulte [Configurar níveis de log de recursos usando a CLI](#).

Também é possível criar expressões de filtro para exibir somente as mensagens necessárias.

Antes que você possa visualizar logs do AWS IoT Wireless no console

Para que o grupo de logs `/aws/iotwireless` apareça no console do CloudWatch, é preciso realizar o seguinte.

- Habilitar o registro em log no AWS IoT Wireless. Para acessar mais informações sobre como habilitar o registro em log no AWS IoT Wireless, consulte [Configurar o registro em log para o AWS IoT Wireless](#).
- Escrever algumas entradas de log executando operações do AWS IoT Wireless.

Para criar e usar expressões de filtro com mais eficiência, recomendamos tentar usar o CloudWatch Insights conforme descrito nos tópicos a seguir. Também recomendamos seguir os tópicos na ordem em que estão apresentados aqui. Isso ajudará você a usar os grupos de logs do CloudWatch primeiro para aprender sobre os diferentes tipos de recursos, seus tipos de eventos e níveis de log que podem ser usados para visualizar entradas de log no console. Depois, você pode aprender a criar expressões de filtro usando o CloudWatch Insights para obter mais informações úteis sobre seus recursos.

## Tópicos

- [Visualizar entradas de log do AWS IoT Wireless no CloudWatch](#)
- [Use o CloudWatch Insights para filtrar logs do AWS IoT Wireless](#)

## Visualizar entradas de log do AWS IoT Wireless no CloudWatch

Após configurar o registro em log do AWS IoT Wireless conforme descrito em [Criar um perfil e uma política de log para o AWS IoT Wireless](#) e escrever algumas entradas de log, você pode visualizar as entradas de log no console do CloudWatch executando as etapas a seguir.

### Visualização de logs do AWS IoT no console de grupos de logs do CloudWatch

No [console do CloudWatch](#), os logs do CloudWatch aparecem em um grupo de logs chamado `/aws/iotwireless`. Para obter mais informações sobre o CloudWatch Logs, consulte [CloudWatch Logs](#).

Visualize os logs AWS IoT no console do CloudWatch

Navegue até o [console do CloudWatch](#) e selecione Grupos de logs no painel de navegação.

1. Na caixa de texto Filtro, insira `/aws/iotwireless` e selecione o grupo de logs `/aws/iotwireless`.

2. Para ver uma lista completa dos logs do AWS IoT Core for LoRaWAN gerados para sua conta, selecione Pesquisar tudo. Para visualizar um fluxo de logs individual, selecione o ícone de expansão.
3. Para filtrar os fluxos de logs, também é possível inserir uma consulta na caixa de texto Filtrar eventos. Estas são algumas consultas para experimentar:

- `{ $.logLevel = "ERROR" }`

Use esse filtro para encontrar todos os logs que têm um nível de log de ERROR. É possível expandir os fluxos de erros individuais para ler as mensagens de erro, o que ajudará você a resolvê-las.

- `{ $.resource = "WirelessGateway" }`

Encontre todos os logs do recurso `WirelessGateway`, independentemente do nível de log.

- `{ $.event = "CUPS_Request" && $.logLevel = "ERROR" }`

Encontre todos os logs que têm um tipo de evento `CUPS_Request` e um nível de log de ERROR.

## Tipos de eventos e recursos

A tabela a seguir exibe os diferentes tipos de eventos para os quais você verá entradas de log. Os tipos de eventos também dependem do tipo de recurso ser um dispositivo sem fio ou um gateway sem fio. É possível usar o nível de log padrão para os tipos de recursos e eventos ou substituir o nível de log padrão especificando um nível de log para cada um deles.

Tipos de eventos com base nos recursos utilizados

| Recurso             | Tipo de recurso | Tipo de evento                                                                                                                      |
|---------------------|-----------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Gateway sem fio     | LoRaWAN         | <ul style="list-style-type: none"> <li>• CUPS_Request</li> <li>• Certificado</li> </ul>                                             |
| Dispositivo sem fio | LoRaWAN         | <ul style="list-style-type: none"> <li>• Ingressar</li> <li>• Reingresso</li> <li>• Uplink_Data</li> <li>• Downlink_Data</li> </ul> |

| Recurso             | Tipo de recurso | Tipo de evento                                                                                         |  |
|---------------------|-----------------|--------------------------------------------------------------------------------------------------------|--|
| Dispositivo sem fio | Sidewalk        | <ul style="list-style-type: none"> <li>Registro</li> <li>Uplink_Data</li> <li>Downlink_Data</li> </ul> |  |

O tópico a seguir contém mais informações sobre esses tipos de eventos e as entradas de log para gateways sem fio e dispositivos sem fio.

### Tópicos

- [Entradas de log para recursos de gateways sem fio e dispositivos sem fio](#)

## Entradas de log para recursos de gateways sem fio e dispositivos sem fio

Após habilitar o registro em log, é possível visualizar as entradas de log de gateways sem fio e dispositivos sem fio. A seção a seguir descreve os vários tipos de entradas de log com base em seus tipos de recursos e eventos.

### Entradas de log de gateway sem fio

Esta seção mostra alguns exemplos de entradas de log para recursos de gateway sem fio que você encontrará no [console do CloudWatch](#). Essas mensagens de log podem ter o tipo de evento CUPS\_Request ou Certificate e podem ser configuradas para exibir um nível de log de INFO, ERROR ou DISABLED no nível do recurso ou no nível do evento. Se quiser ver somente as informações de erro, defina o nível do log como ERROR. A mensagem na entrada de log ERROR conterá informações sobre o motivo da falha.

As entradas de log de um recurso de gateway sem fio podem ser classificadas com base nos seguintes tipos de eventos:

- CUPS\_Request

A LoRa Basics Station em execução no seu gateway envia uma solicitação periódica ao Servidor de Configuração e Atualização (CUPS) para obter atualizações. Para esse tipo de evento, se você definir o nível de log como INFO quando configurar a CLI para seu recurso de gateway sem fio, então, nos logs:

- Se o evento obtiver êxito, você verá mensagens de log com um `LogLevel` de `INFO`. As mensagens incluirão detalhes da resposta do CUPS enviada ao seu gateway e os detalhes do gateway. O seguinte mostra um exemplo dessa entrada de log. Para acessar mais informações sobre o `LogLevel` e outros campos da entrada de log, consulte [Recursos e níveis de log do AWS IoT Wireless](#).

```
{
  "timestamp": "2021-05-13T16:56:08.853Z",
  "resource": "WirelessGateway",
  "wirelessGatewayId": "5da85cc8-3361-4c79-8be3-3360fb87abda",
  "wirelessGatewayType": "LoRaWAN",
  "gatewayEui": "feffff00000000e2",
  "event": "CUPS_Request",
  "logLevel": "INFO",
  "message": "Sending CUPS response of total length 3213 to GatewayEui:
feffff00000000e2 with TC Credentials,"
}
```

- Caso haja um erro, você verá entradas de log com um `LogLevel` de `ERROR` e as mensagens incluirão detalhes sobre o erro. Exemplos de quando um erro pode ocorrer no evento `CUPS_Request` incluem: falta de CRC do CUPS, incompatibilidade no Uri do TC do gateway com AWS IoT Core for LoRaWAN, ausência de `IoTWirelessGatewayCertManagerRole` ou impossibilidade de obter o registro do gateway sem fio. O exemplo a seguir mostra uma entrada de log CRC. Para solucionar o erro, cheque a configuração do gateway para verificar se você inseriu o CRC do CUPS correto.

```
{
  "timestamp": "2021-05-13T16:56:08.853Z",
  "resource": "WirelessGateway",
  "wirelessGatewayId": "5da85cc8-3361-4c79-8be3-3360fb87abda",
  "wirelessGatewayType": "LoRaWAN",
  "gatewayEui": "feffff00000000e2",
  "event": "CUPS_Request",
  "logLevel": "ERROR",
  "message": "The CUPS CRC is missing from the request. Check your gateway setup
and enter the CUPS CRC,"
}
```

- Certificado

Essas entradas de log ajudarão você a verificar se o gateway sem fio apresentou o certificado correto para autenticar a conexão ao AWS IoT. Para esse tipo de evento, se você definir o nível de log como INFO quando configurar a CLI para seu recurso de gateway sem fio, então, nos logs:

- Se o evento obtiver êxito, você verá mensagens de log com um `LogLevel` de INFO. As mensagens incluirão detalhes do ID do certificado e do identificador do gateway sem fio. O seguinte mostra um exemplo dessa entrada de log. Para acessar mais informações sobre o `LogLevel` e outros campos da entrada de log, consulte [Recursos e níveis de log do AWS IoT Wireless](#).

```
{
  "resource": "WirelessGateway",
  "wirelessGatewayId": "5da85cc8-3361-4c79-8be3-3360fb87abda",
  "wirelessGatewayType": "LoRaWAN",
  "event": "Certificate",
  "logLevel": "INFO",
  "message": "Gateway connection authenticated.
  (CertificateId:
  b5942a7aee973eda24314e416889227a5e0aa5ed87e6eb89239a83f515dea17c,
  WirelessGatewayId: 5da85cc8-3361-4c79-8be3-3360fb87abda)"
}
```

- Caso haja um erro, você verá entradas de log com um `LogLevel` de ERROR e as mensagens incluirão detalhes sobre o erro. Exemplos de quando um erro pode ocorrer no evento `Certificate` incluem um ID de certificado inválido, um identificador de gateway sem fio ou uma incompatibilidade entre o identificador de gateway sem fio e o ID do certificado. O exemplo a seguir exibe um ERROR devido a um identificador de gateway sem fio inválido. Para solucionar o erro, verifique os identificadores do gateway.

```
{
  "resource": "WirelessGateway",
  "wirelessGatewayId": "5da85cc8-3361-4c79-8be3-3360fb87abda",
  "wirelessGatewayType": "LoRaWAN",
  "event": "Certificate",
  "logLevel": "INFO",
  "message": "The gateway connection couldn't be authenticated because a
  provisioned gateway associated with the certificate couldn't be found.
  (CertificateId:
  729828e264810f6fc7134daf68056e8fd848afc32bfe8082beeb44116d709d9e)"
}
```

## Entradas de log de dispositivo sem fio

Esta seção mostra alguns exemplos de entradas de log para recursos de dispositivo sem fio que você encontrará no [console do CloudWatch](#). O tipo de evento dessas mensagens de log depende se você está usando um dispositivo LoRaWAN ou Sidewalk. Cada recurso de dispositivo sem fio ou tipo de evento pode ser configurado para exibir um nível de log de INFO, ERROR ou DISABLED.

### Note

Sua solicitação não pode possuir metadados sem fio de LoRaWAN e Sidewalk ao mesmo tempo. Para evitar uma entrada de log de ERROR para esse cenário, especifique os dados sem fio LoRaWAN ou Sidewalk.

## Entradas de log de dispositivo LoRaWAN

As entradas de log de um dispositivo sem fio LoRaWAN podem ser classificadas com base nos seguintes tipos de eventos:

### • **Join e Rejoin**

Quando você adicionar um dispositivo LoRaWAN e conectá-lo ao AWS IoT Core for LoRaWAN, antes que seu dispositivo possa enviar dados de uplink, você deve concluir um processo chamado *activation* ou *join procedure*. Para ter mais informações, consulte [Adicione o dispositivo sem fio ao AWS IoT Core for LoRaWAN](#).

Para esse tipo de evento, se você definir o nível de log como INFO quando configurar a CLI para seu recurso de gateway sem fio, então, nos logs:

- Se o evento obtiver êxito, você verá mensagens de log com um `logLevel` de INFO. As mensagens incluirão detalhes do status de sua solicitação de adesão ou reingresso. O seguinte mostra um exemplo dessa entrada de log. Para acessar mais informações sobre o `logLevel` e outros campos da entrada de log, consulte [Recursos e níveis de log do AWS IoT Wireless](#).

```
{
  "timestamp": "2021-05-13T16:56:08.853Z",
  "resource": "WirelessDevice",
  "wirelessDeviceType": "LoRaWAN",
  "WirelessDeviceId": "5da85cc8-3361-4c79-8be3-3360fb87abda",
  "devEui": "feffff00000000e2",
  "event": "Rejoin",
```

```
"logLevel": "INFO",
"message": "Rejoin succeeded"
}
```

- Caso haja um erro, você verá entradas de log com um `logLevel` de `ERROR` e as mensagens incluirão detalhes sobre o erro. Exemplos de quando um erro pode ocorrer nos eventos `Join` e `Rejoin` incluem a configuração inválida da região LoRaWAN ou verificação inválida do Código de Integridade da Mensagem (MIC). O exemplo a seguir exibe um erro de adesão devido à verificação do MIC. Para solucionar o erro, verifique se você inseriu as chaves raiz corretas.

```
{
  "timestamp": "2020-11-24T01:46:50.883481989Z",
  "resource": "WirelessDevice",
  "wirelessDeviceType": "LoRaWAN",
  "WirelessDeviceId": "cb4c087c-1be5-4990-8654-ccf543ee9fff",
  "devEui": "58a0cb000020255c",
  "event": "Join",
  "logLevel": "ERROR",
  "message": "invalid MIC. It's most likely caused by wrong root keys."
}
```

- **Uplink\_Data e Downlink\_Data**

O tipo de evento `Uplink_Data` é utilizado para mensagens geradas pelo AWS IoT Wireless quando a carga útil é enviada do dispositivo LoRaWAN ou Sidewalk ao AWS IoT. O tipo de evento `Downlink_Data` é usado para mensagens relacionadas a mensagens de downlink enviadas do AWS IoT para um dispositivo sem fio.

Para esse tipo de evento, se você definir o nível de log como `INFO` quando configurar a CLI para seus dispositivos sem fio, então, nos logs, você verá:

- Se o evento obtiver êxito, você verá mensagens de log com um `logLevel` de `INFO`. As mensagens incluirão detalhes do status da mensagem de uplink ou downlink enviada e do identificador do dispositivo sem fio. O seguinte mostra um exemplo dessa entrada de log para um dispositivo Sidewalk. Para acessar mais informações sobre o `logLevel` e outros campos da entrada de log, consulte [Recursos e níveis de log do AWS IoT Wireless](#).

```
{
  "resource": "WirelessDevice",
  "wirelessDeviceId": "5371db88-d63d-481a-868a-e54b6431845d",
  "wirelessDeviceType": "Sidewalk",
  "event": "Downlink_Data",
}
```

```

    "logLevel": "INFO",
    "messageId": "8da04fa8-037d-4ae9-bf67-35c4bb33da71",
    "message": "Message delivery succeeded. MessageId: 8da04fa8-037d-4ae9-
bf67-35c4bb33da71. AWS IoT Core: {\"message\": \"OK\", \"traceId\": \"038b5b05-a340-
d18a-150d-d5a578233b09\"}"
  }

```

- Caso haja um erro, você verá entradas de log com um `logLevel` de `ERROR` e as mensagens incluirão detalhes sobre o erro, o que ajudará você a resolvê-lo. Exemplos de quando um erro pode ocorrer para o evento `Registration` incluem: problemas de autenticação, solicitações inválidas ou em número muito elevado, incapacidade de criptografar ou descriptografar a carga ou incapacidade de encontrar o dispositivo sem fio usando o ID especificado. O exemplo a seguir exibe um erro de permissão encontrado durante o processamento de uma mensagem.

```

{
  "resource": "WirelessDevice",
  "wirelessDeviceId": "cb4c087c-1be5-4990-8654-ccf543ee9fff",
  "wirelessDeviceType": "LoRaWAN",
  "event": "Uplink_Data",
  "logLevel": "ERROR",
  "message": "Cannot assume role MessageId:
ef38877f-3454-4c99-96ed-5088c1cd8dee.
Access denied: User: arn:aws:sts::005196538709:assumed-role/
DataRoutingServiceRole/6368b35fd48c445c9a14781b5d5890ed is not authorized
to perform: sts:AssumeRole on resource: arn:aws:iam::400232685877:role/
ExecuteRules_Role\tstatus code: 403, request id: 471c3e35-f8f3-4e94-b734-
c862f63f4edb"
}

```

## Entradas de log de dispositivo Sidewalk

As entradas de log de um dispositivo Sidewalk podem ser classificadas com base nos seguintes tipos de eventos:

- **Registration**

Essas entradas de log ajudarão você a monitorar o status de qualquer dispositivo Sidewalk que você esteja se registrando no AWS IoT Wireless. Para esse tipo de evento, se você definir o nível de log como `INFO` ao configurar a CLI para seu recurso de dispositivo sem fio, então, nos logs, você verá mensagens de log com um `logLevel` de `INFO` e `ERROR`. As mensagens

incluirão detalhes do progresso de registro, do início até a conclusão. As mensagens de log ERROR conterão informações sobre como solucionar problemas com o registro do dispositivo.

O seguinte mostra um exemplo de uma mensagem de log com nível de log de INFO. Para acessar mais informações sobre o `LogLevel` e outros campos da entrada de log, consulte [Recursos e níveis de log do AWS IoT Wireless](#).

```
{
  "resource": "WirelessDevice",
  "wirelessDeviceId": "8d0b2775-e19b-4b2a-a351-cb8a2734a504",
  "wirelessDeviceType": "Sidewalk",
  "event": "Registration",
  "logLevel": "INFO",
  "message": "Successfully completed device registration. Amazon SidewalkId =
2000000002"
}
```

- Uplink\_Data e Downlink\_Data

Os tipos de eventos `Uplink_Data` e `Downlink_Data` para dispositivos Sidewalk se assemelham aos tipos de eventos correspondentes para dispositivos LoRaWAN. Para obter mais informações, consulte a seção `Uplink_Data` e `Downlink_Data` descrita anteriormente para entradas de log de dispositivos LoRaWAN.

## Próximas etapas

Você aprendeu a visualizar as entradas de log de recursos e as diferentes entradas de log que podem ser visualizadas no console do CloudWatch depois de ativar o registro em log do AWS IoT Wireless. Embora possa criar fluxos de filtros usando grupos de logs, recomendamos que você use o CloudWatch Insights para criar e usar fluxos de filtro. Para ter mais informações, consulte [Use o CloudWatch Insights para filtrar logs do AWS IoT Wireless](#).

## Use o CloudWatch Insights para filtrar logs do AWS IoT Wireless

Embora você possa usar o CloudWatch Logs para criar expressões de filtro, recomendamos usar o CloudWatch Insights para criar e usar expressões de filtro com maior eficiência, conforme a sua aplicação.

Recomendamos você a usar os grupos de logs do CloudWatch primeiro para aprender sobre os diferentes tipos de recursos, seus tipos de eventos e níveis de log que podem ser usados para

visualizar entradas de log no console. Você poderá, então, usar os exemplos de algumas expressões de filtro desta página como referência para criar seus próprios filtros para seus recursos do AWS IoT Wireless.

## Visualização de logs do AWS IoT no console do CloudWatch Logs insights

No [console do CloudWatch](#), os logs do CloudWatch aparecem em um grupo de logs chamado `/aws/iotwireless`. Para obter mais informações sobre o CloudWatch Logs, consulte [CloudWatch Logs](#).

Visualize os logs AWS IoT no console do CloudWatch

Navegue até o [console do CloudWatch](#) e selecione Logs Insights no painel de navegação.

1. Na caixa de texto Filtro, insira `/aws/iotwireless` e selecione o Logs Insights `/aws/iotwireless`.
2. Para visualizar uma lista completa de grupos de logs, selecione Selecionar grupo(s) de logs. Para ver grupos de logs do AWS IoT Wireless, selecione `/aws/iotwireless`.

Você pode agora começar a inserir consultas para filtrar os grupos de logs. As seções a seguir contêm algumas consultas úteis que o ajudarão a obter informações sobre suas métricas de recursos.

## Criar consultas úteis para filtrar e obter informações do AWS IoT Wireless

É possível usar expressões de filtro para exibir informações de log úteis adicionais com o CloudWatch Insights. O seguinte mostra alguns exemplos de consultas:

Mostrar apenas logs de tipos de recursos específicos

É possível criar uma consulta que o ajudará a exibir logs de tipos de recursos específicos apenas, como um gateway LoRaWAN ou um dispositivo Sidewalk. Por exemplo, para filtrar logs para exibir somente mensagens para dispositivos Sidewalk, é possível inserir a consulta a seguir e selecionar Executar consulta. Para salvar essa consulta, escolha Salvar.

```
fields @message
| filter @message like /Sidewalk/
```

Depois que a consulta for executada, você visualizará os resultados na guia Logs, que exibe os registros de data/hora dos logs relacionados aos dispositivos Sidewalk da sua conta. Você também

verá um gráfico de barras mostrando a hora em que os eventos ocorreram, caso esses eventos tenham ocorrido anteriormente em relação ao seu dispositivo Sidewalk. O seguinte exibe um exemplo da expansão de um dos resultados na guia Logs. Como alternativa, se quiser solucionar erros relacionados a dispositivos Sidewalk, é possível adicionar outro filtro que defina o nível de log como ERROR e exiba somente as informações de erro.

| Field              | Value                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| @ingestionTime     | 1623894967640                                                                                                                                                                                                                                                                                                                                                                                    |
| @log               | 954314929104:/aws/iotwireless                                                                                                                                                                                                                                                                                                                                                                    |
| @logStream         | WirelessDevice-Downlink_Data-715adccfb34170214ec2f6667ddfa13cb5af2c3ddfc52fbbee0e554a2e780bed                                                                                                                                                                                                                                                                                                    |
| @message           | {<br>"resource": "WirelessDevice",<br>"wirelessDeviceId": "3b058d05-4e84-4e1a-b026-4932bddf978d",<br>"wirelessDeviceType": "Sidewalk",<br>"devEui": "feffff000000011a",<br>"event": "Downlink_Data",<br>"logLevel": "INFO",<br>"messageId": "7e752a10-28f5-45a5-923f-6fa7133fedda",<br>"message": "Successfully sent downlink message. Amazon SidewalkId = 2000000006, Sequence number = 0"<br>} |
| @timestamp         | 1623894967640                                                                                                                                                                                                                                                                                                                                                                                    |
| devEui             | feffff000000011a                                                                                                                                                                                                                                                                                                                                                                                 |
| event              | Downlink_Data                                                                                                                                                                                                                                                                                                                                                                                    |
| logLevel           | INFO                                                                                                                                                                                                                                                                                                                                                                                             |
| message            | Successfully sent downlink message. Amazon SidewalkId = 2000000006, Sequence number = 0                                                                                                                                                                                                                                                                                                          |
| messageId          | 7e752a10-28f5-45a5-923f-6fa7133fedda                                                                                                                                                                                                                                                                                                                                                             |
| resource           | WirelessDevice                                                                                                                                                                                                                                                                                                                                                                                   |
| wirelessDeviceId   | 3b058d05-4e84-4e1a-b026-4932bddf978d                                                                                                                                                                                                                                                                                                                                                             |
| wirelessDeviceType | Sidewalk                                                                                                                                                                                                                                                                                                                                                                                         |

### Exibir mensagens ou eventos específicos

É possível criar uma consulta que o ajude a mostrar mensagens específicas e observar o momento de ocorrência dos eventos. Por exemplo, se quiser ver quando sua mensagem de downlink foi enviada do seu dispositivo sem fio LoRaWAN, você pode inserir a consulta a seguir e selecionar Executar consulta. Para salvar essa consulta, escolha Salvar.

```
filter @message like /Downlink message sent/
```

Quando a consulta for executada, você verá os resultados na guia Logs, que mostra os registros de data/hora em que a mensagem de downlink foi enviada com êxito para o dispositivo sem fio. Você também verá um gráfico de barras mostrando a hora em que uma mensagem de downlink foi enviada, caso outras mensagens de downlink tenham sido enviadas anteriormente para o dispositivo sem fio. O seguinte exibe um exemplo da expansão de um dos resultados na guia Logs. Alternativamente, se uma mensagem de downlink não tiver sido enviada, você pode modificar a consulta para exibir somente resultados de ocorrências em que a mensagem não foi enviada, para poder depurar o problema.

| Field                                                                        | Value                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| @ingestionTime                                                               | 1623884043676                                                                                                                                                                                                                                                                                                                                                                                                                       |
| @log                                                                         | 954314929104:/aws/iotwireless                                                                                                                                                                                                                                                                                                                                                                                                       |
| @logStream                                                                   | WirelessDevice-                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Downlink_Data-42d0e6d09ba4d7015f4e9756fc616d401cd85fe3ac19854d9fbd866153c872 |                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| @message                                                                     | {<br>"timestamp": "2021-06-16T22:54:00.770493863Z",<br>"resource": "WirelessDevice",<br>"wirelessDeviceId": "3b058d05-4e84-4e1a-b026-4932bddf978d",<br>"wirelessDeviceType": "LoRaWAN",<br>"devEui": "feffff000000011a",<br>"event": "Downlink_Data",<br>"logLevel": "INFO",<br>"messageId": "7e752a10-28f5-45a5-923f-6fa7133fedda",<br>"message": "Downlink message sent. MessageId:<br>7e752a10-28f5-45a5-923f-6fa7133fedda"<br>} |
| @timestamp                                                                   | 1623884040858                                                                                                                                                                                                                                                                                                                                                                                                                       |
| devEui                                                                       | feffff000000011a                                                                                                                                                                                                                                                                                                                                                                                                                    |
| event                                                                        | Downlink_Data                                                                                                                                                                                                                                                                                                                                                                                                                       |
| logLevel                                                                     | INFO                                                                                                                                                                                                                                                                                                                                                                                                                                |
| message                                                                      | Downlink message sent. MessageId:<br>7e752a10-28f5-45a5-923f-6fa7133fedda                                                                                                                                                                                                                                                                                                                                                           |
| messageId                                                                    | 7e752a10-28f5-45a5-923f-6fa7133fedda                                                                                                                                                                                                                                                                                                                                                                                                |
| resource                                                                     | WirelessDevice                                                                                                                                                                                                                                                                                                                                                                                                                      |
| timestamp                                                                    | 2021-06-16T22:54:00.770493863Z                                                                                                                                                                                                                                                                                                                                                                                                      |
| wirelessDeviceId                                                             | 3b058d05-4e84-4e1a-b026-4932bddf978d                                                                                                                                                                                                                                                                                                                                                                                                |
| wirelessDeviceType                                                           | LoRaWAN                                                                                                                                                                                                                                                                                                                                                                                                                             |

## Próximas etapas

Você aprendeu como usar o CloudWatch Insights para obter mais informações úteis com a criação de consultas para filtrar mensagens de log. Você pode combinar alguns dos filtros descritos

anteriormente e desenvolver seus próprios filtros, conforme o recurso que estiver monitorando. Para obter mais informações sobre como usar o CloudWatch Insights, consulte [Analisar dados de log com o CloudWatch Insights](#).

Após criar consultas com o CloudWatch Insights, se você as salvou, é possível carregar e executar as consultas salvas conforme necessário. Como alternativa, se clicar no botão Histórico no console do CloudWatch Logs Insights, você poderá visualizar as consultas executadas anteriormente e executá-las novamente conforme necessário ou modificá-las ainda mais criando consultas adicionais.

# Notificações de eventos para AWS IoT Wireless

AWS IoT Wireless pode publicar mensagens para notificar você sobre eventos nos dispositivos LoRaWAN e Sidewalk que você integra ao AWS IoT Core. Por exemplo, você pode receber notificações de eventos, como quando os dispositivos do Sidewalk em sua conta foram provisionados ou registrados.

## Como seus recursos podem ser notificados sobre eventos

As notificações de eventos são publicadas quando determinados eventos ocorrem. Por exemplo, os eventos são gerados quando seu dispositivo Sidewalk é provisionado. Cada evento faz com que uma única notificação de evento seja enviada. As notificações de eventos são publicadas por meio do MQTT com uma carga JSON. O conteúdo da carga depende do tipo do evento.

### Note

As notificações de eventos são publicadas pelo menos uma vez. É possível que elas sejam publicadas mais de uma vez. A ordenação das mensagens de eventos não é garantida.

## Tipos de eventos e recursos

A tabela a seguir exibe os diferentes tipos de eventos para os quais você receberá notificações. Os tipos de eventos também dependem do tipo de recurso ser um dispositivo sem fio, um gateway sem fio ou uma conta do Sidewalk. Você também pode ativar eventos para seus recursos no nível do recurso, o que se aplica a todos os recursos de um tipo específico, ou para recursos selecionados, conforme descrito na seção a seguir. Para obter mais informações sobre os diferentes tipos de eventos, consulte [Notificações de eventos para recursos LoRaWAN](#) e [Notificações de eventos para recursos do Sidewalk](#).

### Tipos de eventos com base nos recursos

| Recurso             | Tipo de recurso | Tipo de evento                                                                      |
|---------------------|-----------------|-------------------------------------------------------------------------------------|
| Dispositivo sem fio | LoRaWAN         | Ingressar                                                                           |
|                     | Sidewalk        | <ul style="list-style-type: none"> <li>Estado de registro do dispositivo</li> </ul> |

| Recurso         | Tipo de recurso | Tipo de evento                                                                                               |
|-----------------|-----------------|--------------------------------------------------------------------------------------------------------------|
|                 |                 | <ul style="list-style-type: none"> <li>• Proximidade</li> </ul>                                              |
| Gateway sem fio | LoRaWAN         | Status de conexão                                                                                            |
| Conta Sidewalk  | Sidewalk        | <ul style="list-style-type: none"> <li>• Estado de registro do dispositivo</li> <li>• Proximidade</li> </ul> |

## Política para receber notificações de eventos sem fio

Para receber notificações de eventos, o dispositivo deve utilizar uma política adequada que permita que ele se conecte ao gateway de dispositivos do AWS IoT e assine os tópicos de evento do MQTT. Você também deve assinar os filtros apropriados dos tópicos.

Veja a seguir um exemplo da política necessária para receber notificações para os vários eventos sem fio.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Subscribe",
        "iot:Receive"
      ],
      "Resource": [
        "arn:aws:iotwireless:region:account:$aws/iotwireless/events/join/*",
        "arn:aws:iotwireless:region:account:$aws/iotwireless/events/
connection_status/*"
        "arn:aws:iotwireless:region:account:$aws/iotwireless/events/
device_registration_state/*",
        "arn:aws:iotwireless:region:account:$aws/iotwireless/events/proximity/*"
      ]
    }
  ]
}
```

## Formato dos tópicos do MQTT para eventos sem fio

Para enviar notificações de eventos para seus recursos sem fio, o AWS IoT usa tópicos reservados do MQTT que começam com um cifrão (\$). Você pode se inscrever e publicar nesses tópicos reservados. Entretanto, não é possível criar tópicos que comecem com um cifrão.

### Note

Os tópicos do MQTT são específicos para sua Conta da AWS e usam o formato `arn:aws:iotwireless:aws-region:AWS-account-ID:topic/Topic`. Para obter mais informações, consulte [MQTT topics](#) no Guia do desenvolvedor do AWS IoT.

Os tópicos reservados do MQTT para dispositivos sem fio usam o seguinte formato:

- Tópicos em nível de recurso

Esses tópicos se aplicam a todos os recursos de um tipo específico em sua Conta da AWS que você integrou à AWS IoT Wireless.

```
$aws/iotwireless/events/{eventName}/{eventType}/{resourceType}/resources
```

- Tópicos em nível de identificador

Esses tópicos se aplicam a recursos selecionados de um tipo específico em sua Conta da AWS que você integrou à AWS IoT Wireless, especificados pelo identificador de recursos.

```
$aws/iotwireless/events/{eventName}/{eventType}/{resourceType}/
{resourceIdentifierType}/{resourceID}/{id}
```

Para obter mais informações sobre tópicos a nível de recurso e identificador, consulte [Configurações do evento](#).

A tabela a seguir mostra exemplos de tópicos do MQTT para os vários eventos:

### Eventos e tópicos do MQTT

| Evento                | Tópico do MQTT                                                                 | Observações                                                                                                                  |
|-----------------------|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Estado de registro do | <ul style="list-style-type: none"> <li>• Tópico em nível de recurso</li> </ul> | <ul style="list-style-type: none"> <li>• {eventType} pode ser <code>registered</code> ou <code>provisioned</code></li> </ul> |

| Evento               | Tópico do MQTT                                                                                                                                                                                                                                                                                                           | Observações                                                                                                                                                                                                           |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dispositivo Sidewalk | <pre>\$aws/iotwireless/ events/dev ice_regis tration_state/ {eventType}/ sidewalk/w ireless_devices</pre> <ul style="list-style-type: none"> <li>Tópico em nível de identificador</li> </ul> <pre>\$aws/iotwireless/ events/dev ice_regis tration_state/ {eventType}/ sidewalk/{ resourceType}/ {resourceID}/ {id}</pre> | <ul style="list-style-type: none"> <li>{resourceType} pode ser sidewalk_accounts ou wireless_devices</li> <li>{resourceID} é o amazon_id para sidewalk_accounts e wireless_device_id para wireless_devices</li> </ul> |

| Evento                  | Tópico do MQTT                                                                                                                                                                                                                                                                                                                        | Observações                                                                                                                                                                                                                                                                            |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Proximidade do Sidewalk | <ul style="list-style-type: none"><li>• Tópico em nível de recurso<br/><br/><code>\$aws/iotwireless/events/proximity/{eventType}/sidewalk/wireless_devices</code></li><li>• Tópico em nível de identificador<br/><br/><code>\$aws/iotwireless/events/proximity/{eventType}/sidewalk/{resourceType}/{resourceID}/{id}</code></li></ul> | <ul style="list-style-type: none"><li>• {eventType} pode ser beacon_discovered ou beacon_lost</li><li>• {resourceType} pode ser sidewalk_accounts ou wireless_devices</li><li>• {resourceID} é o amazon_id para sidewalk_accounts e wireless_device_id para wireless_devices</li></ul> |

| Evento         | Tópico do MQTT                                                                                                                                                                                                                                                                                                | Observações                                                                                                                                                                                                                                                                             |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Junção LoRaWAN | <ul style="list-style-type: none"><li>Tópico em nível de recurso<br/><code>\$aws/iotwireless/events/join/{eventType}/lorawan/wireless_devices</code></li><li>Tópico em nível de identificador<br/><code>\$aws/iotwireless/events/join/{eventType}/lorawan/wireless_devices/{resourceID}/{id}</code></li></ul> | <ul style="list-style-type: none"><li><code>{eventType}</code> pode ser <code>join_req_0_received</code> ou <code>join_req_2_received</code> ou <code>join_accepted</code></li><li><code>{resourceID}</code> pode ser <code>wireless_device_id</code> ou <code>dev_eui</code></li></ul> |

| Evento                               | Tópico do MQTT                                                                                                                                                                                                                                                                                                     | Observações                                                                                                                                                                                                                                      |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status de conexão do gateway LoRaWAN | <ul style="list-style-type: none"> <li>Tópico em nível de recurso<br/><code>\$aws/iotwireless/events/join/{eventType}/lorawan/wireless_gateways</code></li> <li>Tópico em nível de identificador<br/><code>\$aws/iotwireless/events/join/{eventType}/lorawan/wireless_gateways/{resourceID}/{id}</code></li> </ul> | <ul style="list-style-type: none"> <li><code>{eventType}</code> pode ser <code>connected</code> ou <code>disconnected</code></li> <li><code>{resourceID}</code> pode ser <code>wireless_gateway_id</code> ou <code>gateway_eui</code></li> </ul> |

Para obter mais informações sobre diferentes eventos, consulte [Notificações de eventos para recursos LoRaWAN](#) e [Notificações de eventos para recursos do Sidewalk](#).

Se você se inscreveu nesses tópicos, receberá uma notificação quando uma mensagem for publicada em um dos tópicos de notificação do evento. Para obter mais informações, consulte [MQTT reserved topics](#) no Guia do desenvolvedor do AWS IoT.

## Preços para eventos sem fio

Para obter informações sobre preços para se inscrever em eventos e receber notificações, consulte [preços do AWS IoT Core](#).

# Ativar eventos para recursos sem fio

Antes que os assinantes dos tópicos reservados possam receber mensagens, você deve ativar as notificações de eventos. Para fazer isso, você pode usar o Console de gerenciamento da AWS ou a API do AWS IoT Wireless ou a AWS CLI.

## Configurações do evento

Você pode configurar eventos para enviar notificações para todos os recursos que pertencem a um tipo específico ou para recursos sem fio individuais. O tipo de recurso pode ser um gateway sem fio, uma conta de parceiro do Sidewalk ou um dispositivo sem fio, que pode ser um dispositivo LoRaWAN ou Sidewalk. Para obter informações sobre o tipo de eventos que você pode ativar para seus dispositivos sem fio, consulte [Tipos de eventos para recursos LoRaWAN](#) e [Tipos de eventos para recursos do Sidewalk](#).

### Todos os recursos

Você pode ativar eventos de forma que todos os recursos na sua Conta da AWS pertencentes a um determinado tipo de recurso recebam notificações. Por exemplo, você pode ativar um evento que notifique você sobre alterações no status da conexão de todos os gateways LoRaWAN com os quais você se integrou AWS IoT Core for LoRaWAN. O monitoramento desses eventos ajudará você a receber notificações em casos como quando certos gateways LoRaWAN em sua frota de recursos são desconectados ou se um farol for perdido para vários dispositivos Sidewalk em sua Conta da AWS.

### Recursos individuais

Você também pode adicionar recursos individuais do LoRaWAN e do Sidewalk à configuração do seu evento e ativar as notificações para eles. Isso ajudará você a monitorar recursos individuais de um tipo específico. Por exemplo, você pode adicionar dispositivos LoRaWAN e Sidewalk selecionados à sua configuração e receber notificações de eventos de adesão ou de estado de registro de dispositivos para esses recursos.

## Pré-requisitos

Seu recurso LoRaWAN ou Sidewalk deve ter uma política apropriada que permita receber notificações de eventos. Para ter mais informações, consulte [Política para receber notificações de eventos sem fio](#).

## Habilitar notificações usando o Console de gerenciamento da AWS

Para habilitar mensagens de eventos do console, vá para a guia [Configurações](#) do console de AWS IoT e, em seguida, vá para a seção de notificação de eventos LoRaWAN e Sidewalk.

Você pode ativar notificações para todos os recursos na sua Conta da AWS pertencentes a um determinado tipo de recurso e monitorá-los.

Para ativar as notificações para todos os recursos

1. Na seção de notificação de eventos LoRaWAN e Sidewalk, vá para a guia Todos os recursos, escolha Ação e, em seguida, escolha Gerenciar eventos.
2. Ative os eventos que você deseja monitorar e escolha Atualizar eventos. Se você não quiser mais monitorar determinados eventos, escolha Ação, selecione Gerenciar eventos e, em seguida, desative esses eventos.

Você também pode ativar notificações para recursos individuais na sua Conta da AWS pertencentes a um determinado tipo de recurso e monitorá-los.

Para ativar as notificações para recursos individuais

1. Na seção de notificação de eventos LoRaWAN e Sidewalk, escolha Ação e, em seguida, escolha Adicionar recursos.
2. Selecione o recursos e eventos para os quais quer receber notificações:
  - a. Escolha se você deseja monitorar eventos para seus recursos LoRaWAN ou recursos do Sidewalk.
  - b. Dependendo do tipo de recurso, você pode escolher os eventos que deseja habilitar para os recursos. Você poderá se inscrever nesses eventos e receber notificações. Se você escolher:
    - Recursos LoRaWAN: Você pode habilitar eventos de ingresso para seus dispositivos LoRaWAN ou eventos de status de conexão para seus gateways LoRaWAN.
    - Recursos do Sidewalk: é possível habilitar o Estado do registro do dispositivo ou eventos de proximidade ou ambos para as contas de parceiros do Sidewalk e dispositivos Sidewalk.

3. Dependendo do tipo de recurso e dos eventos escolhidos, selecione os dispositivos sem fio ou gateways que você deseja monitorar. Você pode selecionar até 250 recursos para todos os recursos combinados.
4. Escolha Enviar para adicionar seus recursos.

Os recursos que você adicionar aparecerão com seus tópicos de MQTT na guia do seu tipo de recurso na seção de notificação de eventos LoRaWAN e Sidewalk do console.

- Os eventos de ingresso no LoRaWAN e os eventos para seus dispositivos Sidewalk aparecerão na seção Dispositivos sem fio do console.
- Os eventos de status de conexão para seus gateways LoRaWAN aparecerão na seção Gateways sem fio.
- O estado do registro do dispositivo e os eventos de proximidade de suas contas do Sidewalk aparecerão na guia Contas do Sidewalk.

Inscreva-se em tópicos usando o cliente MQTT

Dependendo se você ativou eventos para todos os recursos ou para tipos de recursos individuais, os eventos que você ativou aparecerão no console com seus tópicos do MQTT na guia Todos os recursos ou na guia do tipo de recurso especificado.

- Se você escolher um dos tópicos do MQTT, poderá acessar o cliente do MQTT para se inscrever nesses tópicos e receber mensagens.
- Se você adicionou vários eventos, pode se inscrever em vários tópicos do evento e receber notificações sobre eles. Para se inscrever em vários tópicos, escolha seus tópicos, selecione Ação e, em seguida, selecione Inscrever-se.

## Habilitar notificações usando a AWS CLI

Você pode configurar eventos e adicionar recursos à sua configuração usando a API AWS IoT Wireless ou o AWS CLI.

Ativar as notificações para todos os recursos

Você pode habilitar notificações para todos os recursos em sua Conta da AWS que pertencem a um determinado tipo de recurso e monitorá-los usando a API

[UpdateEventConfigurationByResourceTypes](#) ou o comando da CLI [update-event-configuration-by-resource-types](#). Por exemplo:

```
aws iotwireless update-event-configuration-by-resource-types \  
  --cli-input-json input.json
```

Conteúdo de input.json

```
{  
  "DeviceRegistrationState": {  
    "Sidewalk": {  
      "AmazonIdEventTopic": "Enabled"  
    }  
  },  
  "ConnectionStatus": {  
    "LoRaWAN": {  
      "WirelessGatewayEventTopic": "Enabled"  
    }  
  }  
}
```

#### Note

Todas as aspas (") são recuadas com uma barra invertida (\).

Você pode obter a configuração atual do evento chamando a API [GetEventConfigurationByResourceTypes](#) ou usando o comando da CLI [get-event-configuration-by-resource-types](#). Por exemplo:

```
aws iotwireless get-event-configuration-by-resource-types
```

### Ativar as notificações para recursos individuais

Para adicionar recursos individuais à sua configuração de eventos e controlar quais eventos são publicados usando a API ou a CLI, chame a API [UpdateResourceEventConfiguration](#) ou use o comando da CLI [update-resource-event-configuration](#). Por exemplo:

```
aws iotwireless update-resource-event-configuration \  
  --identifer 1ffd32c8-8130-4194-96df-622f072a315f \  
  --cli-input-json input.json
```

```
--identifier-type WirelessDeviceId \  
--cli-input-json input.json
```

### Conteúdo de input.json

```
{  
  "Join": {  
    "LoRaWAN": {  
      "DevEuiEventTopic": "Disabled"  
    },  
    "WirelessDeviceIdEventTopic": "Enabled"  
  }  
}
```

#### Note

Todas as aspas (") são recuadas com uma barra invertida (\).

Você pode obter a configuração atual do evento chamando a API [GetResourceEventConfiguration](#) ou usando o comando da CLI [get-resource-event-configuration](#). Por exemplo:

```
aws iotwireless get-resource-event-configuration \  
--identifier-type WirelessDeviceId \  
--identifier 1ffd32c8-8130-4194-96df-622f072a315f
```

### Listar configurações do evento

Você também pode usar a API AWS IoT Wireless ou a AWS CLI para listar as configurações de eventos em que pelo menos um tópico do evento foi ativado. Para listar as configurações, use a operação da API [ListEventConfigurations](#) ou o comando da CLI [list-event-configurations](#). Por exemplo:

```
aws iotwireless list-event-configurations --resource-type WirelessDevice
```

## Notificações de eventos para recursos LoRaWAN

Você pode usar as operações da API Console de gerenciamento da AWS ou AWS IoT Wireless para receber notificações sobre eventos em seus dispositivos e gateways LoRaWAN. Para obter

informações sobre notificações de eventos e como habilitá-las, consulte [Notificações de eventos para AWS IoT Wireless](#) e [Ativar eventos para recursos sem fio](#).

## Tipos de eventos para recursos LoRaWAN

Os eventos que você pode ativar para seus recursos LoRaWAN incluem:

- Ingresse em eventos que notificam você sobre eventos de ingresso em seu dispositivo LoRaWAN. Você receberá notificações quando um dispositivo ingressar com AWS IoT Core for LoRaWAN ou quando uma solicitação de reingresso do tipo 0 ou tipo 2 for recebida.
- Eventos de status de conexão que notificam você quando o status da conexão do seu gateway LoRaWAN muda para conectado ou desconectado.

As seções a seguir contêm mais informações sobre os eventos de seus recursos LoRaWAN:

Tópicos

- [Eventos de ingresso LoRaWAN](#)
- [Eventos de status de conexão](#)

## Eventos de ingresso LoRaWAN

AWS IoT Core for LoRaWAN pode publicar mensagens para notificar você sobre eventos de ingresso nos dispositivos LoRaWAN que você integra ao AWS IoT. Os eventos de ingresso notificam você quando uma solicitação de ingresso ou reingresso do tipo 0 ou tipo 2 é recebida e o dispositivo ingressou com AWS IoT Core for LoRaWAN.

### Como funciona o ingresso em eventos

Quando você integra seus dispositivos LoRaWAN com AWS IoT Core for LoRaWAN, AWS IoT Core for LoRaWAN executa um procedimento de ingresso para seu dispositivo com AWS IoT Core for LoRaWAN. Seu dispositivo então é ativado para uso e pode enviar uma mensagem de uplink para indicar que está disponível. Após o ingresso do dispositivo, as mensagens de uplink e downlink podem ser trocadas entre seu dispositivo e AWS IoT Core for LoRaWAN. Para acessar informações sobre integrar seu dispositivo, consulte [Integrar os dispositivos ao AWS IoT Core for LoRaWAN](#).

Você pode ativar eventos para receber notificações quando seu dispositivo ingressar no AWS IoT Core for LoRaWAN. Você também receberá notificações se o evento de ingresso falhar, quando uma solicitação de reingresso do tipo 0 ou do tipo 2 for recebida e quando for aceita.

## Permita que o LoRaWAN ingresse em eventos

Antes que os assinantes dos tópicos reservados de ingresso do LoRaWAN possam receber mensagens, você deve habilitar as notificações de eventos para eles a partir do Console de gerenciamento da AWS, ou usando a API ou CLI. Você pode habilitar esses eventos para todos os recursos do LoRaWAN em sua Conta da AWS ou para recursos selecionados. Para obter mais informações sobre como configurar esses eventos, consulte [Ativar eventos para recursos sem fio](#).

## Formato dos tópicos do MQTT para eventos LoRaWAN

Os tópicos reservados do MQTT para dispositivos LoRaWAN usam o seguinte formato: Se você se inscreveu nesses tópicos, todos os dispositivos LoRaWAN registrados em sua Conta da AWS podem receber a notificação:

- Tópicos em nível de recurso

```
$aws/iotwireless/events/{eventName}/{eventType}/lorawan/wireless_devices
```

- Tópicos de identificador

```
$aws/iotwireless/events/{eventName}/{eventType}/lorawan/wireless_devices/  
{resourceID}/{id}
```

Em que:

{eventName}

{eventName} deve ser `join`.

{eventType}

{eventType} pode ser:

- `join_req_received`
- `rejoin_req_0_received`
- `rejoin_req_2_received`
- `join_accepted`

{resourceID}

{resourceID} pode ser `dev_eui` ou `wireless_device_id`.

Por exemplo, você pode se inscrever nos tópicos a seguir para receber uma notificação de evento quando AWS IoT Core for LoRaWAN aceitar uma solicitação de ingresso de seus dispositivos.

```
$aws/iotwireless/events/join/join_accepted/lorawan/wireless_devices/  
wireless_device_id/{id}
```

Você também pode usar o caractere curinga + para se inscrever em vários tópicos ao mesmo tempo. O caractere curinga + corresponde a qualquer string no nível que contém o caractere, como no tópico a seguir:

```
$aws/iotwireless/events/join/join_req_received/lorawan/wireless_devices/  
wireless_device_id/+
```

#### Note

Você não pode usar o caractere curinga # para se inscrever nos tópicos reservados.

Para obter mais informações sobre como utilizar o curinga + ao assinar tópicos, consulte [MQTT topic filters](#) no Guia do desenvolvedor do AWS IoT.

## Carga útil da mensagem para o evento de ingresso LoRaWAN

O seguinte mostra a carga útil da mensagem para o evento de ingresso do LoRaWAN.

```
{  
  // General fields  
  "eventId": "string",  
  "eventType": "join_req_received|rejoin_req_0_received|rejoin_req_2_received|  
join_accepted",  
  "WirelessDeviceId": "string",  
  "timestamp": "timestamp",  
  
  // Event-specific fields  
  "LoRaWAN": {  
    "DevEui": "string",  
  
    // The fields below are optional indicating that it can be a null value.  
    "DevAddr": "string",  
    "JoinEui": "string",  
    "AppEui": "string",  
  }  
}
```

```
}
```

As cargas contêm os seguintes atributos:

`eventId`

Um ID de evento exclusivo que é gerado por AWS IoT Core for LoRaWAN (string).

`eventType`

O tipo de evento que ocorreu. Pode ser um dos valores a seguir:

- `join_req_received`: Este campo mostrará os parâmetros `JoinEui` ou `AppEui` do EUI
- `rejoin_req_0_received`
- `rejoin_req_2_received`
- `join_accepted`: Esse campo mostrará a `NetId` e `DevAddr`.

`wirelessDeviceId`

A ID do dispositivo LoRaWAN.

`timestamp`

A data e hora do Unix de quando o evento ocorreu.

`DevEui`

O identificador exclusivo do dispositivo encontrado na etiqueta do dispositivo ou na documentação do dispositivo.

`DevAddr` e EUIs (opcional)

Esses campos são o endereço opcional do dispositivo e os parâmetros EUI `JoinEUI` ou `AppEUI`.

## Eventos de status de conexão

AWS IoT Core for LoRaWAN pode publicar mensagens para notificar você sobre eventos de status de conexão nos gateways LoRaWAN que você integra ao AWS IoT. Eventos de status de conexão notificam você quando o status da conexão de um gateway LoRaWAN muda para conectado ou desconectado.

### Como os eventos de status de conexão funcionam

Depois de integrar seu gateway ao AWS IoT Core for LoRaWAN, você pode conectá-lo ao AWS IoT Core for LoRaWAN e verificar o status da conexão. Este evento notifica você quando o status

da conexão do seu gateway muda para conectado ou desconectado. Para obter mais informações sobre como integrar e conectar seu gateway ao AWS IoT Core for LoRaWAN, consulte [Integre os gateways ao AWS IoT Core for LoRaWAN](#) e [Conecte o gateway LoRaWAN e verifique o status da conexão](#).

## Formato dos tópicos do MQTT para gateways LoRaWAN

Os tópicos reservados do MQTT para gateways LoRaWAN usam o seguinte formato. Se você se inscreveu nesses tópicos, todos os gateways LoRaWAN registrados em sua Conta da AWS podem receber a notificação:

- Para tópicos em nível de recurso:

```
$aws/iotwireless/events/{eventName}/{eventType}/lorawan/wireless_gateways
```

- Para tópicos de identificador:

```
$aws/iotwireless/events/{eventName}/{eventType}/lorawan/  
wireless_gateways/{resourceID}/{id}
```

Em que:

{eventName}

{eventName} deve ser `connection_status`.

{eventType}

{eventType} pode ser `connected` ou `disconnected`.

{resourceID}

{resourceID} pode ser `gateway_eui` ou `wireless_gateway_id`.

Por exemplo, você pode se inscrever nos tópicos a seguir para receber uma notificação de evento quando todos os seus gateways estiverem conectados a AWS IoT Core for LoRaWAN:

```
$aws/iotwireless/events/connection_status/connected/lorawan/  
wireless_gateways/wireless_gateway_id/{id}
```

Você também pode usar o caractere curinga `+` para se inscrever em vários tópicos ao mesmo tempo. O caractere curinga `+` corresponde a qualquer string no nível que contém o caractere, como no tópico a seguir:

```
$aws/iotwireless/events/connection_status/connected/lorawan/  
wireless_gateways/wireless_gateway_id/+
```

### Note

Você não pode usar o caractere curinga # para se inscrever nos tópicos reservados.

Para obter mais informações sobre como utilizar o curinga + ao assinar tópicos, consulte [MQTT topic filters](#) no Guia do desenvolvedor do AWS IoT.

## Carga útil de mensagens para eventos de status de conexão

O seguinte mostra a carga útil da mensagem para o evento de status de conexão.

```
{  
  // General fields  
  "eventId": "string",  
  "eventType": "connected|disconnected",  
  "WirelessGatewayId": "string",  
  "timestamp": "timestamp",  
  
  // Event-specific fields  
  "LoRaWAN": {  
    "GatewayEui": "string"  
  }  
}
```

As cargas contêm os seguintes atributos:

### eventId

Um ID de evento exclusivo que é gerado por AWS IoT Core for LoRaWAN (string).

### eventType

O tipo de evento que ocorreu. Pode ser `connected` ou `disconnected`.

### wirelessGatewayId

O ID do gateway LoRaWAN.

## timestamp

A data e hora do Unix de quando o evento ocorreu.

## GatewayEui

O identificador exclusivo do gateway encontrado na etiqueta do gateway ou na documentação do gateway.

# Notificações de eventos para recursos do Sidewalk

Você pode usar as operações da API Console de gerenciamento da AWS ou AWS IoT Wireless para receber notificações sobre eventos em seus dispositivos do Sidewalk e contas parceiras. Para obter informações sobre notificações de eventos e como ativá-las, consulte [Notificações de eventos para AWS IoT Wireless](#) e [Ativar eventos para recursos sem fio](#).

## Tipos de eventos para recursos do Sidewalk

Os eventos que você pode ativar para seus recursos do Sidewalk incluem:

- Eventos do dispositivo que notificam você sobre alterações no estado do seu dispositivo do Sidewalk, como quando o dispositivo foi registrado e está pronto para uso.
- Eventos de proximidade que notificam você quando AWS IoT Wireless recebe uma notificação do Amazon Sidewalk de que um beacon foi descoberto ou perdido.

As seções a seguir contêm mais informações sobre os eventos de seus recursos do Sidewalk:

### Tópicos

- [Eventos de estado de registro do dispositivo](#)
- [Eventos de proximidade](#)

## Eventos de estado de registro do dispositivo

Eventos de estado de registro do dispositivo publicam notificações de eventos quando há uma alteração no estado de registro do dispositivo, como quando um dispositivo do Sidewalk foi provisionado ou registrado. Os eventos fornecem informações sobre os diferentes estados pelos quais o dispositivo passa desde o momento em que é provisionado até o momento em que é registrado.

## Como eventos de estado de registro do dispositivo funcionam

Quando você integra seu dispositivo do Sidewalk com o Amazon Sidewalk e AWS IoT Wireless, a AWS IoT Wireless executa uma operação `create` e adiciona seu dispositivo Sidewalk a sua Conta da AWS. Seu dispositivo então entra no estado `provisioned` e o `eventType` se torna `provisioned`. Para acessar informações sobre integrar seu dispositivo, consulte [Conceitos básicos do AWS IoT Core para Amazon Sidewalk](#).

Depois que o dispositivo estiver `provisioned`, o Amazon Sidewalk executa uma operação `register` para registrar seu dispositivo Sidewalk com AWS IoT Wireless. O processo de registro começa, onde a criptografia e as chaves de sessão são configuradas com AWS IoT. Quando o dispositivo é registrado, o `eventType` se torna `registered` e seu dispositivo está pronto para uso.

Depois que o dispositivo estiver `registered`, o Sidewalk poderá enviar uma solicitação para `deregister` seu dispositivo. A AWS IoT Wireless, em seguida, atende à solicitação e altera o estado do dispositivo de volta para `provisioned`. Para obter mais informações sobre os estados do dispositivo, consulte [DeviceState](#).

## Ativar notificações para eventos de estado de registro do dispositivo

Antes que os assinantes dos tópicos reservados do estado de registro do dispositivo possam receber mensagens, você deve habilitar as notificações de eventos para eles a partir do Console de gerenciamento da AWS, ou usando a API ou CLI. Você pode habilitar esses eventos para todos os recursos do Sidewalk em sua Conta da AWS ou para recursos selecionados. Para obter mais informações sobre como configurar esses eventos, consulte [Ativar eventos para recursos sem fio](#).

## Formato dos tópicos do MQTT para eventos de estado de registro de dispositivos

Para receber notificações sobre eventos do estado do registro do dispositivo, você pode se inscrever nos tópicos reservados do MQTT que começam com um cifrão (\$). Para obter mais informações, consulte [MQTT topics](#) no Guia do desenvolvedor do AWS IoT.

Os tópicos reservados do MQTT para eventos de estado de registro de dispositivos do Sidewalk usam o seguinte formato:

- Para tópicos em nível de recurso:

```
$aws/iotwireless/events/{eventName}/{eventType}/sidewalk/wireless_devices
```

- Para tópicos de identificador:

```
$aws/iotwireless/events/{eventName}/{eventType}/sidewalk/{resourceType}/  
{resourceID}/{id}
```

Em que:

{eventName}

{eventName} deve ser `device_registration_state`.

{eventType}

{eventType} pode ser `provisioned` ou `registered`.

{resourceType}

{resourceType} pode ser `sidewalk_accounts` ou `wireless_devices`.

{resourceID}

{resourceID} é `amazon_id` para {resourceType} de `sidewalk_accounts` e `wireless_device_id` para {resourceType} de `wireless_devices`.

Você também pode usar o caractere curinga + para se inscrever em vários tópicos ao mesmo tempo. O caractere curinga + corresponde a qualquer string no nível que contém o caractere. Por exemplo, se você quiser ser notificado sobre todos os tipos de eventos possíveis (`provisioned` e `registered`) e sobre todos os dispositivos registrados em um determinado ID da Amazon, você pode usar o seguinte filtro de tópicos:

```
$aws/iotwireless/events/device_registration_state/+ /sidewalk/  
sidewalk_accounts/amazon_id/+
```

#### Note

Você não pode usar o caractere curinga # para se inscrever nos tópicos reservados. Para obter mais informações sobre filtros de tópicos, consulte [MQTT topic filters](#) no Guia do desenvolvedor do AWS IoT.

## Carga útil de mensagens para eventos de estado de registro do dispositivo

Depois de ativar as notificações para eventos de estado de registro do dispositivo, as notificações de eventos são publicadas no MQTT com uma carga JSON. Esses eventos contêm os seguintes exemplos de carga:

```
{
  "eventId": "string",
  "eventType": "provisioned|registered",
  "WirelessDeviceId": "string",
  "timestamp": "timestamp",

  // Event-specific fields
  "operation": "create|deregister|register",
  "Sidewalk": {
    "AmazonId": "string",
    "SidewalkManufacturingSn": "string"
  }
}
```

As cargas contêm os seguintes atributos:

### eventId

Um ID de evento exclusivo (sequência).

### eventType

O tipo de evento que ocorreu. Pode ser `provisioned` ou `registered`.

### wirelessDeviceId

O identificador do dispositivo sem fio.

### timestamp

A data e hora do Unix de quando o evento ocorreu.

### operação

A operação que acionou o evento. Os valores válidos são `create`, `register` e `deregister`.

### sidewalk

O ID da Amazon do Sidewalk ou o `SidewalkManufacturingSn` para o qual quer receber notificações de eventos.

## Eventos de proximidade

Eventos de proximidade publicam notificações de eventos quando o AWS IoT recebe um beacon do dispositivo do Sidewalk. Quando seu dispositivo do Sidewalk se aproxima do Amazon Sidewalk, os beacons enviados do seu dispositivo são filtrados pelo Amazon Sidewalk em intervalos regulares e recebidos pela AWS IoT Wireless. A AWS IoT Wireless, em seguida, notifica você sobre esses eventos quando um beacon é recebido.

### Como funcionam os eventos de proximidade

Os eventos de proximidade notificam você quando o AWS IoT recebe um beacon. Os dispositivos Sidewalk podem emitir beacons a qualquer momento. Quando seu dispositivo está próximo ao Amazon Sidewalk, o Sidewalk recebe os beacons e os encaminha à AWS IoT Wireless em intervalos regulares. O Amazon Sidewalk configurou esse intervalo de tempo como 10 minutos. Quando a AWS IoT Wireless receber o beacon do Sidewalk, você receberá uma notificação do evento.

Os eventos de proximidade notificarão você quando um beacon for descoberto ou perdido. É possível configurar os intervalos nos quais você recebe notificação sobre o evento de proximidade.

### Ativar notificações para eventos de proximidade

Antes que os assinantes dos tópicos reservados de proximidade do Sidewalk possam receber mensagens, você deve habilitar as notificações de eventos para eles a partir do Console de gerenciamento da AWS, ou usando a API ou CLI. Você pode habilitar esses eventos para todos os recursos do Sidewalk em sua Conta da AWS ou para recursos selecionados. Para obter mais informações sobre como configurar esses eventos, consulte [Ativar eventos para recursos sem fio](#).

### Formato dos tópicos do MQTT para eventos de proximidade

Para receber notificações sobre eventos de proximidade, você pode se inscrever nos tópicos reservados do MQTT que começam com um cifrão (\$). Para obter mais informações, consulte [MQTT topics](#) no Guia do desenvolvedor do AWS IoT.

Os tópicos reservados do MQTT para eventos de proximidade no Sidewalk usam o formato:

- Para tópicos em nível de recurso:  
`$aws/iotwireless/events/{eventName}/{eventType}/sidewalk/wireless_devices`
- Para tópicos de identificador:

```
$aws/iotwireless/events/{eventName}/{eventType}/sidewalk/{resourceType}/  
{resourceID}/{id}
```

Em que:

{eventName}

{eventName} deve ser `proximity`.

{eventType}

{eventType} pode ser `beacon_discovered` ou `beacon_lost`.

{resourceType}

{resourceType} pode ser `sidewalk_accounts` ou `wireless_devices`.

{resourceID}

{resourceID} é `amazon_id` para {resourceType} de `sidewalk_accounts` e `wireless_device_id` para {resourceType} de `wireless_devices`.

Você também pode usar o caractere curinga + para se inscrever em vários tópicos ao mesmo tempo. O caractere curinga + corresponde a qualquer string no nível que contém o caractere. Por exemplo, se você quiser ser notificado sobre todos os tipos de eventos possíveis (`beacon_discovered` e `beacon_lost`) e sobre todos os dispositivos registrados em um determinado ID da Amazon, você pode usar o seguinte filtro de tópicos:

```
$aws/iotwireless/events/proximity/+ /sidewalk/sidewalk_accounts/amazon_id/+
```

#### Note

Você não pode usar o caractere curinga # para se inscrever nos tópicos reservados. Para obter mais informações sobre filtros de tópicos, consulte [MQTT topic filters](#) no Guia do desenvolvedor do AWS IoT.

## Carga útil de mensagens para eventos de proximidade

Depois de ativar as notificações para eventos de proximidade, as mensagens de eventos são publicadas no MQTT com uma carga JSON. Esses eventos contêm os seguintes exemplos de carga:

```
{
  "eventId": "string",
  "eventType": "beacon_discovered|beacon_lost",
  "WirelessDeviceId": "string",
  "timestamp": "1234567890123",

  // Event-specific fields
  "Sidewalk": {
    "AmazonId": "string",
    "SidewalkManufacturingSn": "string"
  }
}
```

As cargas contêm os seguintes atributos:

**eventId**

Um ID de evento exclusivo, que é uma string.

**eventType**

O tipo de evento que ocorreu. Pode ser `beacon_discovered` ou `beacon_lost`.

**WirelessDeviceId**

O identificador do dispositivo sem fio.

**timestamp**

A data e hora do Unix de quando o evento ocorreu.

**sidewalk**

O ID da Amazon do Sidewalk ou o `SidewalkManufacturingSn` para o qual quer receber notificações de eventos.

# Operações da API AWS IoT Wireless

As operações adicionais de API descritas abaixo podem ser executadas ao integrar os dispositivos finais LoRaWAN ou Sidewalk ou ao criar uma tarefa de importação para provisionar dispositivos finais do Sidewalk em massa.

As seções a seguir contêm informações adicionais sobre essas operações da API.

## Tópicos

- [Operações de API do AWS IoT Wireless para perfis de dispositivos](#)
- [Operações de API do AWS IoT Wireless para dispositivos LoRaWAN e Sidewalk](#)
- [Operações de API do AWS IoT Wireless para destinos de dispositivos sem fio](#)
- [Operações da API AWS IoT Core para Amazon Sidewalk para provisionamento em massa](#)

## Operações de API do AWS IoT Wireless para perfis de dispositivos

É possível executar as seguintes operações de API para perfis de dispositivos yourLoRaWAN e Sidewalk:

- API [CreateDeviceProfile](#) ou CLI [create-device-profile](#)
- API [GetDeviceProfile](#) ou CLI [get-device-profile](#)
- API [ListDeviceProfiles](#) ou CLI [list-device-profiles](#)
- API [DeleteDeviceProfile](#) ou CLI [delete-device-profile](#)

As seções a seguir mostram como listar e excluir perfis. Para obter informações sobre como criar e recuperar perfis de dispositivos, consulte:

- [Adicionar perfis de dispositivos](#)
- [Etapa 1: Criar um perfil do dispositivo](#)

## Listar perfis de dispositivos em sua Conta da AWS

Você pode usar a operação da API [ListDeviceProfiles](#) para listar os perfis de dispositivos em sua Conta da AWS que você adicionou ao AWS IoT Wireless. Você pode usar essas informações para identificar os dispositivos a que você deseja associar esse perfil.

Para filtrar a lista e exibir somente perfis de dispositivos LoRaWAN ou Sidewalk, defina Type ao executar a API. Um exemplo de um comando da CLI:

```
aws iotwireless list-device-profiles --wireless-device-type "Sidewalk"
```

A execução desse comando retorna uma lista dos perfis de dispositivo adicionados, incluindo o identificador do perfil e o nome do recurso da Amazon (ARN). Para recuperar detalhes adicionais sobre um perfil específico, use a API `GetDeviceProfile`.

```
{
  "DeviceProfileList": [
    {
      "Name": "SidewalkDeviceProfile1",
      "Id": "12345678-a1b2-3c45-67d8-e90fa1b2c34d",
      "Arn": "arn:aws:iotwireless:us-east-1:123456789012:DeviceProfile/12345678-
a1b2-3c45-67d8-e90fa1b2c34d"
    },
    {
      "Name": "SidewalkDeviceProfile2",
      "Id": "a1b2c3d4-5678-90ab-cdef-12ab345c67de",
      "Arn": "arn:aws:iotwireless:us-east-1:123456789012:DeviceProfile/
a1b2c3d4-5678-90ab-cdef-12ab345c67de"
    }
  ]
}
```

## Excluir perfis de dispositivos de sua Conta da AWS

Você pode excluir perfis de dispositivo usando a operação da API [DeleteDeviceProfile](#). Um exemplo de um comando da CLI é mostrado a seguir:

### Warning

As ações de exclusão não podem ser desfeitas. O perfil do dispositivo será removido permanentemente de sua Conta da AWS.

```
aws iotwireless delete-device-profile --name "SidewalkProfile"
```

Esse comando não retorna nenhuma saída. Você pode usar a API `GetDeviceProfile` ou a operação da API `ListDeviceProfiles` para verificar se o perfil foi removido da sua conta.

## Operações de API do AWS IoT Wireless para dispositivos LoRaWAN e Sidewalk

É possível executar as seguintes operações da API para dispositivos LoRaWAN e Sidewalk:

- API [CreateWirelessDevice](#) ou CLI [create-wireless-device](#)
- API [GetWirelessDevice](#) ou CLI [get-wireless-device](#)
- API [ListWirelessDevices](#) ou CLI [list-wireless-devices](#)
- API [DeleteWirelessDevice](#) ou CLI [delete-wireless-device](#)
- API [UpdateWirelessDevice](#) ou CLI [update-wireless-device](#)
- API [AssociateWirelessDeviceWithThing](#) ou CLI [associate-wireless-device-with-thing](#)
- API [DisassociateWirelessDeviceFromThing](#) ou CLI [disassociate-wireless-device-from-thing](#)

As seções a seguir mostram como listar e excluir dispositivos. Para obter informações sobre como criar dispositivos sem fio e recuperar informações do dispositivo, consulte:

- [Adicione o dispositivo sem fio ao AWS IoT Core for LoRaWAN](#)
- [Etapa 2: Adicionar o dispositivo do Sidewalk](#)

## Associar dispositivos sem fio em sua Conta da AWS a uma coisa de IoT

Para associar dispositivos LoRaWAN e Sidewalk a alguma coisa do AWS IoT, utilize a operação de API `AssociateWirelessDeviceWithThing`.

Coisas na AWS IoT facilitam a pesquisa e o gerenciamento de seus dispositivos. Associar alguma coisa ao seu dispositivo permite que ele acesse outros recursos do AWS IoT Core. Para obter mais informações sobre como utilizar essa API, consulte [AssociateWirelessDeviceWithThing](#).

O exemplo a seguir mostra a execução do comando. A execução desse comando não retorna nenhuma saída.

```
aws iotwireless associate-wireless-device-with-thing \  
  --id "12345678-a1b2-3c45-67d8-e90fa1b2c34d" \  
  --thing-arn "arn:aws:iot:us-east-1:123456789012:thing/MySidewalkThing"
```

Para desassociar o dispositivo sem fio de uma coisa do AWS IoT, utilize a operação de API [DisassociateWirelessDeviceFromThing](#), conforme mostrado no exemplo a seguir.

```
aws iotwireless disassociate-wireless-device-from-thing \  
  --id "12345678-a1b2-3c45-67d8-e90fa1b2c34d"
```

## Listar os dispositivos sem fio em sua Conta da AWS

Para listar os dispositivos sem fio em sua Conta da AWS adicionados ao AWS IoT Wireless, utilize a operação de API [ListWirelessDevices](#). Para filtrar a lista e retornar somente dispositivos LoRaWAN e Sidewalk, defina `WirelessDeviceType`.

O exemplo a seguir mostra a execução do comando:

```
aws iotwireless list-wireless-devices --wireless-device-type Sidewalk
```

A execução desse comando retorna uma lista dos dispositivos adicionados, incluindo o identificador do perfil e o nome do recurso da Amazon (ARN). Para recuperar detalhes adicionais sobre um dispositivo específico, use a operação da API [GetWirelessDevice](#).

```
{  
  "WirelessDeviceList": [  
    {  
      "Name": "mySidewalkDevice",  
      "DestinationName": "SidewalkDestination",  
      "Id": "1fffd32c8-8130-4194-96df-622f072a315f",  
      "Type": "Sidewalk",  
      "Sidewalk": {  
        "SidewalkId": "1234567890123456"  
      },  
      "Arn": "arn:aws:iotwireless:us-  
east-1:123456789012:WirelessDevice/1fffd32c8-8130-4194-96df-622f072a315f"  
    }  
  ]  
}
```

## Excluir dispositivos sem fio de sua Conta da AWS

Para excluir os dispositivos sem fio, passe o `WirelessDeviceID` dos dispositivos que você deseja excluir para a operação de API [DeleteWirelessDevice](#).

Um exemplo de comando é mostrado a seguir:

```
aws iotwireless delete-wireless-device --id "23456789-abcd-0123-bcde-fabc012345678"
```

Esse comando não retorna nenhuma saída. Você pode usar a API `GetWirelessDevice` ou a operação da API `ListWirelessDevices` para verificar se o dispositivo foi removido da sua conta.

## Operações de API do AWS IoT Wireless para destinos de dispositivos sem fio

É possível executar as seguintes operações de API para destinos dos dispositivos LoRaWAN e Sidewalk:

- API [CreateDestination](#) ou CLI [create-destination](#)
- API [GetDestination](#) ou CLI [get-destination](#)
- API [UpdateDestination](#) ou CLI [update-destination](#)
- API [ListDestinations](#) ou CLI [list-destinations](#)
- API [DeleteDestination](#) ou CLI [delete-destination](#)

As seções a seguir mostram como obter, listar, atualizar e excluir destinos. Para obter informações sobre a criação de destinos, consulte [Adicionar um destino para o dispositivo final do Sidewalk](#).

### Obter informações sobre o destino

É possível usar a operação da API [GetDestination](#) para obter informações sobre o destino que você adicionou à sua conta para AWS IoT Wireless. Fornecer o nome do destino como entrada para a API. A API retornará informações sobre o destino que correspondem ao identificador especificado.

Um exemplo de um comando da CLI é mostrado a seguir:

```
aws iotwireless get-destination --name SidewalkDestination
```

A execução desse comando retorna os parâmetros do seu destino.

```
{
  "Arn": "arn:aws:iotwireless:us-east-1:123456789012:Destination/
IoTWirelessDestination",
  "Name": "SidewalkDestination",
  "Expression": "IoTWirelessRule",
  "ExpressionType": "RuleName",
  "RoleArn": "arn:aws:iam::123456789012:role/IoTWirelessDestinationRole"
}
```

## Atualizar as propriedades do seu destino

Use a operação da API [UpdateDestination](#) para atualizar as propriedades do seu destino, que você adicionou à sua conta para AWS IoT Wireless. O exemplo a seguir mostra um comando da CLI que atualiza propriedade description:

```
aws iotwireless update-destination --name SidewalkDestination \
  --description "Destination for messages processed using IoTWirelessRule"
```

## Listar destinos em sua Conta da AWS

Utilize a operação de API [ListDestinations](#) para listar destinos em sua Conta da AWS, que você adicionou ao AWS IoT Wireless. Para filtrar a lista para retornar somente destinos para dispositivos finais LoRaWAN e Sidewalk, utilize o parâmetro `WirelessDeviceType`.

Um exemplo de um comando da CLI é mostrado a seguir:

```
aws iotwireless list-destinations --wireless-device-type "Sidewalk"
```

A execução desse comando retorna uma lista dos destinos adicionados, incluindo o nome do recurso da Amazon (ARN). Para recuperar detalhes adicionais sobre um destino específico, use a API `GetDestination`.

```
{
  "DestinationList": [
    {
      "Arn": "arn:aws:iotwireless:us-
east-1:123456789012:Destination/IoTWirelessDestination",
      "Name": "IoTWirelessDestination",

```

```
    "Expression": "IoTWirelessRule",
    "Description": "Destination for messages processed using IoTWirelessRule",
    "RoleArn": "arn:aws:iam::123456789012:role/IoTWirelessDestinationRole"
  },
  {
    "Arn": "arn:aws:iotwireless:us-
east-1:123456789012:Destination/IoTWirelessDestination2",
    "Name": "IoTWirelessDestination2",
    "Expression": "IoTWirelessRule2",
    "RoleArn": "arn:aws:iam::123456789012:role/IoTWirelessDestinationRole"
  }
]
```

## Excluir destinos da sua Conta da AWS

Para excluir um destino, passe o nome do destino a ser excluído como entrada para a operação da API [DeleteDestination](#). Um exemplo de um comando da CLI é mostrado a seguir:

### Warning

As ações de exclusão não podem ser desfeitas. O destino será removido permanentemente da sua Conta da AWS.

```
aws iotwireless delete-destination --name "SidewalkDestination"
```

Esse comando não retorna nenhuma saída. Você pode usar a API [GetDestination](#) ou a operação da API [ListDestinations](#) para verificar se o destino foi removido da sua conta.

## Operações da API AWS IoT Core para Amazon Sidewalk para provisionamento em massa

Você pode executar as seguintes operações da API para provisionamento em massa dos seus dispositivos finais do Sidewalk:

- API [StartWirelessDeviceImportTask](#) ou CLI [start-wireless-device-import-task](#)
- API [StartSingleWirelessDeviceImportTask](#) ou CLI [start-single-wireless-device-import-task](#)

- API [ListWirelessDeviceImportTasks](#) ou CLI [list-wireless-device-import-tasks](#)
- API [ListDevicesForWirelessDeviceImportTask](#) ou CLI [list-devices-for-wireless-device-import-task](#)
- API [GetWirelessDeviceImportTask](#) ou CLI [get-wireless-device-import-task](#)
- API [UpdateWirelessDeviceImportTask](#) ou CLI [update-wireless-device-import-task](#)
- API [DeleteWirelessDeviceImportTask](#) ou CLI [delete-wireless-device-import-task](#)

As seções a seguir mostram como obter, listar, atualizar e excluir tarefas de importação. Para obter informações sobre como criar tarefas de importação, consulte [Operações da API AWS IoT Core para Amazon Sidewalk para provisionamento em massa](#).

## Obter informações sobre a tarefa de importação

Você pode usar a operação da API [ListDevicesForWirelessDeviceImportTask](#) para recuperar informações sobre uma tarefa de importação específica e o status de integração dos dispositivos nessa tarefa. Como entrada para a operação da API, especifique o ID da tarefa de importação obtida das operações da API [StartWirelessDeviceImportTask](#) ou [StartSingleWirelessDeviceImportTask](#). A API retornará informações sobre a tarefa de importação que correspondem ao identificador especificado.

Um exemplo de um comando da CLI é mostrado a seguir:

```
aws iotwireless list-devices-for-wireless-device-import-task --id e2a5995e-743b-41f2-a1e4-3ca6a5c5249f
```

A execução desse comando retorna as informações sobre a tarefa de importação e o status de integração do dispositivo.

```
{
  "DestinationName": "SidewalkDestination",
  "ImportedWirelessDeviceList": [
    {
      "Sidewalk": {
        "OnboardingStatus": "ONBOARDED",
        "LastUpdateTime": "2023-02021T06:11:09.151Z",
        "SidewalkManufacturingSn":
          "82B83C8B35E856F43CE9C3D59B418CC96B996071016DB1C3BE5901F0F3071A4A"
      }
    },
  ],
}
```

```
    "Sidewalk": {
      "OnboardingStatus": "PENDING",
      "LastUpdateTime": "2023-02021T06:22:12.061Z",
      "SidewalkManufacturingSn":
"12345ABCDE6789FABDESBDEF123456789012345FEABC0123679AFEB01234EF"
    },
  }
]
```

## Obter o resumo de dispositivo da tarefa de importação

Para obter uma contagem de informações de resumo do status de integração dos dispositivos adicionados a uma tarefa de importação específica, use a operação da API [GetWirelessDeviceImportTask](#). Um exemplo de um comando da CLI é mostrado a seguir.

```
aws iotwireless get-wireless-device-import-task --Id "e2a5995e-743b-41f2-
a1e4-3ca6a5c5249f"
```

O código a seguir mostra um exemplo de resposta do comando.

```
{
  "NumberOfFailedImportedDevices": 2,
  "NumberOfOnboardedImportedDevices": 4,
  "NumberOfPendingImportedDevices": 1
}
```

## Adicionar dispositivos a uma tarefa de importação

Use a operação da API `UpdateWirelessDeviceImportTask` para adicionar dispositivos a uma tarefa de importação existente adicionada. Você pode usar essa operação da API para adicionar os números de série (SMSN) de dispositivos que não tenham sido incluídos anteriormente na tarefa criada usando a operação da API `StartWirelessDeviceImportTask`.

Para acrescentar dispositivos à tarefa de importação, como parte da solicitação da API, especifique um novo arquivo CSV em um bucket do Amazon S3 que contém os números de série dos dispositivos a serem adicionados. A solicitação será aceita somente se o processo de integração ainda não tiver sido iniciado para os dispositivos que estão atualmente na tarefa de importação. Se o processo de integração já tiver sido iniciado, a solicitação da API `UpdateWirelessDeviceImportTask` falhará.

Se você ainda quiser acrescentar dispositivos à tarefa de importação, poderá realizar a operação da API `UpdateWirelessDeviceImportTask` pela segunda vez. Antes de realizar essa operação da API, a primeira solicitação da API `UpdateWirelessDeviceImportTask` deve ter concluído o processamento do arquivo CSV no bucket do S3.

### Note

Quando você executa uma solicitação da API `ListImportedWirelessDeviceTasks`, o URL do S3 do novo arquivo CSV especificado usando a operação da API `UpdateWirelessDeviceImportTask` não é retornada, no momento. Em vez disso, a operação da API retorna o URL do S3 da solicitação enviada originalmente usando a solicitação da API `StartWirelessDeviceImportTask`.

Um exemplo de um comando da CLI é mostrado a seguir.

```
aws iotwireless update-wireless-device-import task \  
  --Id "e2a5995e-743b-41f2-a1e4-3ca6a5c5249f" \  
  --sidewalk '{"FileForCreateDevices": "s3://import_task_bucket/import_file3"}'
```

## Listar as tarefas de importação em sua Conta da AWS

Use a API `ListWirelessDeviceImportTasks` ou o comando `list-imported-wireless-device-tasks` da CLI para listar as tarefas de importação em sua Conta da AWS. Um exemplo de um comando da CLI é mostrado a seguir.

```
aws iotwireless list-wireless-device-import-tasks
```

A execução desse comando retornará uma lista de tarefas de importação que você criou. A lista inclui os arquivos CSV do Amazon S3 e o perfil do IAM especificado, o ID da tarefa de importação e informações resumidas do status da integração do dispositivo.

```
{  
  "ImportWirelessDeviceTaskList": [  
    {  
      "FileForCreateDevices": "s3://import_task_bucket/import_file1",  
      "ImportTaskId": "e2a5995e-743b-41f2-a1e4-3ca6a5c5249f",  
      "NumberOfFailedImportedDevices": 1,  
      "NumberOfOnboardedImportedDevices": 3,  
    }  
  ]  
}
```

```
    "NumberOfPendingImportedDevices": 2,
    "Role": "arn:aws:iam::123456789012:role/service-role/ACF1zBEI",
    "TimeStamp": "1012202218:23:55"
  },
  {
    "FileForCreateDevices": "s3://import_task_bucket/import_file2",
    "ImportTaskId": "a1b234c5-67ef-21a2-a1b2-3cd4e5f6789a",
    "NumberOfFailedImportedDevices": 2,
    "NumberOfOnboardedImportedDevices": 4,
    "NumberOfPendingImportedDevices": 1,
    "Role": "arn:aws:iam::123456789012:role/service-role/CDEFaBC1",
    "TimeStamp": "1201202210:12:20"
  }
]
```

## Excluir tarefas de importação de sua Conta da AWS

Para excluir uma tarefa de importação, passe o ID da tarefa de importação para a operação da API `DeleteWirelessDeviceImportTask` ou para o comando `delete-wireless-device-import-task` da CLI.

### Warning

As ações de exclusão não podem ser desfeitas. A tarefa de importação será removida permanentemente da sua Conta da AWS.

Quando você executa a solicitação da API `DeleteWirelessDeviceImportTask`, um processo em segundo plano começa a excluir a tarefa de importação. Quando a solicitação está em andamento, os números de série (SMSN) dos dispositivos nas tarefas de importação estão em processo de exclusão. Somente após a conclusão da exclusão, você poderá ver essas informações usando as operações da API `ListImportedWirelessDeviceTasks` ou `GetImportedWirelessDeviceTasks`.

Se uma tarefa de importação ainda contiver dispositivos aguardando a integração, a solicitação da API `DeleteWirelessDeviceImportTask` será processada somente depois que todos os dispositivos na tarefa de importação tiverem sido integrados ou houver falha na integração. Uma tarefa de importação expira após 90 dias e, quando expirar, ela poderá ser excluída da sua conta. No entanto, os dispositivos integrados com sucesso usando a tarefa de importação não serão excluídos.

**Note**

Se você tentar criar outra tarefa de importação que inclua o número de série de um dispositivo com exclusão pendente usando a solicitação da API `DeleteWirelessDeviceImportTask`, a operação da API `StartWirelessDeviceImportTask` retornará um erro.

Um exemplo de um comando da CLI é mostrado a seguir:

```
aws iotwireless delete-import-task --Id "e2a5995e-743b-41f2-a1e4-3ca6a5c5249f"
```

Esse comando não retorna nenhuma saída. Depois que a tarefa for excluída, para verificar se a tarefa de importação foi removida da sua conta, você pode usar a operação da API `GetWirelessDeviceImportTask` ou `ListWirelessDeviceImportTasks`.

# Criar recursos do AWS IoT Wireless com o AWS CloudFormation

O AWS IoT Wireless é integrado ao AWS CloudFormation, um serviço que ajuda você a modelar e a configurar seus recursos da AWS para reduzir o tempo dedicado à criação e ao gerenciamento de recursos e infraestrutura. Você cria um modelo que descreve todos os recursos AWS que deseja, e o CloudFormation se encarrega de provisionar e configurar esses recursos para você.

Ao utilizar o CloudFormation, é possível reutilizar seu modelo para configurar os recursos do AWS IoT Wireless de forma consistente e repetível. Descreva seus recursos uma vez e depois provisione os mesmos recursos repetidamente em várias regiões e Contas da AWS.

## Modelos do AWS IoT Wireless e do CloudFormation

Para provisionar e configurar recursos para o AWS IoT Wireless e serviços relacionados, você precisa conhecer os [modelos do CloudFormation](#). Os modelos são arquivos de texto formatados em JSON ou YAML. Esses modelos descrevem os atributos que você deseja provisionar nas suas pilhas CloudFormation. Se não estiver familiarizado com JSON ou YAML, você pode usar CloudFormation Designer para ajudá-lo a começar a usar os modelos CloudFormation. Para obter mais informações, consulte [O que é o CloudFormation Designer?](#) no Manual do usuário da AWS CloudFormation.

O AWS IoT Wireless permite a criação de recursos sem fio no CloudFormation. Para obter mais informações, incluindo exemplos de modelos JSON e YAML para os recursos do AWS IoT Wireless, consulte a [Referência de tipo de recurso do AWS IoT Wireless](#) no Guia do usuário do AWS CloudFormation.

## Saiba mais sobre a CloudFormation

Para saber mais sobre a CloudFormation, consulte os seguintes recursos:

- [AWS CloudFormation](#)
- [Guia do Usuário AWS CloudFormation](#)
- [Guia do Usuário da Interface de Linha de Comando AWS CloudFormation](#)

# Cotas do AWS IoT Wireless

Sua Conta da AWS tem cotas padrão, anteriormente chamadas de limites, para cada serviço da AWS service (Serviço da AWS). A menos que especificado de outra forma, cada cota é específica da região . Você pode solicitar o aumento de algumas cotas, porém, algumas delas não podem ser aumentadas.

Para visualizar todas as cotas do AWS IoT Wireless, abra o console do [Service Quotas](#). No painel de navegação, escolha AWS service (Serviço da AWS) e selecione AWS IoT Wireless.

Para solicitar o aumento da cota, consulte [Solicitar um aumento de cota](#) no Guia do usuário do Service Quotas. Se a cota ainda não estiver disponível no Service Quotas, use o [formulário de aumento de limite](#).

O AWS IoT Wireless tem cotas para:

- Cotas do AWS IoT Core for LoRaWAN que se aplicam aos dados de dispositivos que são transmitidos entre os dispositivos
- Operações de API do AWS IoT Wireless que se aplicam a dispositivos LoRaWAN e Sidewalk.

Para obter mais informações, consulte [AWS IoT Core for LoRaWAN quotas](#), na Referência geral da AWS.

# Marcando seus Recursos AWS IoT Wireless

Para ajudar no gerenciamento e na organização de seus dispositivos, gateways, destinos e perfis, é possível, opcionalmente, atribuir seus próprios metadados a cada um desses recursos em forma de tags. Esta seção descreve as tags e mostra como criá-las. O AWS IoT Wireless não tem grupos de faturamento e utiliza os mesmos grupos de faturamento usados pelo AWS IoT Core. Para obter mais informações, consulte [Billing groups](#) na documentação do AWS IoT Core.

## Conceitos Básicos de Tags

Quando você tem vários recursos do AWS IoT Wireless do mesmo tipo, é possível utilizar tags para categorizá-los de diferentes formas (por exemplo, por finalidade, proprietário ou ambiente). Isso ajuda a identificar rapidamente um recurso com base nas tags que você atribuiu a ele.

Cada tag consiste em uma chave e em um valor opcional, ambos definidos por você. Por exemplo, é possível definir um conjunto de tags para um grupo de dispositivos LoRaWAN para os quais o respectivo firmware está sendo atualizado. Para gerenciar seus recursos mais facilmente, recomendamos que você crie um conjunto consistente de chaves de tags que atenda às suas necessidades para cada tipo de recurso.

Você pode pesquisar e filtrar recursos conforme as tags que adicionar ou aplicar. Você também pode utilizar tags para controlar o acesso aos recursos utilizando políticas do IAM e tags do grupo de faturamento para categorizar e monitorar os custos.

## Criar e gerenciar tags

É possível criar e gerenciar tags utilizando o Editor de tags no Console de gerenciamento da AWS, no AWS IoT Wireless ou na AWS CLI.

### Usar o console

Para facilitar o uso, o Tag Editor no Console de gerenciamento da AWS fornece uma forma central e unificada para criar e gerenciar suas tags. Para obter mais informações, consulte [Como trabalhar com o Tag Editor](#) no [Como trabalhar com o Console de gerenciamento da AWS](#).

### Como usar a API ou a CLI

Também é possível utilizar a API ou a CLI e associar as tags a dispositivos sem fio, gateways, perfis e destinos ao criá-las utilizando o campo Tags nos seguintes comandos:

- [AssociateAwsAccountWithPartnerAccount](#)
- [CreateDestination](#)
- [CreateDeviceProfile](#)
- [CreateFuotaTask](#)
- [CreateMulticastGroup](#)
- [CreateServiceProfile](#)
- [CreateWirelessGateway](#)
- [CreateWirelessGatewayTaskDefinition](#)
- [CreateWirelessDevice](#)
- [API\\_StartBulkAssociateWirelessDeviceWithMulticastGroup](#)

## Atualizar tags ou listar tags de recursos

Você pode adicionar, modificar ou excluir tags de recursos existentes que oferecem suporte a marcação, usando os seguintes comandos:

- [TagResource](#)
- [ListTagsForResource](#)
- [UntagResource](#)

É possível editar chaves de tags e valores, e é possível remover as tags de um recurso a qualquer momento. É possível definir o valor de uma tag a uma string vazia, mas não pode configurar o valor de um tag como nula. Caso adicione uma tag com a mesma chave de outra existente no recurso, o novo valor substituirá o antigo. Se você excluir um recurso, todas as tags associadas ao recurso também serão excluídas.

## Restrições e limitações de tags

As restrições básicas a seguir se aplicam a tags:

- Número máximo de tags por recurso: 50.

- Comprimento máximo da chave: 127 caracteres Unicode em UTF-8.
- Comprimento do valor máximo: 255 caracteres Unicode em UTF-8.
- As chaves e valores das tags diferenciam maiúsculas de minúsculas.
- Não use o prefixo `aws:` no nome nem no valor das suas tags. Ele é reservado para uso da AWS. Você não pode editar nem excluir nomes ou valores de tag com esse prefixo. As tags com esse prefixo não contam para as tags por limite de recurso.
- Se o seu esquema de tags é usado em vários serviços e recursos, lembre-se de que outros serviços talvez tenham restrições em caracteres permitidos. Os caracteres permitidos incluem letras, espaços e números representáveis em UTF-8, além dos seguintes caracteres especiais: `+ - = . _ : / @`.

## Utilização de tags com políticas do IAM

Para especificar os recursos do IAM que um usuário pode criar, modificar ou utilizar, é possível aplicar permissões em nível de recurso baseadas em tags às políticas do IAM que você utiliza para a maioria das ações de API do AWS IoT Wireless. Para controlar o acesso do usuário (permissões) com base nas tags de um recurso, utilize o elemento `Condition` (também chamado de bloco `Condition`) com as chaves de contexto e valores de condição a seguir em uma política do IAM.

- Use `aws:ResourceTag/tag-key: tag-value`, para permitir ou negar ações do usuário em recursos com tags específicas.
- Use `aws:RequestTag/tag-key: tag-value` para exigir que uma tag específica seja (ou não seja) usada ao fazer uma solicitação de API para criar ou modificar um recurso que permite tags.
- Use `aws:TagKeys: [tag-key, ...]` para exigir que um conjunto específico de chaves de tag seja (ou não seja) usado ao fazer uma solicitação de API para criar ou modificar um recurso que permite tags.

### Note

Os valores e as chaves de contexto de condição em uma política do IAM se aplicam somente às ações do AWS IoT em que um identificador de um recurso que pode ser marcado com tags é um parâmetro obrigatório. Por exemplo, o uso de [DescribeEndpoint](#) não é permitido ou é negado com base nas chaves de contexto e valores de condição, pois nenhum recurso que pode ser marcado é referido nessa solicitação.

Para obter mais informações sobre o uso de tags, consulte [Controlar o acesso usando tags](#) no Guia do usuário do AWS Identity and Access Management. A seção [Referência de política JSON do IAM](#) desse guia detalhou a sintaxe, as descrições e os exemplos dos elementos, variáveis e lógica de avaliação das políticas JSON no IAM.

A política de exemplo a seguir aplica duas restrições com base em tag. Um usuário do IAM restrito por essa política:

- Não pode atribuir um recurso à tag “env=prod” (consulte a linha “aws:RequestTag/env” : “prod” no exemplo).
- Não pode modificar ou acessar um recurso que tenha uma tag existentes “env=prod” (consulte a linha “aws:ResourceTag/env” : “prod” no exemplo).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "iot:CreateMulticastGroup",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/env": "prod"
        }
      }
    },
    {
      "Effect": "Deny",
      "Action": [
        "iot:CreateMulticastGroup",
        "iot:UpdateMulticastGroup",
        "iot:GetMulticastGroup",
        "iot:ListMulticastGroups"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/env": "prod"
        }
      }
    }
  ],
}
```

```
{
  "Effect": "Allow",
  "Action": [
    "iot:CreateMulticastGroup",
    "iot:UpdateMulticastGroup",
    "iot:GetMulticastGroup",
    "iot:ListMulticastGroups"
  ],
  "Resource": "*"
}
```

Você também pode especificar vários valores de tag para uma determinada chave de tag, colocando-as em uma lista como esta:

```
"StringEquals" : {
  "aws:ResourceTag/env" : ["dev", "test"]
}
```

#### Note

Se você permitir ou negar aos usuários o acesso a recursos com base em tags, considere negar explicitamente aos usuários a capacidade de adicionar essas tags ou removê-las dos mesmos recursos. Caso contrário, é possível que um usuário contorne suas restrições e obtenha acesso a um recurso modificando as tags.

# Histórico do documento para o Guia do usuário do AWS IoT Wireless

A tabela a seguir descreve as versões da documentação do AWS IoT Wireless.

| Alteração                          | Descrição                                               | Data                   |
|------------------------------------|---------------------------------------------------------|------------------------|
| <a href="#">Lançamento inicial</a> | A versão inicial do Guia do usuário do AWS IoT Wireless | 31 de dezembro de 2020 |