aws

Guida per gli sviluppatori

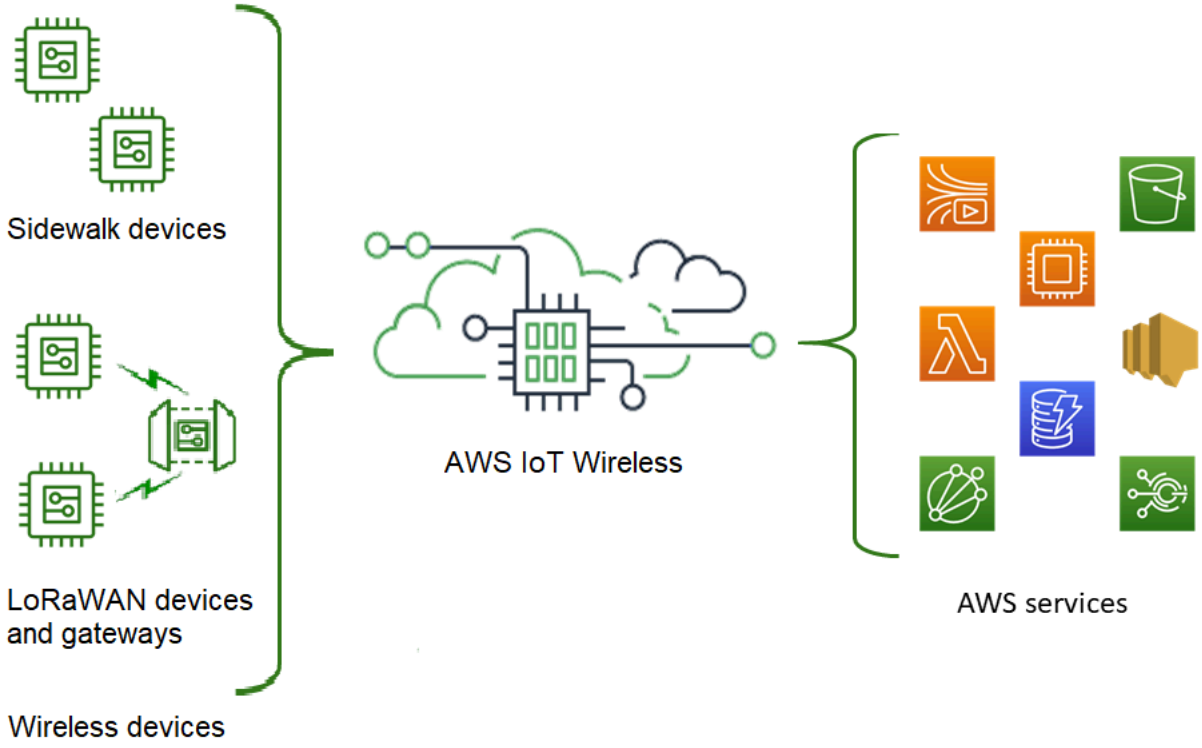
Wireless AWS IoT

Wireless AWS IoT: Guida per gli sviluppatori

Table of Contents

Che cos'è Wireless AWS IoT?

Wireless AWS IoT fornisce i servizi cloud che connettono i dispositivi wireless ad altri dispositivi e servizi Cloud AWS. Collegando i tuoi dispositivi a AWS IoT Wireless, puoi integrarli in soluzioni basate su AWS IoT. Utilizzando Wireless AWS IoT, puoi integrare sia dispositivi LoRaWAN che dispositivi Sidewalk a AWS IoT. Questi dispositivi wireless utilizzano il protocollo di comunicazione LPWAN (Low Power Wide Area Networking) per comunicare con AWS IoT.



Caratteristiche di AWS IoT Wireless

AWS IoT Wireless offre le seguenti caratteristiche:

Onboarding di dispositivi LoRaWAN e Sidewalk

È possibile integrare sia dispositivi LoRaWAN che dispositivi Sidewalk a AWS IoT Wireless.

- AWS IoT Core per LoRaWAN

  Per effettuare l'onboarding dei tuoi dispositivi e gateway LoRaWAN in Wireless AWS IoT, usa AWS IoT Core per LoRaWAN. Si tratta di un server di rete LoRaWAN (LNS) completamente gestito che elimina la necessità di configurare e gestire un LNS privato. AWS IoT Core per LoRaWAN fornisce

la gestione del gateway utilizzando le funzionalità CUPS (Configuration and Update Server) e FUOTA (Firmware Updates Over-The-Air). Per ulteriori informazioni, consultare Cos'è AWS IoT Core per LoRaWAN?.

- AWS IoT Core per Amazon Sidewalk

  Per effettuare l'onboarding dei tuoi dispositivi Sidewalk in Wireless AWS IoT, puoi utilizzare le funzionalità offerte da AWS IoT Core per Amazon Sidewalk. Amazon Sidewalk è una rete condivisa che collega dispositivi come Amazon Echo, le videocamere di sicurezza Ring, le luci esterne e può supportare altri dispositivi Sidewalk nella tua community. Per ulteriori informazioni, consultare Cos'è AWS IoT Core per Amazon Sidewalk?.

Integrazione con AWS IoT Core

Puoi utilizzare le seguenti funzionalità offerte dall'integrazione di Wireless AWS IoT con AWS IoT Core:

- Associazione dei dispositivi a qualsiasi oggetto AWS IoT

  Puoi associare i dispositivi wireless e i gateway a un oggetto AWS IoT che ti consente di memorizzare una rappresentazione del dispositivo su Cloud. Puoi usare oggetti in AWS IoT per cercare e gestire più facilmente i tuoi dispositivi e accedere ad altre funzionalità AWS IoT Core. Per ulteriori informazioni, consultare Gestione di dispositivi con AWS IoT nella Guida per gli sviluppatori di AWS IoT Core.
- Utilizzo delle regole AWS IoT per instradare i messaggi

  Puoi utilizzare la funzionalità delle regole di AWS IoT per interagire con altri Servizio AWS e applicazioni. I messaggi Uplink inviati dai dispositivi al cloud possono essere indirizzati a questi servizi e ad altre applicazioni. Per ulteriori informazioni, consultare Regole per AWS IoT nella Guida per gli sviluppatori di AWS IoT Core.

Per gli utenti alle prime armi di Wireless AWS IoT

Se usi Wireless AWS IoT per la prima volta, ti consigliamo di iniziare leggendo le seguenti sezioni:

- Cos'è AWS IoT Core per LoRaWAN?

  Questa sezione offre una panoramica della tecnologia LoRaWAN e di come funziona AWS IoT Core per LoRaWAN. Fornisce inoltre risorse per aiutarti a saperne di più.

- Cos'è AWS IoT Core per Amazon Sidewalk?

  Questa sezione offre una panoramica della tecnologia Amazon Sidewalk e di come funziona AWS IoT Core per Amazon Sidewalk. Fornisce inoltre risorse per aiutarti a saperne di più.

- Nozioni di base sull'utilizzo di AWS IoT Core per Amazon Sidewalk

  Leggi questa sezione per scoprire come usare AWS IoT Core per Amazon Sidewalk e come effettuare l'onboarding dei tuoi dispositivi Amazon Sidewalk.

- Collegamento di gateway e dispositivi ad AWS IoT Core per LoRaWAN

  In seguito, potrai apprendere ulteriori informazioni su come integrare i tuoi dispositivi LoRaWAN utilizzando la console e l'API.

Servizi correlati

- Amazon CloudWatch

  Dopo aver effettuato l'onboarding dei dispositivi LoRaWAN o Sidewalk in AWS IoT Wireless, puoi utilizzare Amazon CloudWatch per registrare e monitorare i tuoi dispositivi wireless e gateway in tempo reale. Per monitorare i dispositivi e i gateway LoRaWAN, puoi utilizzare anche l'analizzatore di rete, che riduce il tempo necessario per impostare una connessione e iniziare a ricevere i messaggi di tracciamento.

- AWS IoT Core

  Puoi utilizzare inoltre l'integrazione AWS IoT Core per connetterti ai Servizio AWS a cui è possibile accedere dal motore delle regole. Per ulteriori informazioni, consultare I Servizio AWS utilizzati dal motore delle regole.

Accesso a Wireless AWS IoT

Puoi utilizzare la console, l'API o la CLI per effettuare l'onboarding dei tuoi dispositivi LoRaWAN e Sidewalk.

- Utilizzo della console di AWS IoT

  Per effettuare l'onboarding dei tuoi dispositivi wireless, usa la pagina AWS IoT Wireless di AWS Management Console.

- Uso dell'API AWS IoT Wireless

  Puoi integrare sia dispositivi LoRaWAN che dispositivi Sidewalk utilizzando l'API AWS IoT Wireless. L'API AWS IoT Wireless su cui si basa AWS IoT Core è supportata dall'AWS SDK. Per ulteriori informazioni, consulta AWS SDKs and Toolkits (SDK e kit di strumenti).

- Utilizzo di AWS CLI

  Puoi utilizzare la AWS CLI per eseguire comandi per l'onboarding e la gestione dei dispositivi LoRaWAN e Amazon Sidewalk. Per ulteriori informazioni, consulta la documentazione di riferimento dell'interfaccia della riga di comando AWS IoT Wireless.

Nozioni di base su Wireless AWS IoT

Puoi accedere alle nozioni di base su AWS IoT Wireless registrandoti a un Account AWS e seguendo i passaggi per creare un utente IAM. Dopo esserti registrato, puoi utilizzare la AWS Management Console, l'API AWS IoT Wireless o la AWS CLI per effettuare l'onboarding dei tuoi dispositivi e gateway Sidewalk e LoRaWAN. Durante l'onboarding dei dispositivi, considera come descrivere ed etichettare le risorse per identificarle più facilmente.

I seguenti argomenti offrono le nozioni di base su AWS IoT Wireless.

Argomenti

Configurazione di Wireless AWS IoT

Quando effettui la registrazione ad AWS, il tuo account Account AWS viene automaticamente registrato per tutti i servizi in AWS, incluso AWS IoT Wireless. Ti vengono addebitati solo i servizi che utilizzi.

Per configurare AWS IoT Wireless, attieniti alla procedura descritta nella sezione seguente:

Argomenti

Configurare l'account Account AWS

Prima di usare AWS IoT Core per LoRaWAN o AWS IoT Core per Amazon Sidewalk per la prima volta, devi completare le seguenti operazioni di configurazione del tuo Account AWS:

Argomenti

Effettua la registrazione per creare un account AWS.

Se non disponi di un Account AWS, completa la procedura seguente per crearne uno.

Per registrarsi a un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Durante la registrazione di un Account AWS, viene creato un Utente root dell'account AWS. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWSnell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente amministrativo e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

Crea un utente IAM

Per creare un utente amministratore, scegli una delle seguenti opzioni.

Scelta di un modo per gestire il tuo amministratore	Per	Come	Puoi anche
In IAM Identity Center (Consigliato)	Usa credenziali a breve termine per accedere a AWS. Ciò è in linea con le best practice per la sicurezza. Per informazioni sulle best practice, consulta	Segui le istruzioni riportate in Nozioni di base nella Guida per l'utente di AWS IAM Identity Center.	Configura l'accesso programmatico seguendo quanto riportato in Configurazione della AWS CLI per utilizzare AWS IAM Identity Center nella Guida per l'utente di AWS Command Line Interface.

Scelta di un modo per gestire il tuo amministratore	Per	Come	Puoi anche
	Best practice per la sicurezza in IAM nella Guida per l'utente di IAM.		
In IAM (Non consigliato)	Usa credenziali a lungo termine per accedere a AWS.	Segui le istruzioni in Creazione del primo utente e gruppo di utenti IAM di amministrazione nella Guida per l'utente di IAM.	Configura l'accesso programmatico seguendo quanto riportato in Gestione delle chiavi di accesso per gli utenti IAM nella Guida per l'utente di IAM.

Accesso come utente IAM

Dopo aver creato un utente IAM, puoi accedere ad AWS con il nome utente e la password IAM.

Prima di accedere come utente IAM, puoi verificare il link di accesso per gli utenti IAM nella console IAM. Nel pannello di controllo IAM, nel link di accesso degli utenti IAM, puoi visualizzare il link di accesso per l'Account AWS. L'URL del link di accesso contiene il tuo ID account Account AWS senza trattini (-).

Se non desideri che l'URL per il tuo link di accesso contenga il tuo ID Account AWS, puoi creare un alias dell'account. Per maggiori informazioni, consulta Creazione, eliminazione e visualizzazione di un alias di un account Account AWS nella Guida per l'utente di IAM.

Accesso come utente IAM

1. Disconnettiti dalla AWS Management Console.
2. Inserisci il tuo link di accesso, che include il tuo ID Account AWS (senza trattini) o l'alias Account AWS.

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

3. Immettere il nome utente e la password di IAM appena creati.

Una volta effettuato l'accesso, la barra di navigazione visualizza *"your_user_name @ your_aws_account_id"*.

Installazione di Python e della AWS CLI

Prima di collegare il dispositivo finale LoRaWAN o Sidewalk, è necessario installare Python e configurare la AWS CLI.

> **Important**
>
> Per eseguire l'intero flusso di lavoro di onboarding per il provisioning e la registrazione del dispositivo finale Sidewalk, è necessario anche configurare il gateway Sidewalk e l'HDK. Per istruzioni, consultare le pagine relative alla configurazione del kit di sviluppo dell'hardware (HDK) e alla configurazione di un gateway Sidewalk nella documentazione di Amazon Sidewalk.

Argomenti

- Installazione di Python e Python3-PIP
- Configurazione di AWS CLI

Installazione di Python e Python3-PIP

Per utilizzare AWS CLI e boto3 come descritto nella sezione successiva, è necessario utilizzare Python versione 3.6 o successive. Se si desidera eseguire l'onboarding dei dispositivi finali utilizzando la console AWS IoT, è possibile saltare questa sezione e continuare a configurare Account AWS. Per verificare se Python e Python3-PIP sono già installati, esegui i comandi seguenti. Se l'esecuzione di questi comandi restituisce la versione, significa che Python e Python3-PIP sono stati installati correttamente.

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

Se questo comando restituisce un errore, è possibile che Python non sia installato o che il sistema operativo chiami l'eseguibile Python v3.x come Python3. In tal caso, sostituisci tutte le istanze di `python` con `python3` quando esegui i comandi. Se l'errore persiste, scarica ed esegui il programma di installazione di Python o installa Python a seconda del sistema operativo in uso come descritto di seguito.

Windows

Sul computer Windows, scarica Python dal sito Web di Python, quindi esegui il programma di installazione per installare Python sul computer.

Linux

Sul computer Ubuntu, esegui il comando `sudo` seguente per installare Python.

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

macOS

Sul computer Mac, utilizza Homebrew per installare Python. Homebrew installa anche pip, che quindi punta alla versione Python3 installata.

```
$ brew install python
```

Configurazione di AWS CLI

Nei passaggi seguenti viene illustrato come configurare AWS CLI e boto3 (AWS SDK per Python). Prima di seguire questi passaggi, devi registrarti a Account AWS e creare un utente amministrativo. Per istruzioni, consulta Configurazione di Wireless AWS IoT.

1. Installazione e configurazione dell'AWS CLI

   Puoi utilizzare la AWS CLI per eseguire l'onboarding programmatico dei dispositivi finali Sidewalk in AWS IoT Core per Amazon Sidewalk. Se desideri eseguire l'onboarding dei dispositivi utilizzando la console AWS IoT, puoi saltare questa sezione. Apri la console AWS IoT Core e continua con la sezione successiva per iniziare a connettere i dispositivi a AWS IoT Core per Amazon Sidewalk. Per istruzioni sulla configurazione di AWS CLI, consultare la pagina relativa all'installazione e alle configurazione di AWS CLI.

2. Installazione di boto3 (AWS SDK per Python)

   I seguenti comandi mostrano come installare boto3 (AWS SDK per Python) e AWS CLI. Verrà installato anche botocore, che è richiesto per eseguire boto3. Per istruzioni dettagliate, consultare Installazione di Boto3 nella Guida alla documentazione di Boto3.

   > **Note**
   >
   > `awscli` versione `1.26.6` richiede PyYAML versione 3.10 o successiva, ma non successiva alla 5.5.

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

3. Configurazione delle credenziali e della regione predefinita

   Configura le credenziali e la regione predefinita nei file `~/.aws/credentials` e `~/.aws/config`. La libreria boto3 utilizza queste credenziali per identificare Account AWS e autorizzare le chiamate API. Per le istruzioni di configurazione, consultare:

   - Configurazione nella Guida alla documentazione di Boto3
   - Configurazione e impostazioni del file delle credenziali nella Guida alla documentazione di AWS CLI

Descrizione delle risorse AWS IoT Wireless

Prima di iniziare l'onboarding dei dispositivi LoRaWAN o Sidewalk, devi considerare la convenzione di denominazione dei dispositivi, dei gateway e della destinazione. AWS IoT Wireless offre diverse opzioni per identificare le risorse create. Quando vengono create, alle risorse AWS IoT Wireless viene assegnato un ID univoco che non è descrittivo né può essere modificato dopo la creazione della risorsa. Per rendere più agevole la selezione, l'identificazione e la gestione delle risorse, è possibile assegnare un nome, aggiungere una descrizione e assegnare tag e valori di tag alla maggior parte delle risorse AWS IoT Wireless.

- Nomi delle risorse e descrizione

Per gateway, dispositivi e profili, il nome della risorsa è un campo facoltativo che è possibile modificare dopo la creazione della risorsa. Il nome viene visualizzato negli elenchi visualizzati nelle pagine dell'hub delle risorse.

Per le destinazioni, fornisci un nome univoco al tuo account AWS e alla regione Regione AWS. Non è possibile modificare il nome di destinazione dopo aver creato la risorsa di destinazione.

Mentre un nome può contenere fino a 256 caratteri, lo spazio di visualizzazione nell'hub della risorsa è limitato. Assicurati che la parte distintiva del nome venga visualizzata nei primi 20-30 caratteri, se possibile.

- Tag delle risorse

  I tag sono coppie chiave-valore (metadati) che possono essere collegati alle risorse AWS. È possibile scegliere sia le chiavi tag che i relativi valori.

  A gateway, destinazioni e profili possono essere collegati fino a 50 tag. I dispositivi non supportano i tag.

Nomi delle risorse e descrizione

Supporto di risorse AWS IoT Wireless per nome

Risorsa	Supporto del campo nome
Destinazione	Il nome è un ID univoco della risorsa e non può essere modificato.
Dispositivo wireless	Il nome è un descrittore facoltativo della risorsa e può essere modificato.
Gateway LoRaWAN	Il nome è un descrittore facoltativo della risorsa e può essere modificato.

Risorsa	Supporto del campo nome	
Profilo	Il nome è un descrittore facoltativo della risorsa e può essere modificato.	

Il campo nome viene visualizzato negli elenchi di hub di risorse delle risorse; tuttavia, lo spazio è limitato e quindi potrebbero essere visibili solo i primi 15-30 caratteri del nome. Quando selezioni i nomi per le tue risorse, considera come vuoi che identifichino le risorse e come verranno visualizzate nella console.

Descrizione

Le risorse di destinazione, dispositivo e gateway supportano anche un campo di descrizione, che può accettare fino a 2.048 caratteri. Il campo descrizione viene visualizzato solo nella pagina dettagli della singola risorsa. Anche se il campo della descrizione può contenere molte informazioni, poiché viene visualizzato solo nella pagina dettagli della risorsa, non è conveniente eseguire la scansione nel contesto di più risorse.

Tag delle risorse

Supporto di risorse AWS IoT Wireless per i tag AWS

Risorsa	Supporto dei tag AWS	
Destinazione	È possibile aggiungere fino a 50 tag AWS alla risorsa.	
Dispositivo wireless	Questa risorsa non supporta tag AWS.	
Gateway LoRaWAN	È possibile aggiungere fino a 50 tag AWS alla risorsa.	
Profilo	È possibile aggiungere fino a 50 tag AWS alla risorsa.	

I tag sono parole o frasi che fungono da metadati e che puoi utilizzare per identificare e organizzare le risorse dei servizi AWS. È possibile considerare la chiave del tag come una categoria di informazioni e il valore del tag come un valore specifico in quella categoria. Ad esempio, si potrebbe avere un valore di tag pari a colore e poi dare ad alcune risorse un valore di blu per quel tag e ad altre un valore di rosso. Con questo, potresti usare l'Editor di tag nella console AWS per trovare le risorse con un tag colore del valore di blu.

Per ulteriori informazioni sull'assegnazione di tag in AWS IoT Wireless, consulta Tagging delle risorse AWS IoT Wireless.

Per ulteriori informazioni sulle strategie di tagging, consulta Editor di tag.

AWS IoT Core per LoRaWAN

AWS IoT Core per LoRaWAN è un server di rete LoRaWAN (LNS) completamente gestito che fornisce la gestione del gateway utilizzando le funzionalità CUPS (Configuration and Update Server) e FUOTA (Firmware Updates Over-The-Air). Puoi sostituire il tuo LNS privato con AWS IoT Core per LoRaWAN e connettere i tuoi dispositivi e i gateway LoRaWAN (Long Range Wide Area Network) a AWS IoT Core. In questo modo, si riducono la manutenzione, i costi operativi, i tempi di configurazione e i costi generali.

> **Note**
>
> AWS IoT Core per LoRaWAN supporta solo il formato di indirizzo IPv4. Non supporta IPv6 o la configurazione dual-stack (IPv4 e IPv6). Per ulteriori informazioni, consulta i Servizio AWS che supportano IPv6.

Introduzione

I dispositivi LoRaWAN sono dispositivi a batteria a lungo raggio e a bassa potenza che utilizzano il protocollo LoRaWAN per funzionare in uno spettro radio senza licenza. LoRaWAN è un protocollo di comunicazione LPWAN (Low Power Wide Area Network) basato su LoRa. LoRa è il protocollo a livello fisico che abilita la comunicazione a bassa potenza e ampia area tra i dispositivi.

Per collegare i tuoi dispositivi LoRaWAN a AWS IoT, è necessario utilizzare un gateway LoRaWAN. Il gateway funge da ponte per collegare il tuo dispositivo a AWS IoT Core per LoRaWAN e per scambiare messaggi. AWS IoT Core per LoRaWAN utilizza il motore di regole AWS IoT per instradare i messaggi dai dispositivi LoRaWAN ad altri servizi AWS IoT.

Per ridurre lo sforzo di sviluppo e installare rapidamente i dispositivi in AWS IoT Core per LoRaWAN, consigliamo di utilizzare dispositivi finali certificati LoRaWAN. Per ulteriori informazioni, consultare la pagina Panoramica del prodotto AWS IoT Core per LoRaWAN. Per informazioni su come ottenere la certificazione LoRaWAN dei dispositivi, consulta Certificazione dei prodotti LoRaWAN.

Accesso a AWS IoT Core per LoRaWAN

È possibile integrare rapidamente i dispositivi e i gateway LoRaWAN in AWS IoT Core per LoRaWAN utilizzando la console o l'API AWS IoT Wireless.

Utilizzo della console

Per integrare i dispositivi e i gateway LoRaWAN utilizzando la AWS Management Console, accedi alla AWS Management Console e vai alla pagina AWS IoT Core per LoRaWAN per LoRaWAN nella console AWS IoT. Puoi quindi utilizzare la sezione Introduzione per aggiungere gateway e dispositivi a AWS IoT Core per LoRaWAN. Per ulteriori informazioni, consultare Utilizzo della console per integrare il dispositivo e il gateway per AWS IoT Core per LoRaWAN.

Utilizzo dell'API o dell'interfaccia a riga di comando

È possibile integrare sia dispositivi LoRaWAN che dispositivi Sidewalk utilizzando l'API AWS IoT Wireless. L'API AWS IoT Wireless su cui si basa AWS IoT Core per LoRaWAN è supportata dall'SDK AWS. Per ulteriori informazioni, consulta AWS SDK e kit di strumenti.

Puoi utilizzare la AWS CLI per eseguire comandi per l'integrazione e la gestione dei gateway e dei dispositivi LoRaWAN. Per ulteriori informazioni, consulta la documentazione di riferimento dell'interfaccia della riga di comando AWS IoT Wireless.

Regioni ed endpoint AWS IoT Core per LoRaWAN

AWS IoT Core per LoRaWAN fornisce supporto per gli endpoint API del piano di controllo e del piano dati specifici per la tua Regione AWS. Gli endpoint API del piano dati sono specifici per il tuo Account AWS e la tua Regione AWS. Per ulteriori informazioni sugli endpoint AWS IoT Core per LoRaWAN, consulta la pagina relativa agli Endpoint AWS IoT Core per LoRaWAN nelle Informazioni di riferimento generali su AWS.

Per una comunicazione più sicura tra i tuoi dispositivi e AWS IoT, puoi collegare i tuoi dispositivi a AWS IoT Core per LoRaWAN attraverso AWS PrivateLink nel tuo Virtual Private Cloud (VPC) invece che tramite Internet pubblico. Per ulteriori informazioni, consultare AWS IoT Core per LoRaWAN ed endpoint VPC dell'interfaccia (AWS PrivateLink).

AWS IoT Core per LoRaWAN ha quote applicabili ai dati del dispositivo che vengono trasmessi tra i dispositivi e il TPS massimo per le operazioni API AWS IoT Wireless. Per ulteriori informazioni, consultare AWS IoT Core per LoRaWAN quotas in Riferimenti generali di AWS.

Prezzi di AWS IoT Core per LoRaWAN

Se sei un nuovo cliente, la registrazione ad AWS, puoi iniziare a utilizzare AWS IoT Core per LoRaWAN gratuitamente tramite il piano gratuito AWS. Con AWS IoT Core per LoRaWAN, si pagano

solo i servizi usati. Per ulteriori informazioni sulla panoramica generale del prodotto e sui prezzi, consulta prezzi di AWS IoT Core.

Cos'è AWS IoT Core per LoRaWAN?

AWS IoT Core per LoRaWAN sostituisce un server di rete LoRaWAN privato (LNS) collegando i tuoi dispositivi e i gateway LoRaWAN a AWS. Tramite il motore di regole AWS IoT, puoi instradare messaggi ricevuti dai dispositivi LoRaWAN dove possono essere formattati e inviati ad altri servizi AWS IoT. Per le comunicazioni sicure dei dispositivi con AWS IoT, AWS IoT Core per LoRaWAN utilizza i certificati X.509.

AWS IoT Core per LoRaWAN gestisce le policy dei servizi e dei dispositivi di cui AWS IoT Core richiede la comunicazione con i gateway e i dispositivi LoRaWAN. AWS IoT Core per LoRaWAN gestisce anche le destinazioni che descrivono le regole AWS IoT che inviano i dati del dispositivo ad altri servizi.

Caratteristiche di AWS IoT Core per LoRaWAN

Con il AWS IoT Core per LoRaWAN puoi:

- Integrare e connettere dispositivi e gateway LoRaWAN a AWS IoT senza dover configurare e gestire un LNS privato.
- Connettere dispositivi LoRaWAN conformi alle specifiche 1.0.x o 1.1 LoRaWAN standardizzate da LoRa Alliance. Questi dispositivi possono funzionare in modalità classe A, classe B o classe C.
- Utilizzare i gateway LoRaWAN che supportano LoRaWAN Basics Station versione 2.0.4 o successive. Tutti i gateway qualificati per AWS IoT Core per LoRaWAN utilizzano una versione compatibile di LoRa Basics Station.
- Connetti i dispositivi LoRaWAN al cloud utilizzando reti LoRaWAN disponibili pubblicamente, con conseguente riduzione dei tempi di implementazione e della necessità di gestire una rete LoRaWAN privata, con conseguente risparmio di tempo e costi.
- Monitora la potenza del segnale, la larghezza di banda e il fattore di diffusione utilizzando la velocità di dati adattiva di AWS IoT Core per LoRaWAN e ottimizza la velocità dati se necessario. Puoi anche utilizzare l'analizzatore di rete per monitorare le risorse in tempo reale.
- Aggiorna il firmware dei gateway LoRaWAN utilizzando il servizio CUPS e il firmware dei dispositivi LoRaWAN utilizzando Firmware Updates Over-The-Air (FUOTA).

I seguenti argomenti forniranno ulteriori informazioni sulla tecnologia LoRaWAN e AWS IoT Core per LoRaWAN.

Argomenti

Che cos'è LoRaWAN?

La LoRa Alliance descrive LoRaWan come “un protocollo di rete LPWA (Low Power, Wide Area) progettato per connettere in modalità wireless ‘oggetti’ alimentati a batteria a Internet nelle reti regionali, nazionali o globali e si rivolge ai requisiti chiave dell'Internet of Things (IoT) come la comunicazione bidirezionale, la sicurezza end-to-end, la mobilità e i servizi di localizzazione.".

LoRa e LoRaWAN

Il protocollo LoRaWAN è un protocollo di comunicazione Low Power Wide Area Networking (LPWAN) che funziona su LoRa.

LoRaWAN è stato riconosciuto come standard internazionale per LPWAN. Per ulteriori informazioni, vedere LoRaWAN formalmente riconosciuto come standard internazionale ITU. La specifica LoRaWAN è aperta in modo che chiunque possa configurare e gestire una rete LoRa.

LoRa è una tecnologia di frequenza audio wireless che opera in uno spettro di radiofrequenze senza licenza. LoRa è un protocollo di livello fisico che utilizza la modulazione di spettro diffuso e supporta la comunicazione a lungo raggio al costo di una larghezza di banda ridotta. Utilizza una forma d'onda a banda stretta con una frequenza centrale per inviare dati in modo da essere robusto alle interferenze.

Caratteristiche della tecnologia LoRaWAN

- Comunicazione a lungo raggio fino a 10 miglia in linea di vista.
- Lunga durata della batteria, fino a 10 anni. Per una maggiore durata della batteria, è possibile utilizzare i dispositivi in modalità Classe A o Classe B, che richiedono una maggiore latenza downlink.
- Basso costo per dispositivi e manutenzione.
- Spettro radio senza licenza ma si applicano normative specifiche per regione.

- Bassa potenza ma una dimensione di payload limitata da 51 byte a 241 byte, a seconda della velocità dati. La velocità dati può essere di 0,3 Kbit/s — 27 Kbit/s con una dimensione massima di payload di 222.

Versioni del protocollo LoRaWAN

LoRa Alliance specifica il protocollo LoRaWAN utilizzando i documenti delle specifiche LoRaWAN. Per tenere conto delle normative specifiche della regione, LoRa Alliance pubblica anche documenti sui parametri regionali. Per ulteriori informazioni, consultare Parametri e specifiche regionali LoRaWAN.

La versione iniziale di LoRaWAN è la 1.0. Le versioni aggiuntive rilasciate sono 1.0.1, 1.0.2, 1.0.3, 1.0.4 e 1.1. Le versioni 1.0.1-1.0.4 sono comunemente denominate 1.0.x.

Ulteriori informazioni su LoRaWAN

I seguenti link contengono informazioni utili sulla tecnologia LoRaWAN e sulla LoRa Basics Station, il software che viene eseguito sui gateway LoRaWAN per il collegamento di dispositivi finali ad AWS IoT Core per LoRaWAN.

- LoRaWAN è riconosciuto come standard internazionale ITU

  LoRaWAN è stato formalmente documentato come standard internazionale dall'ITU per le reti LPWAN. Lo standard è intitolato Raccomandazione ITU-T Y.4480 "Protocollo a bassa potenza per reti wireless WAN".
- I fondamenti degli oggetti su LoRaWAN

  Things Fundamentals on LoRaWAN contiene un video introduttivo che tratta i fondamenti di LoRaWAN e una serie di capitoli che ti aiuteranno a conoscere LoRa e LoRaWAN.
- Che cos'è LoRaWAN

  LoRa Alliance fornisce una panoramica tecnica di LoRa e LoRaWAN, incluso un riepilogo delle specifiche LoRaWAN in diverse regioni.
- LoRa Basics Station

  Semtech Corporation fornisce concetti utili su LoRa basics per gateway e nodi finali. LoRa Basics Station, un software open source che viene eseguito sul gateway LoRaWAN, viene gestito e distribuito tramite la repository GitHub della Semtech Corporation. È inoltre possibile conoscere i

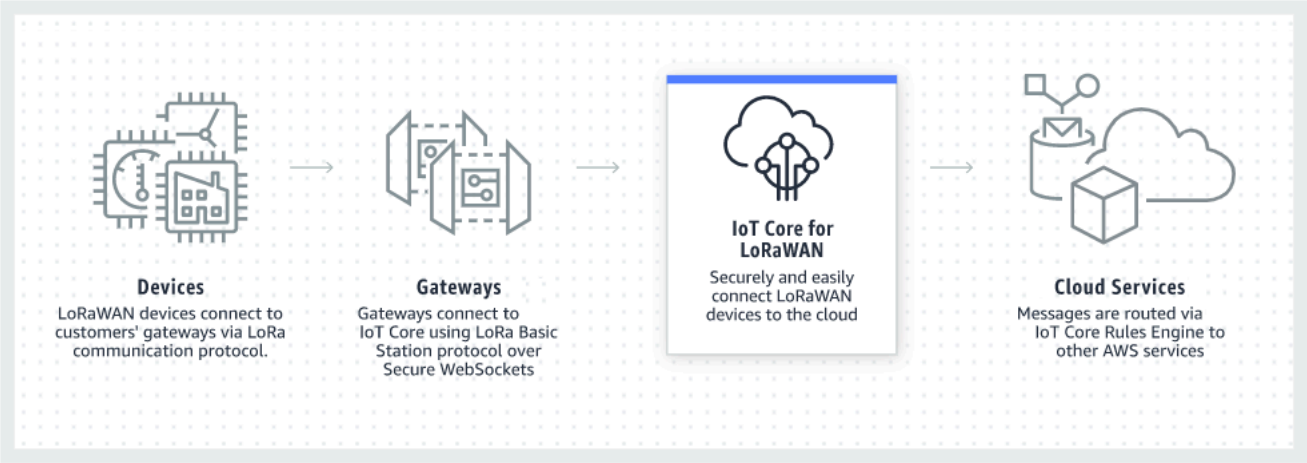
protocolli LNS e CUPS che descrivono come scambiare dati LoRaWAN ed eseguire aggiornamenti di configurazione.

- Parametri e specifiche regionali LoRaWAN

  Il documento RP002-1.0.2 include il supporto per tutte le versioni della specifica LoRaWAN Layer 2. Include informazioni sulle specifiche LoRaWAN e sui parametri regionali e sulle diverse versioni di LoRaWAN.

Funzionamento di AWS IoT Core per LoRaWAN

L'architettura di rete LoRaWAN è distribuita in una topologia a stella di stelle in cui i gateway trasmettono informazioni tra i dispositivi finali e il server di rete LoRaWAN (LNS). Di seguito viene illustrato come un dispositivo LoRaWAN interagisce con AWS IoT Core per LoRaWAN. Mostra inoltre come AWS IoT Core per LoRaWAN sostituisce un LNS e comunica con altri Servizio AWS in Cloud AWS.



I dispositivi LoRaWAN comunicano con AWS IoT Core attraverso i gateway LoRaWAN. AWS IoT Core per LoRaWAN gestisce le policy dei servizi e dei dispositivi di cui AWS IoT Core richiede la gestione e la comunicazione con i gateway e i dispositivi. AWS IoT Core per LoRaWAN gestisce anche le destinazioni che descrivono le regole AWS IoT che inviano i dati del dispositivo ad altri servizi.

Nozioni di base sull'utilizzo di AWS IoT Core per LoRaWAN

I passaggi seguenti mostrano una panoramica di come iniziare a utilizzare AWS IoT Core per LoRaWAN.

1. Seleziona i dispositivi wireless e i gateway LoRaWAN di cui avrai bisogno.

Il Catalogo dei dispositivi dei partner AWS contiene gateway e kit di sviluppo qualificati per l'utilizzo con AWS IoT Core per LoRaWAN. Per ulteriori informazioni, consultare Utilizzo di gateway qualificati dal Catalogo dei dispositivi dei partner di AWS.

2. Aggiungi i tuoi dispositivi wireless e i gateway LoRaWAN a AWS IoT Core per LoRaWAN.

   Collegamento di gateway e dispositivi ad AWS IoT Core per LoRaWAN fornisce informazioni su come descrivere le risorse e aggiungere i dispositivi wireless e i gateway LoRaWAN ad AWS IoT Core per LoRaWAN. Inoltre imparerai a configurare le altre risorse AWS IoT Core per LoRaWAN di cui avrai bisogno per gestire questi dispositivi e inviare i loro dati ai servizi AWS.

3. Completa la tua soluzione AWS IoT Core per LoRaWAN.

   Inizia con il nostro esempio di soluzione AWS IoT Core per LoRaWAN e rendilo tuo.

Risorse AWS IoT Core per LoRaWAN

Le risorse seguenti ti forniranno maggiori informazioni su AWS IoT Core per LoRaWAN e su come iniziare.

- Nozioni di base su AWS IoT Core per LoRaWAN

  Il seguente video descrive come lavora AWS IoT Core per LoRaWAN e ti guiderà attraverso il processo di aggiunta di gateway LoRaWAN dalla AWS Management Console.

- Workshop AWS IoT Core per LoRaWAN

  Il workshop tratta i fondamenti della tecnologia LoRaWAN e la sua implementazione con AWS IoT Core per LoRaWAN. È inoltre possibile utilizzare il workshop per visitare laboratori che mostrano come collegare il gateway e il dispositivo ad AWS IoT Core per LoRaWAN per la creazione di una soluzione IoT di esempio.

- Implementazione di soluzioni LPWAN (Low-Power Wide-Area Network) con AWS IoT

  Questo documento fornisce un quadro decisionale per aiutare a decidere se LPWAN è la scelta giusta per il vostro caso d'uso IoT, fornisce una panoramica delle tecnologie di connettività LPWAN e delle relative funzionalità e fornisce linee guida per l'implementazione.

Collegamento di gateway e dispositivi ad AWS IoT Core per LoRaWAN

AWS IoT Core per LoRaWAN ti aiuta a connettere e gestire dispositivi wireless LoRaWAN (Low Power Long Range Wide Area Network) e sostituisce la necessità di sviluppare e utilizzare un LNS. I dispositivi e i gateway WAN a lungo raggio (LoRaWAN) possono connettersi ad AWS IoT Core utilizzando AWS IoT Core per LoRaWAN.

Convenzioni di denominazione per dispositivi, gateway, profili e destinazioni

Prima di iniziare a utilizzare AWS IoT Core per LoRaWAN e creare le risorse, considera la convenzione di denominazione dei tuoi dispositivi, gateway e destinazione.

AWS IoT Core per LoRaWAN assegna ID univoci alle risorse create per dispositivi wireless, gateway e profili; tuttavia, è anche possibile assegnare alle risorse nomi più descrittivi per facilitarne l'identificazione. Prima di aggiungere dispositivi, gateway, profili e destinazioni ad AWS IoT Core per LoRaWAN, considera come nominarli per renderli più facili da gestire.

È possibile aggiungere i tag alle risorse create. Prima di aggiungere i tuoi dispositivi LoRaWAN, considera come utilizzare i tag per identificare e gestire le tue risorse AWS IoT Core per LoRaWAN. I tag possono essere modificati dopo averli aggiunti.

Per ulteriori informazioni su denominazione e l'assegnazione di tag, consulta Descrizione delle risorse AWS IoT Wireless.

Mappatura dei dati del dispositivo ai dati del servizio

I dati dei dispositivi wireless LoRaWAN sono spesso codificati per ottimizzare la larghezza di banda. Questi messaggi codificati arrivano ad AWS IoT Core per LoRaWAN in un formato che potrebbe non essere facilmente utilizzato da altri servizi AWS. AWS IoT Core per LoRaWAN utilizza regole AWS IoT che possono utilizzare funzioni AWS Lambda per elaborare e decodificare i messaggi del dispositivo in un formato che altri servizi AWS possono utilizzare.

Per trasformare i dati del dispositivo e inviarli ad altri servizi AWS, devi sapere:

- Il formato e il contenuto dei dati inviati dai dispositivi wireless.
- Il servizio a cui inviare i dati.
- Il formato richiesto dal servizio.

Utilizzando tali informazioni, è possibile creare la regola AWS IoT che esegue la conversione e invia i dati convertiti ai servizi AWS che lo utilizzeranno.

Utilizzo della console per integrare il dispositivo e il gateway per AWS IoT Core per LoRaWAN

Puoi utilizzare l'interfaccia della console o l'API per aggiungere il gateway e i dispositivi LoRaWAN. Se utilizzi AWS IoT Core per LoRaWAN per la prima volta, consigliamo di utilizzare la console. L'interfaccia della console è più pratica quando si gestiscono alcune risorse AWS IoT Core per LoRaWAN alla volta. Quando si gestiscono un numero elevato di risorse AWS IoT Core per LoRaWAN, prendi in considerazione la creazione di soluzioni più automatizzate utilizzando l'API AWS IoT Wireless .

Gran parte dei dati immessi durante la configurazione delle risorse AWS IoT Core per LoRaWAN sono forniti dai fornitori dei dispositivi e sono specifici per le specifiche LoRaWAN che supportano. I seguenti argomenti descrivono in che modo puoi descrivere le risorse AWS IoT Core per LoRaWAN e usare la console o l'API per aggiungere gateway e dispositivi.

> **Note**
>
> Se utilizzi una rete pubblica per connettere i tuoi dispositivi LoRaWAN al cloud, puoi saltare l'onboarding dei tuoi gateway. Per ulteriori informazioni, consultare Gestione del traffico LoRaWAN da reti di dispositivi LoRaWAN pubbliche (Everynet).

Argomenti

- Integrare i gateway per AWS IoT Core per LoRaWAN
- Integra i tuoi dispositivi su AWS IoT Core per LoRaWAN

Integrare i gateway per AWS IoT Core per LoRaWAN

Se utilizzi AWS IoT Core per LoRaWAN per la prima volta, puoi aggiungere il primo gateway e il dispositivo LoRaWAN utilizzando la console.

> **Note**
>
> Se utilizzi una rete pubblica per connettere i tuoi dispositivi LoRaWAN al cloud, puoi saltare l'onboarding dei tuoi gateway. Per ulteriori informazioni, consultare Gestione del traffico LoRaWAN da reti di dispositivi LoRaWAN pubbliche (Everynet).

Prima di effettuare l'onboarding del gateway

Prima di effettuare l'onboarding del gateway su AWS IoT Core per LoRaWAN, ti consigliamo di:

- Utilizzare gateway qualificati per l'utilizzo con AWS IoT Core per LoRaWAN. Questi gateway si connettono ad AWS IoT Core senza ulteriori impostazioni di configurazione e dispongono di una versione 2.0.4 o successiva compatibile con il software LoRa Basics Station in esecuzione su di essi. Per ulteriori informazioni, consultare Gestione dei gateway con AWS IoT Wireless.
- Considera la convenzione di denominazione delle risorse create in modo da poterle gestire più facilmente. Per ulteriori informazioni, consultare Descrizione delle risorse AWS IoT Wireless.
- I parametri di configurazione univoci di ciascun gateway sono pronti per essere inseriti in anticipo, così da rendere più agevole l'immissione dei dati nella console. I parametri di configurazione del gateway wireless con cui AWS IoT richiede di comunicare e gestire il gateway includono l'EUI del gateway e la sua banda di frequenza LoRa.

Per l'onboarding dei gateway su AWS IoT Core per LoRaWAN:

- Considera la selezione della banda di frequenza e aggiungi il ruolo IAM necessario
- Aggiungi un gateway a AWS IoT Core per LoRaWAN
- Connetti il tuo gateway LoRaWAN e verifica lo stato della connessione

Considera la selezione della banda di frequenza e aggiungi il ruolo IAM necessario

Prima di aggiungere il gateway ad AWS IoT Core per LoRaWAN, si consiglia di considerare la banda di frequenza in cui il gateway sarà operativo e di aggiungere il ruolo IAM necessario per connettere il gateway ad AWS IoT Core per LoRaWAN.

> **Note**
>
> Se stai aggiungendo il gateway tramite la console, fai clic su Create role (Crea ruolo) nella console per creare il ruolo IAM necessario, in modo da poter saltare questi passaggi. È necessario eseguire questi passaggi solo se si utilizza la CLI per creare il gateway.

Considerate la selezione delle bande di frequenza LoRa per i gateway e la connessione del dispositivo

AWS IoT Core per LoRaWAN supporta le bande di frequenza EU863-870, US902-928, AU915 e AS923-1 che è possibile utilizzare per collegare gateway e dispositivi fisicamente presenti in paesi che supportano le gamme di frequenza e le caratteristiche di queste bande. Le bande EU863-870 e US902-928 sono comunemente utilizzate rispettivamente in Europa e Nord America. La banda AS923-1 è comunemente usata in Australia, Nuova Zelanda, Giappone e Singapore, tra gli altri paesi. L'AU915 è utilizzato in Australia e Argentina, tra gli altri paesi. Per ulteriori informazioni sulla banda di frequenza da utilizzare nella propria area geografica o nel proprio paese, consulta Parametri regionali LoRaWAN®.

LoRa Alliance pubblica le specifiche di LoRaWAN e i documenti sui parametri regionali disponibili per il download dal sito web LoRa Alliance. I parametri regionali LoRa Alliance aiutano le aziende a decidere quale banda di frequenza utilizzare nella loro regione o paese. L'implementazione della banda di frequenza di AWS IoT Core per LoRaWAN segue il suggerimento contenuto nel documento di specifica dei parametri regionali. Questi parametri regionali sono raggruppati in una serie di parametri radio, insieme a un'allocazione di frequenza adattata alla banda Industriale, Scientifica e Medica (ISM). Ti consigliamo di collaborare con i team di conformità per assicurarti di soddisfare i requisiti normativi applicabili.

Aggiungi un ruolo IAM per permettere a Configuration and Update Server (CUPS) di gestire le credenziali del gateway

Questa procedura descrive come aggiungere un ruolo IAM per permettere a Configuration and Update Server (CUPS) di gestire le credenziali del gateway. Assicurati di eseguire questa procedura prima che un gateway LoRaWAN tenti di connettersi con AWS IoT Core per LoRaWAN; tuttavia, è necessario eseguire questa operazione una sola volta.

Aggiungi il ruolo IAM per permettere a Configuration and Update Server (CUPS) di gestire le credenziali del gateway

1. Apri Roles hub of the IAM console (Ruoli hub della console IAM) e scegli Create role (Crea ruolo).
2. Se ritieni di aver già aggiunto il ruolo IoTWirelessGatewayCertManagerRole, inserisci **`IoTWirelessGatewayCertManagerRole`** nella barra di ricerca.

   Se viene visualizzato un ruolo IoTWirelessGatewayCertManagerRole nei risultati della ricerca, disponi del ruolo IAM necessario. Ora puoi lasciare la procedura.

   Se i risultati della ricerca sono vuoti, non disponi del ruolo IAM necessario. Continua la procedura per aggiungerlo.
3. In Seleziona tipo di entità attendibile, scegli Altro Account AWS.
4. In Account ID (Account ID), inserisci il tuo account Account AWS ID, quindi scegli Next: Permissions (Successivo: Autorizzazioni).
5. Nella casella di ricerca immetti **`AWSIoTWirelessGatewayCertManager`**.
6. Nell'elenco dei risultati della ricerca, seleziona la policy denominata AWSIoTWirelessGatewayCertManager.
7. Scegli Successivo: Tag, quindi Successivo: Rivedi.
8. In Role name (Nome ruolo) inserisci **`IoTWirelessGatewayCertManagerRole`** e quindi scegli Create role (Crea ruolo).
9. Per modificare il nuovo ruolo, nel messaggio di conferma, scegli IoTWirelessGatewayCertManagerRole.
10. In Summary (Riepilogo), scegli Trust relationships (Relazioni di trust) e scegli Edit trust relationship (Modifica relazione di trust).
11. In Policy Document (Documento policy), modifica la proprietà di `Principal` affinché appaia come nell'esempio.

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

    Dopo aver modificato la proprietà `Principal`, il documento completo di policy dovrebbe essere simile al seguente.

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

12. Per salvare le modifiche, scegli Update Trust Policy (Aggiorna policy di attendibilità).

Ora è stato creato il IoTWirelessGatewayCertManagerRole. Non dovrai farlo di nuovo.

Se è stata eseguita questa procedura mentre si aggiungeva un gateway, puoi chiudere questa finestra e la console IAM e tornare alla console AWS IoT per completare l'aggiunta del gateway.

Aggiungi un gateway a AWS IoT Core per LoRaWAN

È possibile aggiungere il gateway ad AWS IoT Core per LoRaWAN utilizzando la console o la CLI.

Prima di aggiungere il gateway, ti consigliamo di considerare i fattori menzionati in Prima di eseguire l'onboarding del gateway, nella sezione di Integrare i gateway per AWS IoT Core per LoRaWAN.

Se utilizzi il tuo gateway per la prima volta, consigliamo di utilizzare la console. Se desideri aggiungere il gateway utilizzando il CLI, devi aver già creato il ruolo IAM necessario in modo che il gateway possa connettersi con AWS IoT Core per LoRaWAN. Per informazioni su come creare il ruolo, consulta Aggiungi un ruolo IAM per permettere a Configuration and Update Server (CUPS) di gestire le credenziali del gateway.

Aggiungere un gateway utilizzando la console

Vai alla pagina Intro AWS IoT Core per LoRaWAN della console AWS IoT e scegli Get started (Nozioni di base), poi scegli Add gateway (Aggiungi gateway). Se hai già aggiunto un gateway, scegli View gateway (Visualizza gateway) per visualizzare il gateway aggiunto. Se desideri aggiungere altri gateway, scegli Add gateway (Aggiungi gateway).

1. Fornisci dettagli sul gateway e informazioni sulla banda di frequenza

   Utilizza Gateway details (Dettagli gateway) per fornire informazioni sui dati di configurazione del dispositivo, ad esempio l'EUI del gateway e la configurazione della banda di frequenza.

   - EUI del Gateway

     L'EUI (Extended Unique Identifier) del singolo dispositivo di gateway. L'EUI è un codice alfanumerico a 16 cifre, come `c0ee40ffff29df10`, che identifica in modo univoco un gateway nella tua rete LoRaWAN. Queste informazioni sono specifiche per il tuo modello gateway e puoi trovarle sul tuo dispositivo gateway o nel relativo manuale utente.

     > **Note**
     >
     > L'EUI del gateway è diverso dall'indirizzo MAC Wi-Fi che potresti vedere stampato sul tuo dispositivo gateway. L'EUI segue uno standard EUI-64 che identifica in modo univoco il gateway e quindi non può essere ripreso in altre regioni e account Account AWS.

   - Banda di frequenza (RFRegion)

     La banda di frequenza del gateway. Puoi scegliere tra `US915`, `EU868`, `AU915` oppure `AS923-1`, a seconda del tipo di supporto del gateway e del paese da cui il gateway si connette fisicamente. Per ulteriori informazioni sulle bande, consulta Considerate la selezione delle bande di frequenza LoRa per i gateway e la connessione del dispositivo.

2. Specificare i dati di configurazione del gateway wireless (opzionale)

   Questi campi sono facoltativi ed è possibile utilizzarli per fornire ulteriori informazioni sul gateway e sulla sua configurazione.

   - Nome, Descrizione e Tag per il gateway

     Le informazioni contenute in questi campi facoltativi provengono da come organizzi e descrivi gli elementi del sistema wireless. Puoi assegnare un Nome al gateway, utilizzare il comando Description (Descrizione) per fornire informazioni sul gateway e utilizzare Tag per aggiungere coppie chiave-valore di metadati sul gateway. Per ulteriori informazioni sulla denominazione e sulla descrizione delle risorse, consulta Descrizione delle risorse AWS IoT Wireless.

   - Configurazione LoRaWAN con sottobande e filtri

Facoltativamente, è inoltre possibile specificare i dati di configurazione di LoRaWAN, ad esempio le sottobande che si desidera utilizzare e i filtri in grado di controllare il flusso di traffico. Per questo tutorial, è possibile saltare questi campi. Per ulteriori informazioni, consultare Configurare le sottobande e le funzionalità di filtraggio del gateway.

3. Associa un oggetto AWS IoT con il gateway

   Specifica se creare un oggetto AWS IoT e associarlo al gateway. Gli oggetti in AWS IoT possono semplificare la ricerca e la gestione dei dispositivi. L'associazione di un oggetto al gateway consente al gateway di accedere ad altre caratteristiche di AWS IoT Core.

4. Crea e scarica il certificato gateway

   Per autenticare il gateway in modo che possa comunicare in modo sicuro con AWS IoT, il gateway LoRaWAN deve presentare ad AWS IoT Core per LoRaWAN una chiave privata e un certificato. Creazione di un Certificato gateway in modo che AWS IoT possa verificare l'identità del gateway utilizzando lo standard X.509.

   Fai clic sul pulsante Create certificate (Crea un certificato) e scarica i file del certificato. Li userai in seguito per configurare il gateway.

5. Copia gli endpoint CUPS e LNS e scarica i certificati

   Il gateway LoRaWAN deve connettersi a un endpoint CUPS o LNS quando si stabilisce una connessione ad AWS IoT Core per LoRaWAN. Ti consigliamo di utilizzare l'endpoint CUPS in quanto fornisce anche la gestione della configurazione. Per verificare l'autenticità degli endpoint di AWS IoT Core per LoRaWAN, il gateway utilizzerà un certificato di attendibilità per ciascuno degli endpoint CUPS e LNS,

   Fai clic su Copy (Copia) per copiare gli endpoint CUPS e LNS. Queste informazioni serviranno in seguito per configurare il gateway. Quindi fai clic sul pulsante Download server trust certificates (Scarica certificati di attendibilità server) per scaricare i certificati di attendibilità per gli endpoint CUPS e LNS.

6. Crea il ruolo IAM per le autorizzazioni del gateway

   Aggiungi un ruolo IAM per permettere a Configuration and Update Server (CUPS) di gestire le credenziali del gateway.

> **Note**
>
> In questo passaggio, crei il ruolo IoTWirelessGatewayCertManager. Puoi ignorare questa fase se questo spazio dei nomi è già stato creato. È necessario farlo prima che un gateway LoRaWAN tenti di connettersi con AWS IoT Core per LoRaWAN; tuttavia, è necessario farlo solo una volta.

Per creare il ruolo IAM IoTWirelessGatewayCertManager per il tuo account, fai clic sul pulsante Create role (Crea ruolo). Se il ruolo esiste già, selezionalo dall'elenco a discesa.

Fai clic su Submit (Invia) per completare la creazione del gateway.

Aggiungi un gateway utilizzando l'API

Se si sta aggiungendo un gateway per la prima volta utilizzando l'API o la CLI, è necessario aggiungere il ruolo IAM IoTWirelessGatewayCertManager in modo che il gateway possa connettersi con AWS IoT Core per LoRaWAN. Per informazioni sulla creazione del ruolo, consulta la seguente sezione Aggiungi un ruolo IAM per permettere a Configuration and Update Server (CUPS) di gestire le credenziali del gateway.

Gli elenchi seguenti descrivono le operazioni API che eseguono le attività associate all'aggiunta, all'aggiornamento o all'eliminazione di un gateway LoRaWAN.

Operazioni dell'API AWS IoT Wireless per gateway AWS IoT Core per LoRaWAN

- CreateWirelessGateway
- GetWirelessGateway
- ListWirelessGateways
- UpdateWirelessGateway
- DeleteWirelessGatewa

Per l'elenco completo delle operazioni e dei tipi di dati disponibili per creare e gestire le risorse AWS IoT Core per LoRaWAN, consulta la documentazione di riferimento delle API AWS IoT Wireless

Come utilizzare AWS CLI per aggiungere un gateway

Puoi utilizzare AWS CLI per creare un gateway wireless utilizzando il comando create-wireless-gateway. Nell'esempio seguente viene creato un gateway per dispositivo LoRaWAN wireless. Puoi anche fornire un file `input.json` che conterrà ulteriori dettagli, ad esempio il certificato del gateway e le credenziali di provisioning.

> **Note**
>
> È inoltre possibile eseguire questa procedura con l'API utilizzando i metodi dell'API AWS corrispondenti ai comandi CLI illustrati di seguito.

```
aws iotwireless create-wireless-gateway \
    --lorawan GatewayEui="a1b2c3d4567890ab",RfRegion="US915" \
    --name "myFirstLoRaWANGateway" \
    --description "Using my first LoRaWAN gateway"
    --cli-input-json input.json
```

Per informazioni sulle CLI utilizzabili, consulta Riferimento AWS CLI

Connetti il tuo gateway LoRaWAN e verifica lo stato della connessione

Prima di controllare lo stato della connessione del gateway, è necessario aver già aggiunto il gateway e averlo connesso ad AWS IoT Core per LoRaWAN. Per informazioni su come aggiungere il gateway, consulta Aggiungi un gateway a AWS IoT Core per LoRaWAN.

Connetti il gateway a AWS IoT Core per LoRaWAN

Dopo aver aggiunto il gateway, connettiti all'interfaccia di configurazione del gateway per inserire le informazioni di configurazione e i certificati di attendibilità.

Dopo aver aggiunto le informazioni del gateway ad AWS IoT Core per LoRaWAN, aggiungi alcune informazioni di AWS IoT Core per LoRaWAN al dispositivo gateway. La documentazione fornita dal fornitore del gateway deve descrivere il processo per caricare i file di certificato nel gateway e configurare il dispositivo gateway per comunicare con AWS IoT Core per LoRaWAN.

Gateway qualificati per l'utilizzo con AWS IoT Core per LoRaWAN

Per istruzioni su come configurare il gateway LoRaWAN, consulta la sezione configure gateway device (configurare il dispositivo gateway) del workshop AWS IoT Core per LoRaWAN. Qui troverai

informazioni sulle istruzioni per la connessione di gateway qualificati per l'uso con AWS IoT Core per LoRaWAN.

Gateway che supportano il protocollo CUPS

Le istruzioni seguenti mostrano come collegare i gateway che supportano il protocollo CUPS.

1. Carica i seguenti file ottenuti durante l'aggiunta del gateway.
   - Certificato del dispositivo gateway e file di chiavi private.
   - File di certificato attendibile per l'endpoint CUPS `cups.trust`.
2. Specifica l'URL dell'endpoint CUPS ottenuto in precedenza. L'endpoint sarà del formato *`prefix`*`.cups.lorawan.`*`region`*`.amazonaws.com:443`.

Per i dettagli su come ottenere queste informazioni, consulta Aggiungi un gateway a AWS IoT Core per LoRaWAN.

Gateway che supportano il protocollo LNS

Le istruzioni seguenti mostrano come collegare i gateway che supportano il protocollo LNS.

1. Carica i seguenti file ottenuti durante l'aggiunta del gateway.
   - Certificato del dispositivo gateway e file di chiavi private.
   - File di certificato attendibile per l'endpoint LNS `lns.trust`.
2. Specifica l'URL dell'endpoint LNS ottenuto in precedenza. L'endpoint sarà del formato https://*`prefix`*`.lns.lorawan.`*`region`*`.amazonaws.com:443`.

Per i dettagli su come ottenere queste informazioni, consulta Aggiungi un gateway a AWS IoT Core per LoRaWAN.

Dopo aver collegato il gateway ad AWS IoT Core per LoRaWAN, puoi controllare lo stato della tua connessione e ottenere informazioni su quando è stato ricevuto l'ultimo uplink utilizzando la console o l'API.

Controllare lo stato della connessione gateway utilizzando la console

Per verificare lo stato della connessione utilizzando la console, passa alla pagina Gateway della console AWS IoT e scegli il gateway aggiunto. Nella sezione LoRaWAN specific details (LoRaWAN dettagli specifici) della pagina dei dettagli del gateway, vedrai lo stato della connessione e la data e l'ora in cui è stato ricevuto l'ultimo uplink.

Controllare lo stato della connessione gateway utilizzando l'API

Per verificare lo stato della connessione utilizzando l'API, utilizza l'API `GetWirelessGatewayStatistics`. Questa API non ha un corpo della richiesta e contiene solo un corpo di risposta che mostra se il gateway è connesso e quando è stato ricevuto l'ultimo uplink.

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

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

Integra i tuoi dispositivi su AWS IoT Core per LoRaWAN

Dopo aver effettuato l'onboarding del gateway su AWS IoT Core per LoRaWAN e aver verificato il suo stato di connessione, è possibile caricare i dispositivi wireless. Per informazioni su come effettuare l'onboarding dei gateway, consulta Integrare i gateway per AWS IoT Core per LoRaWAN.

I dispositivi LoRaWAN utilizzano un protocollo LoRaWAN per scambiare dati con applicazioni ospitate nel cloud. AWS IoT Core per LoRaWAN supporta dispositivi conformi alle specifiche 1.0.x o 1.1 LoRaWAN standardizzate da LoRa Alliance.

Un dispositivo LoRaWAN contiene in genere uno o più sensori e attori. I dispositivi inviano dati di telemetria uplink attraverso i gateway LoRaWAN ad AWS IoT Core per LoRaWAN. Le applicazioni ospitate nel cloud possono controllare i sensori inviando comandi downlink ai dispositivi LoRaWAN tramite gateway LoRaWAN.

Prima di effettuare l'onboarding del dispositivo wireless

Prima di caricare il dispositivo wireless su AWS IoT Core per LoRaWAN, è necessario disporre di tutte le informazioni necessarie in anticipo:

- Specifiche LoRaWAN e configurazione del dispositivo wireless

  I parametri di configurazione univoci di ciascun dispositivo sono pronti per essere inseriti in anticipo, così da rendere più agevole l'immissione dei dati nella console. I parametri specifici che è necessario inserire dipendono dalla specifica LoRaWAN utilizzata dal dispositivo. Per l'elenco

completo delle specifiche e dei parametri di configurazione, vedi la documentazione di ciascun dispositivo.

- Nome e descrizione del dispositivo (facoltativo)

  Le informazioni contenute in questi campi facoltativi provengono da come organizzi e descrivi gli elementi del sistema wireless. Per ulteriori informazioni sulla denominazione e sulla descrizione delle risorse, consulta Descrizione delle risorse AWS IoT Wireless.

- Profili di dispositivo e di servizio

  Avere alcuni parametri di configurazione dei dispositivi wireless pronti, condivisi da molti dispositivi e che possono essere memorizzati in AWS IoT Core per LoRaWAN come profili di dispositivi e servizi. I parametri di configurazione sono disponibili nella documentazione del dispositivo o nel dispositivo. È necessario identificare un profilo del dispositivo che corrisponda ai parametri di configurazione del dispositivo o crearne uno, se necessario, prima di aggiungere il dispositivo. Per ulteriori informazioni, consultare Aggiungi profili a AWS IoT Core per LoRaWAN.

- Destinazione AWS IoT Core per LoRaWAN

  Ogni dispositivo deve essere assegnato a una destinazione che elaborerà i propri messaggi da inviare ad AWS IoT e altri servizi. Le regole AWS IoT che elaborano e inviano i messaggi del dispositivo sono specifiche del formato dei messaggi del dispositivo. Per elaborare i messaggi dal dispositivo e inviarli al servizio corretto, identifica la destinazione da utilizzare con i messaggi del dispositivo e assegnala al dispositivo.

Per caricare il dispositivo wireless su AWS IoT Core per LoRaWAN

- Aggiungi il dispositivo wireless ad AWS IoT Core per LoRaWAN
- Aggiungi profili a AWS IoT Core per LoRaWAN
- Aggiunta di destinazioni a AWS IoT Core per LoRaWAN
- Creare regole per elaborare i messaggi del dispositivo LoRaWAN
- Connetti il tuo dispositivo LoRaWAN e verifica lo stato della connessione

Aggiungi il dispositivo wireless ad AWS IoT Core per LoRaWAN

Se stai aggiungendo il dispositivo wireless per la prima volta, ti consigliamo di utilizzare la console. Naviga sulla pagina Intro AWS IoT Core per LoRaWAN della console AWS IoT, scegli Get started (Nozioni di base), quindi scegli Add device (Aggiungi dispositivo). Se hai già aggiunto un dispositivo,

scegli View device (Visualizza il dispositivo) per visualizzare il gateway aggiunto. Se desideri aggiungere altri dispositivi, scegli Add device (Aggiungi dispositivo).

In alternativa, puoi anche aggiungere dispositivi wireless dalla pagina Devices (Dispositivi) della console AWS IoT.

Aggiungi le specifiche del dispositivo wireless ad AWS IoT Core per LoRaWAN utilizzando la console

Scegli una Specificazione del dispositivo wireless in base al tuo metodo di attivazione e alla versione LoRaWAN. Una volta selezionati, i dati vengono crittografati con una chiave che AWS possiede e gestisce per te.

Modalità di attivazione OTAA e ABP

Prima che il tuo dispositivo LoRaWAN possa inviare dati uplink, devi completare un processo chiamato Attivazione o Procedura join. Per attivare il dispositivo, è possibile utilizzare OTAA (attivazione per via etere) o ABP (Attivazione per personalizzazione).

ABP non richiede una procedura di join e utilizza chiavi statiche. Quando si utilizza OTAA, il dispositivo LoRaWAN invia una richiesta di join e il server di rete può permettere la richiesta. Si consiglia di utilizzare OTAA per attivare il dispositivo in quanto vengono generate nuove chiavi di sessione per ogni attivazione così da renderlo più sicuro.

Versione di LoRaWAN

Quando utilizzi OTAA, il dispositivo LoRaWAN e le applicazioni ospitate nel cloud condividono le chiavi di root. Queste chiavi di root dipendono dal fatto che tu stia utilizzando la versione v1.0.x o v1.1. v1.0.x ha solo una chiave di root, AppKey (Chiave applicazione) mentre v1.1 ha due chiavi root, AppKey (Chiave applicazione) e NwkKey (Chiave di rete). Le chiavi di sessione sono derivate in base alle chiavi di root per ogni attivazione. Sia NwkKey che AppKey sono valori esadecimali a 32 cifre forniti dal fornitore wireless.

EUI del dispositivo wireless

Dopo aver selezionato l'opzione Wireless device specification (Specificazione del dispositivo wireless), vengono visualizzati i parametri EUI (Extended Unique Identifier) per il dispositivo wireless sulla console. Puoi trovare queste informazioni sulla documentazione relativa al dispositivo o al fornitore wireless.

- DevEUI: valore esadecimale a 16 cifre univoco per il dispositivo e trovato sull'etichetta del dispositivo o sulla relativa documentazione.

- AppEUI: valore esadecimale a 16 cifre univoco per il server di join e trovato nella documentazione del dispositivo. Nella versione v1.1 di LoRaWAN, AppEUI viene chiamato JoinEUI.

Per ulteriori informazioni sugli identificatori univoci, le chiavi di sessione e le chiavi root, fai riferimento alla documentazione della LoRa Alliance.

Aggiungere le specifiche del dispositivo wireless ad AWS IoT Core per LoRaWAN utilizzando l'API

Se stai aggiungendo un dispositivo wireless utilizzando l'API, prima di creare il dispositivo wireless devi creare il tuo profilo di servizio e dispositivo. Utilizzerai il profilo del dispositivo e l'ID profilo del servizio durante la creazione del dispositivo wireless. Per informazioni su come creare questi profili usando l'API, consulta Aggiungi un profilo del dispositivo utilizzando l'API.

Negli elenchi seguenti vengono descritte le operazioni API che eseguono le attività associate all'aggiunta, all'aggiornamento o all'eliminazione di un profilo di servizio.

Operazioni API AWS IoT Wireless per i profili di servizio

- CreateWirelessDevice
- GetWirelessDevice
- ListWirelessDevices
- UpdateWirelessDevice
- DeleteWirelessDevice

Per l'elenco completo delle operazioni e dei tipi di dati disponibili per creare e gestire le risorse AWS IoT Core per LoRaWAN, consulta la documentazione di riferimento delle API AWS IoT Wireless

Come utilizzare AWS CLI per creare un dispositivo wireless

Puoi utilizzare AWS CLI per creare un dispositivo wireless utilizzando il comando create-wireless-device. L'esempio seguente crea un dispositivo wireless utilizzando un file input.json per immettere i parametri.

> **Note**
>
> È inoltre possibile eseguire questa procedura con l'API utilizzando i metodi dell'API AWS corrispondenti ai comandi CLI illustrati di seguito.

Contenuto di 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
}
```

È possibile fornire questo file come input per il comando `create-wireless-device`.

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

Per informazioni sulle CLI utilizzabili, consulta Riferimento AWS CLI

Aggiungi profili a AWS IoT Core per LoRaWAN

È possibile definire profili di dispositivo e servizio per descrivere le configurazioni più comuni del dispositivo. Questi profili descrivono i parametri di configurazione condivisi dai dispositivi per semplificare l'aggiunta di tali dispositivi. AWS IoT Core per LoRaWAN supporta profili di dispositivi e profili di servizio.

I parametri di configurazione e i valori da inserire in questi profili sono forniti dal produttore del dispositivo.

Aggiungi profili di dispositivo

I profili del dispositivo definiscono le funzionalità del dispositivo e i parametri di avvio utilizzati dal server di rete per impostare il servizio di accesso radio LoRaWAN. Include la selezione di parametri come banda di frequenza LoRa, versione dei parametri regionali LoRa e versione MAC del

dispositivo. Per informazioni sulle diverse bande di frequenza, consulta Considerate la selezione delle bande di frequenza LoRa per i gateway e la connessione del dispositivo.

Aggiungi un profilo dispositivo utilizzando la console

Se si aggiunge un dispositivo wireless utilizzando la console come descritto in Aggiungi le specifiche del dispositivo wireless ad AWS IoT Core per LoRaWAN utilizzando la console, dopo aver aggiunto le specifiche del dispositivo wireless, è possibile aggiungere il profilo del dispositivo. In alternativa, puoi anche aggiungere dispositivi wireless dalla pagina Profiles (Profili) della console AWS IoT nella scheda LoRaWAN.

È possibile scegliere tra i profili dispositivo di default o creare un nuovo profilo dispositivo. Ti consigliamo di utilizzare i profili del dispositivo di default. Se l'applicazione richiede la creazione di un profilo di dispositivo, fornisci un Nome del profilo del dispositivo, seleziona la Banda di frequenza (RFRegion) che stai utilizzando per il dispositivo e il gateway e mantieni le altre impostazioni ai valori predefiniti, a meno che non sia specificato diversamente nella documentazione del dispositivo.

Aggiungi un profilo del dispositivo utilizzando l'API

Se stai aggiungendo un dispositivo wireless utilizzando l'API, prima di creare il dispositivo wireless devi creare il tuo profilo di dispositivo.

Negli elenchi seguenti vengono descritte le operazioni API che eseguono le attività associate all'aggiunta, all'aggiornamento o all'eliminazione di un profilo di servizio.

Operazioni API AWS IoT Wireless per i profili di servizio

- CreateDeviceProfile
- GetDeviceProfile
- ListDeviceProfiles
- UpdateDeviceProfile
- DeleteDeviceProfile

Per l'elenco completo delle operazioni e dei tipi di dati disponibili per creare e gestire le risorse AWS IoT Core per LoRaWAN, consulta la documentazione di riferimento delle API AWS IoT Wireless

Come utilizzare AWS CLI per creare un profilo di dispositivo

Puoi utilizzare AWS CLI per creare un profilo del dispositivo utilizzando il comando create-device profile. Nell'esempio seguente viene creato un profilo di dispositivo.

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

L'esecuzione di questo comando crea automaticamente un profilo di dispositivo con un ID che è possibile utilizzare durante la creazione del dispositivo wireless. Ora è possibile creare il profilo del servizio utilizzando la seguente API e quindi creare il dispositivo wireless utilizzando i profili del dispositivo e del servizio.

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

Per informazioni sulle CLI utilizzabili, consulta Riferimento AWS CLI

Aggiungi profili di servizio

I profili di servizio descrivono i parametri di comunicazione che il dispositivo deve comunicare con il server applicazioni.

Aggiunta di un profilo di servizio utilizzando la console

Se si aggiunge un dispositivo wireless utilizzando la console come descritto in Aggiungi le specifiche del dispositivo wireless ad AWS IoT Core per LoRaWAN utilizzando la console, dopo aver aggiunto il profilo del dispositivo, è possibile aggiungere il profilo del servizio. In alternativa, puoi anche aggiungere dispositivi wireless dalla pagina Profiles (Profili) della console AWS IoT nella scheda LoRaWAN.

Ti consigliamo di lasciare abilitata l'impostazione AddGWMetaData in modo da ricevere metadati gateway aggiuntivi per ogni payload, ad esempio RSSI e SNR per la trasmissione dei dati.

Aggiunta di un profilo di servizio utilizzando l'API

Se stai aggiungendo un dispositivo wireless utilizzando l'API, prima di creare il dispositivo wireless devi creare il tuo profilo di servizio.

Negli elenchi seguenti vengono descritte le operazioni API che eseguono le attività associate all'aggiunta, all'aggiornamento o all'eliminazione di un profilo di servizio.

Operazioni API AWS IoT Wireless per i profili di servizio

- CreateServiceProfile

- GetServiceProfile
- ListServiceProfiles
- UpdateServiceProfile
- DeleteServiceProfile

Per l'elenco completo delle operazioni e dei tipi di dati disponibili per creare e gestire le risorse AWS IoT Core per LoRaWAN, consulta la documentazione di riferimento delle API AWS IoT Wireless

Come utilizzare AWS CLI per creare un profilo di servizio

Puoi utilizzare AWS CLI per creare un servizio utilizzando il comando create-service-profile. Nell'esempio seguente viene creato un profilo di servizio.

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

L'esecuzione di questo comando crea automaticamente un profilo di dispositivo con un ID che è possibile utilizzare durante la creazione del dispositivo wireless. Ora è possibile creare il dispositivo wireless utilizzando il dispositivo e i profili di servizio.

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

Aggiunta di destinazioni a AWS IoT Core per LoRaWAN

Le destinazioni di AWS IoT Core per LoRaWAN descrivono la regola di AWS IoT che elabora i dati di un dispositivo per l'utilizzo dai servizi AWS.

Poiché la maggior parte dei dispositivi LoRaWAN non invia dati ad AWS IoT Core per LoRaWAN in un formato che può essere usato dai servizi AWS, una regola di AWS IoT deve prima elaborarli. La regola AWS IoT contiene l'istruzione SQL che interpreta i dati del dispositivo e le operazioni della regola dell'argomento che inviano il risultato dell'istruzione SQL ai servizi che la utilizzeranno.

Se stai aggiungendo la destinazione per la prima volta, ti consigliamo di utilizzare la console.

Aggiunta di una destinazione tramite la console

Se si aggiunge un dispositivo wireless utilizzando la console come descritto in Aggiungi le specifiche del dispositivo wireless ad AWS IoT Core per LoRaWAN utilizzando la console, dopo aver già aggiunto le specifiche e i profili del dispositivo wireless ad AWS IoT Core per LoRaWAN come descritto in precedenza, puoi andare avanti e aggiungere una destinazione.

In alternativa, puoi aggiungere anche una destinazione di AWS IoT Core per LoRaWAN dalla pagina Destinations (Destinazioni) della console AWS IoT.

Per elaborare i dati di un dispositivo, specifica i seguenti campi durante la creazione di una destinazione di AWS IoT Core per LoRaWAN, quindi scegli Add destination (Aggiungi destinazione).

- Dettagli della destinazione

  Inserisci un Nome della destinazione e una descrizione facoltativa per la destinazione.
- Nome regola

  La regola AWS IoT configurata per valutare i messaggi inviati dal tuo dispositivo ed elaborare i dati del dispositivo. Il nome della regola verrà mappato alla tua destinazione. La destinazione richiede la regola per elaborare i messaggi ricevuti. È possibile scegliere se elaborare i messaggi richiamando una regola AWS IoT o pubblicando sul broker di messaggi AWS IoT.
  - Se scegli Ente a rule name (Inserisci il nome di una regola), inserisci un nome, e quindi scegli Copy (Copia) per copiare il nome di una regola che inserirai quando crei la regola AWS IoT. Puoi scegliere Create a rule (Crea una regola) per creare la regola ora o passare all'hub Rules (Regole) della console AWS IoT e creare una regola con quel nome.

    Puoi anche inserire una regola e utilizzare impostazione Advanced (Avanzata) per specificare un nome dell'argomento. Il nome dell'argomento viene fornito durante l'invocazione della regola e si accede utilizzando l'espressione `topic` all'interno della regola. Per ulteriori informazioni sulle regole AWS IoT, consulta https://docs.aws.amazon.com/iot/latest/developerguide/iot-rules.html.
  - Se scegli Publish to AWS IoT message broker (Pubblica sul broker di messaggi IoT), inserisci un nome di argomento. È quindi possibile copiare il nome dell'argomento MQTT e più sottoscriventi possono iscriversi a questo argomento per ricevere messaggi pubblicati su tale argomento. Per ulteriori informazioni, consultare https://docs.aws.amazon.com/iot/latest/developerguide/topics.html.

  Per ulteriori informazioni sulle regole di AWS IoT per le destinazioni, consulta Creare regole per elaborare i messaggi del dispositivo LoRaWAN.

- Nome ruolo

  Il ruolo IAM che fornisce al dispositivo l'autorizzazione ai dati per accedere alla regola denominata in Rule name (Nome regola). Nella console puoi creare un nuovo ruolo di servizio o selezionare un ruolo di servizio già esistente. Se stai creando un nuovo ruolo di servizio, puoi inserire un nome di ruolo (ad esempio, **`IoTWirelessDestinationRole`**), o lasciare vuoto per consentire a AWS IoT Core per LoRaWAN di generare un nuovo nome ruolo. AWS IoT Core per LoRaWAN creerà automaticamente il ruolo IAM con le autorizzazioni appropriate per tuo conto.

  Per ulteriori informazioni sui ruoli IAM, consulta Utilizza ruoli IAM.

Aggiungi una destinazione utilizzando l'API

Se invece desideri aggiungere una destinazione utilizzando la CLI, è necessario aver già creato la regola e il ruolo IAM per la destinazione. Per ulteriori informazioni sui dettagli richiesti da una definizione nel ruolo, consulta Creazione di un ruolo IAM per le destinazioni.

Gli elenchi seguenti descrivono le operazioni API che eseguono le attività associate all'aggiunta, all'aggiornamento o all'eliminazione di una destinazione.

Operazioni API AWS IoT Wireless per le destinazioni

- CreateDestination
- GetDestination
- ListDestinations
- UpdateDestination
- DeleteDestination

Per l'elenco completo delle operazioni e dei tipi di dati disponibili per creare e gestire le risorse AWS IoT Core per LoRaWAN, consulta la documentazione di riferimento delle API AWS IoT Wireless

Come utilizzare la AWS CLI per aggiungere una destinazione

Puoi utilizzare AWS CLI per aggiungere una destinazione utilizzando il comando create-destination. L'esempio seguente mostra come creare una destinazione inserendo un nome di regola utilizzando `RuleName` come valore per il parametro `expression-type`. Se desideri specificare il nome di un argomento per la pubblicazione o la sottoscrizione al broker di messaggi, modifica il valore del parametro `expression-type` in `MqttTopic`.

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

L'esecuzione di questo comando crea una destinazione con il nome di destinazione, il nome della regola e il nome del ruolo specificati. Per informazioni sui nomi di regole e ruoli per le destinazioni, consulta Creare regole per elaborare i messaggi del dispositivo LoRaWAN e Creazione di un ruolo IAM per le destinazioni.

Per informazioni sulle CLI utilizzabili, consulta Riferimento AWS CLI.

Creazione di un ruolo IAM per le destinazioni

Destinazioni AWS IoT Core per LoRaWAN richiedono ruoli IAM che danno ad AWS IoT Core per LoRaWAN le autorizzazioni necessarie per inviare i dati alla regola AWS IoT. Se tale ruolo non è già definito, è necessario definirlo in modo che venga visualizzato nell'elenco dei ruoli.

Quando utilizzi la console per aggiungere una destinazione, AWS IoT Core per LoRaWAN crea automaticamente un ruolo IAM per te, come descritto in precedenza in questo argomento. Quando aggiungi una destinazione utilizzando l'API o la CLI, devi creare il ruolo IAM per la tua destinazione.

Per creare una policy IAM per il ruolo di destinazione di AWS IoT Core per LoRaWAN

1. Apri la pagina Policies hub of the IAM console (Hub delle policy nella console IAM).
2. Scegli Create policy (Crea policy), quindi scegli la scheda JSON.
3. Nell'editor, elimina qualsiasi contenuto dall'editor e incolla il documento relativo alle policy.

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

```
}
```

4. Scegli Review policy (Rivedi la policy), e inserisci un nome per questa policy in Name (Nome). Dovrai utilizzare questo nome nella procedura successiva.

   Se necessario, è inoltre possibile descrivere questa policy in Description (Descrizione).

5. Scegli Crea policy.

Per creare un ruolo IAM per una destinazione di AWS IoT Core per LoRaWAN

1. Apri Roles hub of the IAM console (Hub dei ruoli della console IAM) e scegli Create role (Crea ruolo).
2. In Seleziona tipo di entità attendibile, scegli Altro Account AWS.
3. In Account ID (ID account), inserisci il tuo account Account AWS ID, quindi scegli Next: Permissions (Successivo: autorizzazioni).
4. Nella casella di ricerca, inserisci il nome della policy IAM creata nella procedura precedente.
5. Nei risultati della ricerca, controlla la policy IAM creata nella procedura precedente.
6. Scegli Successivo: Tag, quindi Successivo: Rivedi.
7. In Role Name (Nome ruolo), inserisci il nome di questo ruolo, quindi scegli Create role (Crea ruolo).
8. Nel messaggio di conferma, scegli il nome del ruolo creato per modificare il nuovo ruolo.
9. In Summary (Riepilogo), scegli la finestra Trust relationships (Relazioni di trust) e seleziona Edit trust relationship (Modifica relazione di trust).
10. In Policy Document (Documento policy), modifica la proprietà di `Principal` affinché appaia come nell'esempio.

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

Dopo aver modificato la proprietà `Principal`, il documento completo di policy dovrebbe essere simile al seguente.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "iotwireless.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {}
    }
  ]
}
```

11. Per salvare le modifiche, scegli Update Trust Policy (Aggiorna policy di attendibilità).

Puoi trovare questo ruolo definito nell'elenco dei ruoli quando configuri le tue destinazioni AWS IoT Core per LoRaWAN.

Creare regole per elaborare i messaggi del dispositivo LoRaWAN

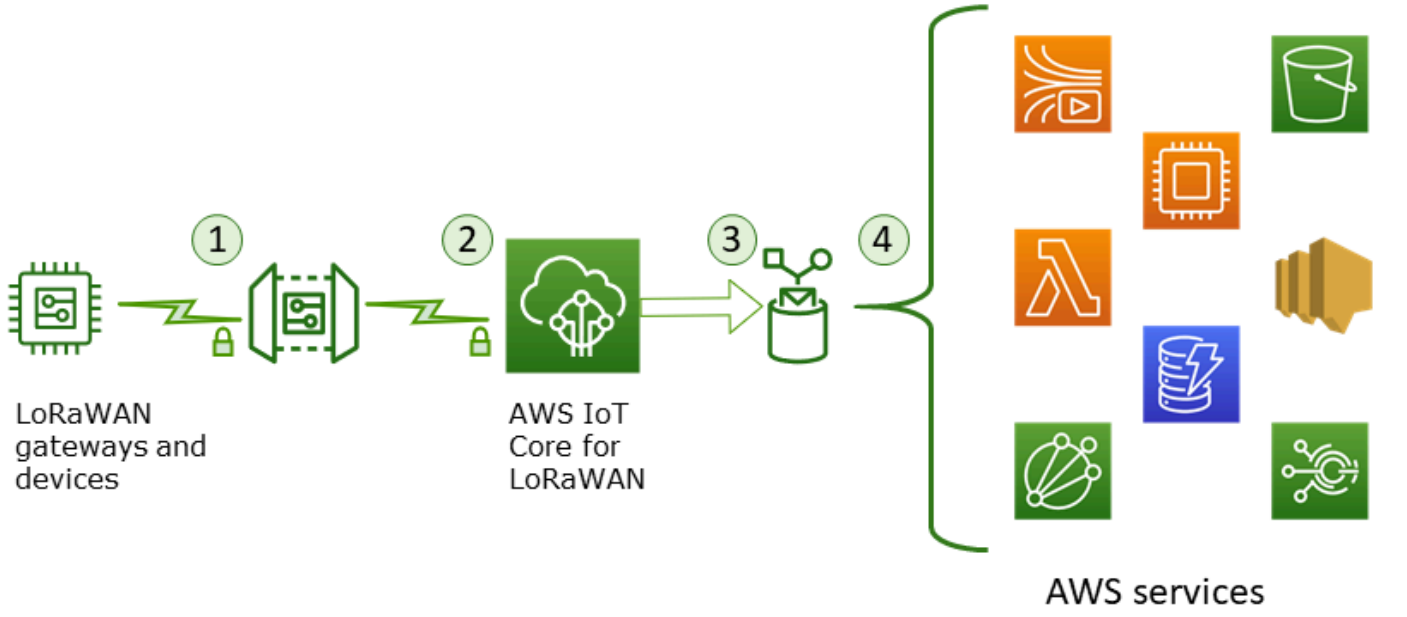
Le regole AWS IoT inviano messaggi del dispositivo ad altri servizi. Le regole AWS IoT possono anche elaborare i messaggi binari ricevuti da un dispositivo LoRaWAN per convertire i messaggi in altri formati che possono renderli più facili per altri servizi da utilizzare.

Destinazioni AWS IoT Core per LoRaWAN associano un dispositivo wireless alla regola che elabora i dati dei messaggi del dispositivo da inviare ad altri servizi. La regola agisce sui dati del dispositivo non appena AWS IoT Core per LoRaWAN lo riceve. Le destinazioni AWS IoT Core per LoRaWAN possono essere condivise da tutti i dispositivi i cui messaggi hanno lo stesso formato di dati e che inviano i loro dati allo stesso servizio.

Come funziona il processo di regole AWS IoT per i messaggi del dispositivo

Come una regola AWS IoT elabora i dati dei messaggi di un dispositivo dipende dal servizio che riceverà i dati, dal formato dei dati dei messaggi del dispositivo e dal formato dei dati richiesto dal servizio. In genere, la regola chiama una funzione AWS Lambda per convertire i dati dei messaggi del dispositivo nel formato richiesto da un servizio e quindi invia il risultato al servizio.

Nella figura seguente viene illustrato come i dati dei messaggi vengono protetti ed elaborati mentre vengono spostati dal dispositivo wireless a un servizio AWS.



1. Il dispositivo wireless LoRaWAN crittografa i suoi messaggi binari utilizzando la modalità CTR AES128 prima di trasmetterli.
2. AWS IoT Core per LoRaWAN decritta il messaggio binario e codifica il payload del messaggio binario decrittato come stringa base64.
3. Il messaggio codificato su base 64 risultante viene inviato come payload del messaggio, non formattato come documento JSON, alla regola AWS IoT descritta nella destinazione assegnata al dispositivo.
4. La regola AWS IoT indirizza i dati del messaggio al servizio descritto nella configurazione della regola.

Il payload binario crittografato ricevuto dal dispositivo wireless non viene alterato o interpretato da AWS IoT Core per LoRaWAN. Il payload del messaggio binario decrittato è codificato solo come stringa base64. Affinché i servizi possano accedere agli elementi dati nel payload del messaggio binario, gli elementi dati devono essere analizzati fuori dal payload da una funzione chiamata dalla regola. Il payload del messaggio con codifica base64 è una stringa ASCII, quindi potrebbe essere archiviata come tale per essere analizzata in un secondo momento.

Creazione di regole per dispositivi LoRaWAN

AWS IoT Core per LoRaWAN utilizza regole AWS IoT per inviare in modo sicuro i messaggi del dispositivo direttamente ad altri servizi AWS senza la necessità di utilizzare il broker di messaggi.

Rimuovere il broker di messaggi dal percorso di importazione dati riduce i costi e ottimizza il flusso di dati.

Una regola AWS IoT Core per LoRaWAN per inviare messaggi del dispositivo ad altri servizi AWS, richiede una destinazione AWS IoT Core per LoRaWAN una regola AWS IoT assegnata a quella destinazione. La regola AWS IoT deve contenere un'istruzione di query SQL e almeno un'operazione della regola.

In genere, l'istruzione query della regola AWS IoT è composta da:

- Una clausola SQL SELECT che seleziona e formatta i dati dal payload del messaggio
- Un filtro argomento (l'oggetto FROM nell'istruzione query di regole) che identifichi i messaggi da utilizzare
- Un'istruzione condizionale facoltativa (una clausola SQL WHERE) che specifica le condizioni su cui agire

Di seguito è illustrato un esempio di dichiarazione di query di regole:

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

Durante la costruzione delle regole AWS IoT per elaborare payload dai dispositivi LoRaWAN, non è necessario specificare la clausola FROM come parte dell'oggetto query regola. L'istruzione di query delle regole deve avere la clausola SQL SELECT e facoltativamente può avere la clausola WHERE. Se l'istruzione query utilizza la clausola FROM, viene ignorata.

Di seguito è illustrato un esempio di un'istruzione di query di regole in grado di elaborare i payload dai dispositivi LoRaWAN:

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

In questo esempio, `PayloadData` è un payload binario codificato in base64, inviato dal tuo dispositivo LoRaWAN.

Ecco un'istruzione query di regola di esempio che può eseguire una decodifica binaria del payload in entrata e trasformarlo in un formato diverso come 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
```

Per ulteriori informazioni sull'utilizzo delle clausole SELECT AND WHERE, consulta https://docs.aws.amazon.com/iot/latest/developerguide/iot-sql-reference.html.

Per informazioni sulle regole AWS IoT e su come crearle e utilizzarle, consulta https://docs.aws.amazon.com/iot/latest/developerguide/iot-rules.html e https://docs.aws.amazon.com/iot/latest/developerguide/iot-rules-tutorial.html.

Per informazioni su come creare e utilizzare destinazioni AWS IoT Core per LoRaWAN, consulta Aggiunta di destinazioni a AWS IoT Core per LoRaWAN.

Per informazioni sull'utilizzo dei payload dei messaggi binari in una regola, consulta https://docs.aws.amazon.com/iot/latest/developerguide/binary-payloads.html.

Per ulteriori informazioni sulla sicurezza dei dati e sulla crittografia utilizzati per proteggere il payload dei messaggi durante il percorso, consulta Protezione dei dati in Wireless AWS IoT.

Per un'architettura di riferimento che mostra un esempio di decodifica e implementazione binaria per le regole IoT, consulta Esempi di soluzioni AWS IoT Core per LoRaWAN su GitHub.

Connetti il tuo dispositivo LoRaWAN e verifica lo stato della connessione

Prima di poter controllare lo stato della connessione del dispositivo, è necessario aver già aggiunto il dispositivo e averlo collegato ad AWS IoT Core per LoRaWAN. Per informazioni su come aggiungere un dispositivo, consulta Aggiungi il dispositivo wireless ad AWS IoT Core per LoRaWAN.

Dopo aver aggiunto il dispositivo, consulta il manuale utente del dispositivo per informazioni su come avviare l'invio di un messaggio di uplink dal dispositivo LoRaWAN.

Controllare lo stato della connessione del dispositivo utilizzando la console

Per verificare lo stato della connessione utilizzando la console, passa alla pagina Devices (Dispositivi) della console AWS IoT e scegli il dispositivo che hai aggiunto. Nella sezione Details (Dettagli) della pagina dei dettagli dei dispositivi wireless, vedrai la data e l'ora in cui è stato ricevuto l'ultimo uplink.

Controllare lo stato della connessione del dispositivo utilizzando l'API

Per verificare lo stato della connessione utilizzando l'API, utilizza l'API `GetWirelessDeviceStatistics`. Questa API non ha un corpo della richiesta e contiene solo un corpo di risposta che mostra quando è stato ricevuto l'ultimo uplink.

```
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"
}
```

Passaggi successivi

Dopo aver collegato il dispositivo e verificato lo stato della connessione, è possibile osservare il formato dei metadati uplink ricevuti dal dispositivo utilizzando il Client di prova MQTT sulla pagina Test della console AWS IoT. Per ulteriori informazioni, consultare Visualizza il formato dei messaggi di uplink inviati dai dispositivi LoRaWAN.

Configurazione della posizione delle risorse wireless con AWS IoT Core per LoRaWAN

Prima di utilizzare questa funzione, tenere presente che il fornitore di terze parti scelto per la risoluzione delle informazioni sulla posizione dei dispositivi LoRaWAN si basa su feed di dati e set di dati forniti o gestiti da International GNSS Service (IGS), EarthData via NASA o da altre terze parti. Questi feed di dati e set di dati sono contenuti di terze parti (come definito nel Contratto con il

cliente) e vengono forniti così come sono. Per ulteriori informazioni, consultare Termini del servizio AWS.

È possibile utilizzare AWS IoT Core per LoRaWAN per specificare i dati sulla posizione statica o attivare il posizionamento per identificare la posizione del dispositivo in tempo reale utilizzando risolutori di terze parti. Puoi aggiungere o aggiornare le informazioni sulla posizione per dispositivi o gateway LoRaWAN o entrambi.

È possibile specificare le informazioni sulla posizione quando si aggiunge il dispositivo o il gateway a AWS IoT Core per LoRaWAN o quando si modificano i dettagli di configurazione del dispositivo o del gateway. Le informazioni sulla posizione sono specificate come un payload GeoJSON. Il formato GeoJSON viene utilizzato per codificare strutture di dati geografici. Il payload contiene le coordinate di latitudine e longitudine della posizione del dispositivo, basate sul sistema di coordinate World Geodetic System (WGS84).

Dopo che i risolutori calcolano la posizione della risorsa, se si dispone del servizio di posizione Amazon, è possibile attivare una mappa delle posizioni Amazon in cui verrà visualizzata la risorsa. Utilizzando i dati sulla posizione, potrai:

- Attivare il posizionamento per identificare e ottenere la posizione dei dispositivi LoRaWAN.
- Tracciare e monitorare i gateway e i dispositivi.
- Definire le regole AWS IoT che elaborano eventuali aggiornamenti ai dati sulla posizione e li instradano a un altro Servizio AWS. Per un elenco delle azioni delle regole, consulta le azioni delle regole AWS IoT nella Guida per gli sviluppatori AWS IoT.
- Creare avvisi e ricevere notifiche sui dispositivi in caso di attività insolite utilizzando i dati sulla posizione e Amazon SNS.

Funzionamento del posizionamento per i dispositivi LoRaWAN

È possibile attivare il posizionamento per identificare la posizione dei dispositivi utilizzando risolutori Wi-Fi e GNSS di terze parti. Queste informazioni possono essere utilizzate per tracciare e monitorare il dispositivo. Nei seguenti passaggi viene illustrato come attivare il posizionamento e visualizzare le informazioni sulla posizione per dispositivi LoRaWAN.

> **Note**
>
> Il risolutore di terze parti può essere utilizzato solo con dispositivi LoRaWAN dotati del chip LoRa Edge. Non può essere utilizzato con i gateway LoRaWAN. Per i gateway, è comunque possibile specificare le informazioni sulla posizione statica e identificare la posizione su una mappa delle posizioni Amazon.

1. Aggiunta del dispositivo

   Prima di attivare il posizionamento, aggiungere innanzitutto il dispositivo a AWS IoT Core per LoRaWAN Il dispositivo LoRaWAN deve essere dotato di un chipset LoRa Edge, che è una piattaforma a bassissima potenza che integra un ricetrasmettitore LoRa a lungo raggio, uno scanner GNSS multi-costellazione e uno scanner MAC Wi-Fi passivo destinato alle applicazioni di geolocalizzazione.

2. Attivazione del posizionamento

   Per ottenere la posizione in tempo reale dei dispositivi, attivare il posizionamento. Quando il dispositivo LoRaWAN invia un messaggio di uplink, i dati di scansione Wi-Fi e GNSS contenuti nel messaggio vengono inviati a AWS IoT Core per LoRaWAN utilizzando la porta del frame di geolocalizzazione.

3. Recupero delle informazioni sulla posizione

   Recuperare la posizione stimata del dispositivo dai risolutori calcolati in base ai risultati della scansione dei ricetrasmettitori. Se le informazioni sulla posizione sono state calcolate utilizzando i risultati della scansione Wi-Fi e GNSS, AWS IoT Core per LoRaWAN seleziona la posizione stimata con la maggiore precisione.

4. Visualizzazione delle informazioni sulla posizione

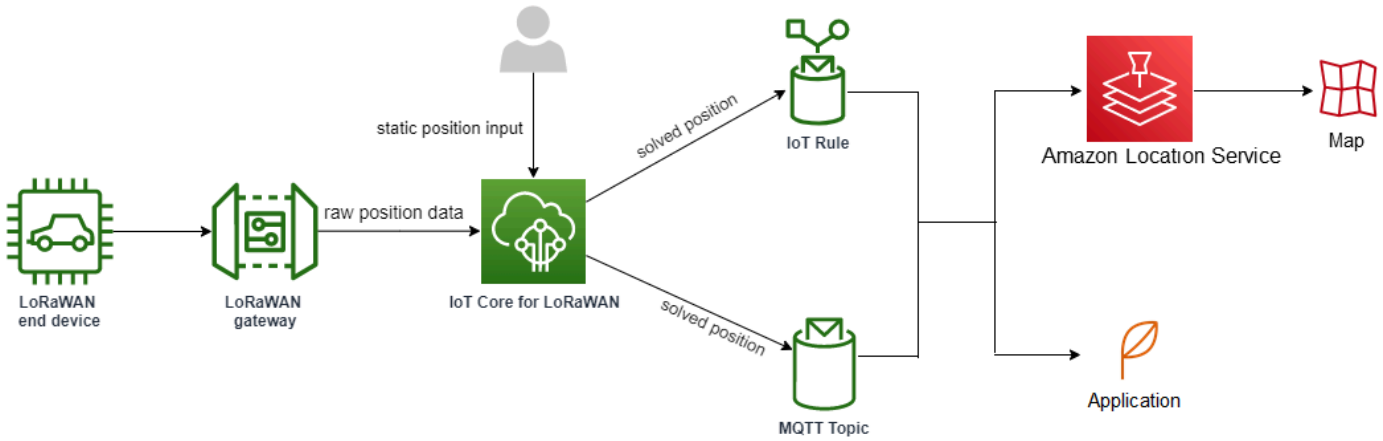
   Dopo che il risolutore calcola le informazioni sulla posizione, fornirà le informazioni sulla precisione che indicano la differenza tra la posizione calcolata dai risolutori e le informazioni sulla posizione statica immesse. È anche possibile visualizzare la posizione del dispositivo su una mappa delle posizioni Amazon.

> **Note**
>
> Poiché i risolutori non possono essere utilizzati per i gateway LoRaWAN, le informazioni sulla precisione verranno riportate come `0.0`.

Per ulteriori informazioni sul formato dei messaggi di uplink e sulle porte di frequenza utilizzate per il risolutore di posizionamento, consulta Messaggio di uplink da AWS IoT Core per LoRaWAN a motore delle regole.

Panoramica del flusso di lavoro di posizionamento

Il seguente diagramma mostra come AWS IoT Core per LoRaWAN memorizza e aggiorna le informazioni sulla posizione dei tuoi dispositivi e gateway.



1. Specifica della posizione statica della risorsa

   Specificare le informazioni sulla posizione statica del dispositivo o del gateway come un payload GeoJSON, utilizzando le coordinate di latitudine e longitudine. Facoltativamente, puoi anche specificare un valore per l'altitudine. Queste coordinate sono basate sul sistema di coordinate WGS84. Per ulteriori informazioni, consulta la pagina del sistema geodetico mondiale (WGS84).

2. Attivazione del posizionamento per i dispositivi

   Se si utilizzano dispositivi LoRaWAN dotati del chip LoRa Edge, è possibile attivare il posizionamento per tracciare la posizione del dispositivo in tempo reale. Quando il dispositivo invia un messaggio di uplink, i dati di scansione Wi-Fi e GNSS vengono inviati a AWS IoT Core per

LoRaWAN utilizzando la porta del frame di geolocalizzazione. I risolutori utilizzano quindi queste informazioni per risolvere la posizione del dispositivo.

3. Aggiunta di una destinazione ai dati per l'instradamento dei dati sulla posizione

   È possibile aggiungere una destinazione che descrive la regola IoT per l'elaborazione dei dati del dispositivo e instradare le informazioni aggiornate sulla posizione a AWS IoT Core per LoRaWAN. È anche possibile visualizzare l'ultima posizione nota della risorsa su una mappa delle posizioni Amazon.

Configurazione della posizione della risorsa

Puoi configurare la posizione della risorsa utilizzando la AWS Management Console, l'API AWS IoT Wireless o la AWS CLI.

Se i dispositivi dispongono del chip LoRa Edge, è possibile attivare il posizionamento per calcolare le informazioni sulla posizione in tempo reale. Per i tuoi gateway, puoi comunque inserire le coordinate di posizione statiche e utilizzare il servizio di posizione Amazon. per tracciare la posizione del gateway su una mappa delle posizioni Amazon.

Argomenti

- Configurazione della posizione dei gateway LoRaWAN
- Configurazione della posizione dei dispositivi LoRaWAN

Configurazione della posizione dei gateway LoRaWAN

Quando si aggiunge il gateway a AWS IoT Core per LoRaWAN, è possibile specificare i dati sulla posizione statica. Se sono state attivate le mappe del servizio di posizione Amazon, i dati sulla posizione vengono visualizzati su una mappa delle posizioni Amazon.

> **Note**
>
> I risolutori di terze parti non possono essere utilizzati con i gateway LoRaWAN. Per i gateway, è comunque possibile specificare le coordinate della posiziona statica. Se per calcolare la posizione non vengono utilizzati i risolutori, ad esempio nel caso dei gateway, le informazioni sulla precisione verranno riportate come `0.0`.

Puoi configurare la posizione della gateway utilizzando la AWS Management Console, l'API AWS IoT Wireless o la AWS CLI.

Configurazione della posizione del gateway utilizzando la console

Per configurare la posizione delle risorse gateway utilizzando la AWS Management Console, accedi prima alla console quindi passa alla pagina hub Gateway della console AWS IoT.

Aggiunta di informazioni sulla posizione

Aggiunta di una configurazione della posizione per il gateway

1. Nella pagina hub Gateway, scegli Add gateway (Aggiungi gateway).
2. Specifica l'identificatore univoco esteso (EUI) del gateway, la banda di frequenza (RFRegion) e tutti i dettagli aggiuntivi del gateway, oltre alle informazioni di configurazione LoRaWAN. Per ulteriori informazioni, consultare Aggiungere un gateway utilizzando la console.
3. Vai alla sezione Position information - Optional (Informazioni sulla posizione - facoltativa) e inserisci le informazioni sulla posizione per il gateway utilizzando le coordinate di latitudine e longitudine e una coordinata di altitudine facoltativa. Le informazioni sulla posizione si basano sul sistema di coordinate WGS84.

Visualizzazione della posizione del gateway

Dopo aver configurato la posizione del gateway, AWS IoT Core per LoRaWAN crea una mappa delle posizioni Amazon chiamata `iotwireless.map`. Questa mappa è presente sulla pagina dei dettagli del tuo gateway nella scheda Position (Posizione). In base alle coordinate di posizione specificate, la posizione del gateway verrà visualizzata come contrassegno sulla mappa. Puoi ingrandire o rimpicciolire la mappa per visualizzare chiaramente la posizione del tuo gateway. Nella scheda Position (Posizione), vengono anche visualizzate informazioni sulla precisione e il timestamp del momento in cui è stata determinata la posizione del gateway.

> **Note**
>
> Se non hai installato le mappe del servizio di posizione Amazon, sarà visualizzato un messaggio che indica che è necessario utilizzare questo servizio per accedere alla mappa e visualizzare la posizione del gateway. L'utilizzo di mappe del servizio di posizione Amazon può comportare addebiti aggiuntivi al tuo Account AWS. Per ulteriori informazioni, consultare Prezzi di AWS IoT Core.

La mappa, `iotwireless.map`, funge da fonte di dati cartografici a cui si accede tramite operazioni API `Get`, ad esempio `GetMapTile`. Per informazioni sulle API `Get` utilizzate con le mappe, consulta Amazon Location Service API reference (Documentazione di riferimento delle API del servizio di posizione Amazon).

Per ulteriori dettagli su questa mappa, vai alla console del servizio di posizione Amazon, scegli maps (mappe) quindi seleziona iotwireless.map. Per ulteriori informazioni, consultare Mappe nella Guida per gli sviluppatori del servizio di posizione Amazon.

Aggiornamento della configurazione della posizione del gateway

Per modificare la configurazione della posizione del gateway, nella pagina dei dettagli del gateway, seleziona Edit (Modifica), quindi aggiorna le informazioni sulla posizione e la destinazione.

> **Note**
>
> Le informazioni sui dati storici della posizione non sono disponibili. Quando aggiorni le coordinate di posizione del gateway, i dati sulla posizione riportati in precedenza vengono sovrascritti. Dopo aver aggiornato la posizione, nella scheda Position (Posizione) dei dettagli del gateway, vedrai le nuove informazioni sulla posizione. Una modifica del timestamp indica che corrisponde all'ultima posizione nota del gateway.

Configurazione della posizione del gateway tramite l'API

Puoi specificare le informazioni sulla posizione e configurare il gateway utilizzando l'API AWS IoT Wireless o la AWS CLI.

> **Important**
>
> Le operazioni API UpdatePosition, GetPosition, PutPositionConfiguration, GetPositionConfiguration e ListPositionConfigurations non sono più supportate. Le chiamate per aggiornare e recuperare le informazioni sulla posizione devono utilizzare le operazioni API GetResourcePosition e UpdateResourcePosition.

Aggiunta di informazioni sulla posizione

Per aggiungere le informazioni sulla posizione statica per un determinato gateway wireless, specificare le coordinate utilizzando l'operazione API UpdateResourcePosition o il comando update-

resource-position della CLI. Specificare `WirelessGateway` come `ResourceType`, l'ID del gateway wireless da aggiornare come `ResourceIdentifier` e le informazioni sulla posizione come payload GeoJSON.

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

Nell'esempio seguente viene mostrato il contenuto del file *`gatewayposition.json`*.

Contenuto di gatewayposition.json

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

L'esecuzione di questo comando non produce output. Per visualizzare le informazioni sulla posizione specificate, utilizzare l'operazione API `GetResourcePosition`.

Ottenimento delle informazioni sulla posizione

Per ottenere le informazioni sulla posizione di un determinato gateway wireless, utilizzare l'API GetResourcePosition o il comando get-resource-position della CLI. Specifica `WirelessGateway` come `resourceType` e immetti l'ID del gateway wireless come `resourceIdentifier`.

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

L'esecuzione di questo comando visualizza le informazioni sulla posizione del gateway wireless come un payload GeoJSON. Saranno visualizzate le informazioni sulle coordinate della posizione, il tipo di informazioni sulla posizione e proprietà aggiuntive, come il timestamp che corrisponde all'ultima posizione nota del gateway.

```
{
```

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

Configurazione della posizione dei dispositivi LoRaWAN

Quando si aggiunge il dispositivo a AWS IoT Core per LoRaWAN, è possibile specificare le informazioni sulla posizione statica, attivare facoltativamente il posizionamento e specificare una destinazione. La destinazione descrive la regola IoT che elabora le informazioni sulla posizione del dispositivo e instrada la posizione aggiornata al servizio di posizione Amazon. Dopo aver configurato la posizione del dispositivo, i dati sulla posizione vengono visualizzati su una mappa di posizioni di Amazon con le informazioni sulla precisione e la destinazione specificata.

Puoi configurare la posizione del dispositivo utilizzando la AWS Management Console, l'API AWS IoT Wireless o la AWS CLI.

Porte di frame e formato dei messaggi di uplink

Se si attiva il posizionamento, è necessario specificare la porta di frame di geolocalizzazione per comunicare i dati di scansione Wi-Fi e GNSS dal dispositivo a AWS IoT Core per LoRaWAN. Le informazioni sulla posizione vengono comunicate a AWS IoT Core per LoRaWAN tramite la porta di frame.

La specifica LoRaWAN fornisce un campo di consegna dati (FRMPayload) e un campo Port (FPort) per distinguere tra diversi tipi di messaggi. Per comunicare le informazioni sulla posizione, per la porta di frame è possibile specificare un valore qualsiasi compreso tra 1 e 223. FPort 0 è riservato ai messaggi MAC, FPort 224 è riservato ai test di conformità MAC e le porte 225-255 sono riservate per future estensioni di applicazioni standardizzate.

Messaggio di uplink da AWS IoT Core per LoRaWAN a motore delle regole

Quando aggiungi una destinazione, viene creata una regola AWS IoT per instradare i dati al servizio di posizione Amazon utilizzando il motore delle regole. Le informazioni aggiornate sulla posizione vengono quindi visualizzate su una mappa delle posizioni Amazon. Se il posizionamento non è stato

attivato, la destinazione instrada i dati sulla posizione quando si aggiornano le coordinate di posizione statiche del dispositivo.

Il seguente codice mostra il formato del messaggio di uplink inviato da AWS IoT Core per LoRaWAN con le informazioni sulla posizione, la precisione, la configurazione del risolutore e i metadati wireless. I campi evidenziati di seguito sono facoltativi. Se non sono disponibili informazioni sulla precisione verticale, il valore è `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 per 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": "80029cfffe5cf1cc",
                    "Snr": -29,
                    "Rssi": 9.75
                }
                ],
            "MIC": "7255cb07",
            "MType": "UnconfirmedDataUp",
            "Major": "LoRaWANR1",
            "Modulation": "LORA",
            "PolarizationInversion": false,
            "SpreadingFactor": 12,
            "Timestamp": "2021-05-03T03:24:29Z"

        }
    }
}
```

Configurazione della posizione dei dispositivi tramite la console

Per configurare e gestire la posizione dei dispositivi tramite la AWS Management Console, accedere innanzitutto alla console quindi passare alla pagina hub Devices (Dispositivi) della console AWS IoT.

Aggiunta di informazioni sulla posizione

Per aggiungere informazioni sulla posizione per il dispositivo:

1. Nella pagina hub Devices (Dispositivi), scegli Add wireless device (Aggiungi dispositivo wireless).
2. Immetti le specifiche del dispositivo wireless, i profili di dispositivo e servizio e la destinazione che definisce la regola IoT per l'instradamento dei dati a un altro Servizio AWS. Per ulteriori informazioni, consultare Integra i tuoi dispositivi su AWS IoT Core per LoRaWAN.
3. Immetti le informazioni sulla posizione, attiva facoltativamente la geolocalizzazione e specifica una destinazione dei dati sulla posizione che desideri utilizzare per instradare i messaggi.
   - Informazioni sulla posizione

     Specifica i dati sulla posizione per il dispositivo utilizzando le coordinate di latitudine e longitudine e una coordinata di altitudine facoltativa. Le informazioni sulla posizione si basano sul sistema di coordinate WGS84.
   - GeoLocation

Attiva il posizionamento se desideri che AWS IoT Core per LoRaWAN utilizzi la geolocalizzazione per calcolare la posizione del dispositivo. I risolutori GNSS e Wi-Fi di terze parti vengono utilizzati per identificare la posizione del dispositivo in tempo reale.

Per inserire le informazioni di geolocalizzazione, scegli Attiva posizionamento e inserisci la porta di frame di geolocalizzazione per comunicare i dati di scansione GNSS e Wi-Fi a AWS IoT Core per LoRaWAN. Come riferimento, sono già inseriti i valori di FPort predefiniti. Tuttavia, puoi scegliere un valore diverso compreso tra 1 e 223.

- Destinazione dei dati sulla posizione

  Scegli una destinazione per descrivere la regola AWS IoT che elabora i dati sulla posizione del dispositivo e invia la posizione aggiornata a AWS IoT Core per LoRaWAN. Utilizza questa destinazione solo per instradare i dati sulla posizione. Deve essere diversa dalla destinazione utilizzata per l'instradamento dei dati del dispositivo ad altri Servizio AWS.

Visualizzazione della configurazione della posizione del dispositivo

Dopo aver configurato la posizione del dispositivo, AWS IoT Core per LoRaWAN crea una mappa delle posizioni Amazon chiamata `iotwireless.map`. Questa mappa è presente sulla pagina dei dettagli del tuo dispositivo nella scheda Position (Posizione). In base alle coordinate di posizione specificate o alla posizione calcolata dai risolutori di terze parti, la posizione del dispositivo verrà visualizzata come un contrassegno sulla mappa. Puoi ingrandire o rimpicciolire la mappa per visualizzare chiaramente la posizione del tuo dispositivo. Nella pagina dei dettagli del dispositivo, nella scheda Position (Posizione), vedrai anche le informazioni sulla precisione, il timestamp in cui è stata determinata la posizione del dispositivo e la destinazione dei dati sulla posizione che hai specificato.

> **Note**
>
> Se non hai attivato le mappe del servizio di posizione Amazon, sarà visualizzato un messaggio che indica che è necessario utilizzare il servizio di posizione Amazon per accedere alla mappa e visualizzare la posizione. L'utilizzo di mappe del servizio di posizione Amazon può comportare addebiti aggiuntivi al tuo Account AWS. Per ulteriori informazioni, consultare Prezzi di AWS IoT Core.

La mappa, `iotwireless.map`, funge da fonte di dati cartografici a cui si accede tramite operazioni API `Get`, ad esempio `GetMapTile`. Per informazioni sulle API `Get` utilizzate con le mappe, consulta Amazon Location Service API reference (Documentazione di riferimento delle API del servizio di posizione Amazon).

Per ulteriori dettagli su questa mappa, vai alla console del servizio di posizione Amazon, scegli maps (mappe) quindi seleziona iotwireless.map. Per ulteriori informazioni, consultare Mappe nella Guida per gli sviluppatori del servizio di posizione Amazon.

Aggiornamento della configurazione della posizione del dispositivo

Per modificare la configurazione della posizione del dispositivo, nella pagina dei dettagli del dispositivo, scegli Edit (Modifica), quindi aggiorna le informazioni sulla posizione, eventuali impostazioni di geolocalizzazione e la destinazione.

> **Note**
>
> Le informazioni sui dati storici della posizione non sono disponibili. Quando aggiorni le coordinate di posizione del dispositivo, i dati sulla posizione riportati in precedenza vengono sovrascritti. Dopo aver aggiornato la posizione, nella scheda Position (Posizione) dei dettagli del dispositivo, vedrai le nuove informazioni sulla posizione. Una modifica del timestamp indica che corrisponde all'ultima posizione nota del dispositivo.

Configurazione della posizione del dispositivo tramite l'API

Puoi specificare le informazioni sulla posizione, configurare la posizione del dispositivo e attivare la geolocalizzazione facoltativa mediante l'API AWS IoT Wireless o la AWS CLI.

> **Important**
>
> Le operazioni API UpdatePosition, GetPosition, PutPositionConfiguration, GetPositionConfiguration e ListPositionConfigurations non sono più supportate. Le chiamate per aggiornare e recuperare le informazioni sulla posizione devono utilizzare le operazioni API GetResourcePosition e UpdateResourcePosition.

Aggiunta di informazioni sulla posizione e configurazione

Per aggiungere le informazioni sulla posizione per un determinato dispositivo wireless, specificare le coordinate utilizzando l'operazione API UpdateResourcePosition o il comando update-resource-position della CLI. Specificare `WirelessDevice` come `ResourceType`, l'ID del dispositivo wireless da aggiornare come `ResourceIdentifier` e le informazioni sulla posizione.

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

Nell'esempio seguente viene mostrato il contenuto del file *deviceposition.json*. Per specificare i valori FPort per l'invio dei dati di geolocalizzazione, utilizzare l'oggetto Positioning (Posizionamento) con le operazioni API CreateWirelessDevice e UpdateWirelessDevice.

Contenuto di deviceposition.json

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

L'esecuzione di questo comando non produce output. Per visualizzare le informazioni sulla posizione specificate, utilizzare l'operazione API `GetResourcePosition`.

Ottenimento delle informazioni su posizione e configurazione

Per ottenere le informazioni sulla posizione per un determinato dispositivo wireless, utilizzare l'API GetResourcePosition o il comando get-resource-position della CLI. Specifica `WirelessDevice` come `resourceType` e immetti l'ID del dispositivo wireless come `resourceIdentifier`.

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

L'esecuzione di questo comando visualizza le informazioni sulla posizione del dispositivo wireless come un payload GeoJSON. Saranno visualizzate le informazioni sulle coordinate della posizione, il tipo di posizione e le proprietà che includono le informazioni sulla precisione e il timestamp che corrisponde all'ultima posizione nota del 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"
      }
}
```

Gestione dei gateway con AWS IoT Wireless

Di seguito sono riportate alcune considerazioni importanti quando si utilizzano i gateway con AWS IoT Core per LoRaWAN. Per informazioni su come aggiungere il tuo gateway al AWS IoT Core per LoRaWAN, consulta Integrare i gateway per AWS IoT Core per LoRaWAN.

Requisiti software LoRa Basics Station

Per connettersi ad AWS IoT Core per LoRaWAN, il gateway LoRaWAN deve avere un software chiamato LoRa Basics Station in esecuzione. LoRa Basics Station è un software open source che viene gestito da Semtech Corporation e distribuito dalla loro repository GitHub. AWS IoT Core per LoRaWAN supporta LoRa Basics Station versione 2.0.4 e quelle successive. La versione più recente è la 2.0.6.

Utilizzo di gateway qualificati dal Catalogo dei dispositivi dei partner di AWS

Il Catalogo dei dispositivi dei partner AWS contiene gateway e kit di sviluppo qualificati per l'utilizzo con AWS IoT Core per LoRaWAN. Si consiglia di utilizzare questi gateway qualificati perché non è necessario modificare il software di incorporamento per la connessione dei gateway ad AWS IoT Core. Questi gateway dispongono già di una versione del software BasicStation compatibile con AWS IoT Core per LoRaWAN.

> **Note**
>
> Se disponi di un gateway non elencato nel Catalogo partner come gateway qualificato con AWS IoT Core per LoRaWAN, potresti ancora utilizzarlo se il gateway esegue il software LoRa Basics Station con la versione 2.0.4 e quelle successive. Assicurati di utilizzare Autenticazione client e server TLS per l'autenticazione del gateway LoRaWAN.

Utilizzo di protocolli CUPS e LNS

Il software LoRa Basics Station contiene due protocolli secondari per la connessione di gateway a server di rete, protocolli LoRaWAN Network Server (LNS) e Configuration and Update Server (CUPS).

Il protocollo LNS stabilisce una connessione dati tra un gateway compatibile LoRa Basics Station e un server di rete. I messaggi di uplink e downlink LoRa vengono scambiati tramite questa connessione dati tramite WebSockets sicuri.

Il protocollo CUPS abilita la gestione delle credenziali e la configurazione remota e l'aggiornamento del firmware dei gateway. AWS IoT Core per LoRaWAN fornisce endpoint LNS e CUPS rispettivamente per l'importazione di dati LoRaWAN e la gestione remota del gateway.

Per ulteriori informazioni, consulta Protocollo LNS e Protocollo CUPS.

Argomenti

- Configurazione delle funzionalità di beaconing e filtraggio dei gateway LoRaWAN
- Aggiornare il firmware del gateway utilizzando il servizio CUPS con AWS IoT Core per LoRaWAN
- Scelta dei gateway per ricevere il traffico dati in downlink LoRaWAN

Configurazione delle funzionalità di beaconing e filtraggio dei gateway LoRaWAN

Quando si utilizzano dispositivi LoRaWAN, è possibile configurare alcuni parametri opzionali per i gateway LoRaWAN. I parametri includono:

- Beaconing

È possibile configurare i parametri di beaconing per i gateway LoRaWAN che fungono da bridge per i dispositivi LoRaWAN di classe B. Questi dispositivi ricevono un messaggio di downlink nelle fasce orarie pianificate, pertanto è necessario configurare i parametri di beaconing affinché i gateway trasmettano questi beacon sincronizzati nel tempo.

- Filtraggio

  È possibile configurare i parametri `NetID` e `JoinEUI` per i gateway LoRaWAN per filtrare il traffico dati del dispositivo. Il filtraggio del traffico aiuta a preservare l'utilizzo della larghezza di banda e riduce il flusso di traffico tra gateway e LNS.

- Sottobande

  È possibile configurare le sottobande del gateway per specificare la particolare sottobanda che si desidera utilizzare. Per i dispositivi wireless che non possono passare da una sottobanda all'altra, è possibile utilizzare questa funzionalità per comunicare con i dispositivi utilizzando solo i canali di frequenza in quella particolare sottobanda.

I seguenti argomenti contengono ulteriori informazioni su questi parametri e su come configurarli. I parametri di beaconing non sono disponibili nella AWS Management Console e possono essere specificato solo mediante l'API AWS IoT Wireless API o l'AWS CLI.

Argomenti

Configurazione dei gateway per inviare beacon a dispositivi di classe B

Se si installano dispositivi wireless di classe B su AWS IoT Core per LoRaWAN, i dispositivi ricevono messaggi di downlink in intervalli temporali programmati. I dispositivi aprono questi intervalli in base a beacon sincronizzati nel tempo che vengono trasmessi dal gateway. Affinché i gateway trasmettano questi beacon sincronizzati nel tempo, è possibile usare AWS IoT Core per LoRaWAN per configurare determinati parametri relativi ai beacon per i gateway.

Per configurare questi parametri di beaconing, il gateway deve eseguire la versione del software LoRa Basics Station versione 2.0.6. Per informazioni, consulta Utilizzo di gateway qualificati dal Catalogo dei dispositivi dei partner di AWS.

Come configurare i parametri di beaconing

> **Note**
>
> È necessario configurare i parametri di beaconing per il gateway solo se comunica con un dispositivo wireless di classe B.

I parametri di beaconing vengono configurati quando si aggiunge il gateway a AWS IoT Core per LoRaWAN mediante l'operazione API `CreateWirelessGateway`. Quando si richiama l'operazione API, specificare i seguenti parametri utilizzando l'oggetto `Beaconing` per i gateway. Dopo aver configurato i parametri, i gateway invieranno i beacon ai dispositivi a intervalli di 128 secondi.

- `DataRate`: la velocità dei dati dei gateway che trasmettono i beacon.
- `Frequencies`: l'elenco delle frequenze con cui i gateway trasmettono i beacon.

L'esempio seguente mostra come configurare tali parametri per il gateway. Il file `input.json` conterrà ulteriori dettagli, ad esempio il certificato del gateway e le credenziali di provisioning. Per ulteriori informazioni sull'aggiunta di gateway a AWS IoT Core per LoRaWAN mediante l'operazione API `CreateWirelessGateway`, consulta Aggiungi un gateway utilizzando l'API.

> **Note**
>
> I parametri di beaconing non sono disponibili quando si aggiunge il gateway a AWS IoT Core per LoRaWAN mediante la console AWS IoT.

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

Nell'esempio seguente viene mostrato il contenuto del file `input.json`.

Contenuto di 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]
    }
}
```

Il seguente codice mostra l'output dell'esecuzione del comando.

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

Ottenimento delle informazioni sui parametri di beaconing

È possibile ottenere informazioni sui parametri di beaconing per il gateway utilizzando l'operazione API `GetWirelessGateway`.

> **Note**
>
> Se un gateway è già stato integrato, non è possibile utilizzare l'operazione API `UpdateWirelessGateway` per configurare i parametri di beaconing. Per configurare i parametri, è necessario eliminare il gateway e quindi specificare i parametri quando si aggiunge il gateway mediante l'operazione API `CreateWirelessGateway`.

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

L'esecuzione di questo comando restituisce informazioni sul gateway e sui parametri di beaconing.

Configurare le sottobande e le funzionalità di filtraggio del gateway

I gateway LoRaWAN eseguono un software LoRa Basics Station che abilita ai gateway di connettersi ad AWS IoT Core per LoRaWAN. Per connettersi ad AWS IoT Core per LoRaWAN, il tuo gateway LoRa interroga innanzitutto il server CUPS per l'endpoint LNS, quindi stabilisce una connessione dati WebSockets con tale endpoint. Una volta stabilita la connessione, i frame uplink e downlink possono essere scambiati tramite tale connessione.

Filtro dei frame dati LoRa ricevuti dal gateway

Dopo che il gateway LoRaWAN ha stabilito una connessione all'endpoint, AWS IoT Core per LoRaWAN risponde con un `router_config` messaggio che specifica un insieme di parametri per la configurazione del gateway LoRa, inclusi i parametri di filtraggio `NetID` e `JoinEui`. Per ulteriori informazioni su `router_config` e come viene stabilita una connessione con il server di rete LoRaWAN (LNS), consulta Protocollo 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
}
```

I gateway trasportano i dati dei dispositivi LoRaWAN da e verso LNS, di solito su reti ad alta larghezza di banda come Wi-Fi, Ethernet o Cellular. Di solito i gateway raccolgono tutti i messaggi e passano attraverso il traffico che arriva ad essi tramite AWS IoT Core per LoRaWAN. Tuttavia, è possibile configurare i gateway per filtrare parte del traffico dati del dispositivo, il che aiuta a preservare l'utilizzo della larghezza di banda e riduce il flusso di traffico tra gateway e LNS.

Per configurare il gateway LoRa per filtrare i frame di dati, è possibile utilizzare i parametri `NetID` e `JoinEui` nel messaggio `router_config`. `NetID` è un elenco di valori NetID accettati. Qualsiasi frame di dati LoRa contenente un frame di dati diverso da quelli elencati verrà eliminato. `JoinEui` è un elenco di coppie di valori interi che codificano intervalli di valori JoinEUI. I frame di richiesta

di join verranno eliminati dal gateway a meno che il campo nel messaggio `JoinEui` sia all'interno dell'intervallo [BegEui,EndEui].

Canali di frequenza e sottobande

Per le regioni RF US915 e AU915, i dispositivi wireless hanno una scelta di 64 canali di uplink 125 kHz e 8 500 kHz per accedere alle reti LoRaWAN utilizzando i gateway LoRa. I canali di frequenza uplink sono divisi in 8 sottobande, ciascuna con 8 canali 125kHz e un canale da 500 kHz. Per ogni gateway normale nella regione AU915, saranno supportate una o più sottobande.

Alcuni dispositivi wireless non possono passare tra le sottobande e utilizzare i canali di frequenza in una sola sottobanda quando sono connessi ad AWS IoT Core per LoRaWAN. Affinché i pacchetti uplink vengano trasmessi da tali dispositivi, configura i gateway LoRa per utilizzare quella particolare sottobanda. Per i gateway in altre regioni RF, come EU868, questa configurazione non è necessaria.

Come configurare il gateway affinché utilizzi filtri e sottobande utilizzando la console

È possibile configurare il gateway per utilizzare una particolare sottobanda e abilitare anche la capacità di filtrare i frame di dati LoRa. Per specificare questi parametri utilizzando la console:

1. Passa alla pagina AWS IoT Core per LoRaWAN Gateway della console AWS IoT e scegli Aggiungi gateway.
2. Specifica i dettagli del gateway, ad esempio Eui di Gateway, Banda di frequenza (RFRegion), un Nome opzionale, una Descrizione e scegli se associare un oggetto AWS IoT al gateway. Per informazioni su come aggiungere un gateway, consulta Aggiungere un gateway utilizzando la console.
3. Nella sezione LoRaWAN configuration (Configurazione LoRaWAN), è possibile specificare le sottobande e le informazioni di filtraggio.
   - `SubBands`: per aggiungere una sottobanda, scegli Add SubBand (Aggiungi sottobanda) e specifica un elenco di valori interi che indicano quali sottobande sono supportate dal gateway. Il parametro `SubBands` può essere configurato solo nelle `RfRegion` US915 e AU915 e devono avere valori nell'intervallo `[1,8]` in una di queste regioni supportate.
   - `NetIdFilters`: per filtrare i fotogrammi uplink, scegli Add NetId (Aggiungi NetID) e specifica un elenco di valori stringa utilizzati dal gateway. Il NetID del frame uplink in entrata dal dispositivo wireless deve corrispondere ad almeno uno dei valori elencati, altrimenti il fotogramma viene eliminato.
   - `JoinEuiFilters`: scegli Add JoinEui range (Aggiungi l'intervallo JoinEUI) e specifica un elenco di coppie di valori stringa utilizzati da un gateway per filtrare i frame LoRa. Il valore

JoinEUI specificato come parte della richiesta di join dal dispositivo wireless deve essere compreso nell'intervallo di almeno uno dei valori joinEuiRange, ciascuno elencato come una coppia di [BegEui, EndEui], altrimenti il frame viene eliminato.

4. È quindi possibile continuare a configurare il gateway seguendo le istruzioni descritte in Aggiungere un gateway utilizzando la console.

Dopo aver aggiunto un gateway, nella pagina AWS IoT Core per LoRaWAN Gateway della console AWS IoT, se selezioni il gateway aggiunto, è possibile visualizzare le `SubBands` e filtri `NetIdFilters` e `JoinEuiFilters` nella sezione Dettagli specifici di LoRaWAN della pagina dei dettagli del gateway.

Come configurare il gateway affinché utilizzi filtri e sottobande tramite l'API

Puoi utilizzare l'API CreateWirelessGateway utilizzata per creare un gateway per configurare le sottobande che desideri utilizzare e abilitare la funzionalità di filtraggio. Utilizzando dell'API `CreateWirelessGateway`, è possibile specificare le sottobande e i filtri come parte delle informazioni di configurazione del gateway fornite utilizzando il campo `LoRaWAN`. Di seguito viene illustrato il token di richiesta che include queste informazioni.

```
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
}
```

È possibile utilizzare anche l'API UpdateWirelessGateway per aggiornare i filtri ma non le sottobande. Se i valori `JoinEuiFilters` e `NetIdfilters` sono nulli, significa che non c'è alcun aggiornamento per i campi. Se i valori non sono nulli e vengono inclusi elenchi vuoti, viene applicato l'aggiornamento. Per ottenere i valori dei campi specificati, utilizza l'API GetWirelessGateway.

Aggiornare il firmware del gateway utilizzando il servizio CUPS con AWS IoT Core per LoRaWAN

Il software LoRa Basics Station che viene eseguito sul gateway fornisce la gestione delle credenziali e l'interfaccia di aggiornamento del firmware utilizzando il protocollo CUPS (Configuration and Update Server). Il protocollo CUPS fornisce un aggiornamento sicuro del firmware con firme ECDSA.

Dovrai aggiornare frequentemente il firmware del gateway. È possibile utilizzare il servizio CUPS con AWS IoT Core per LoRaWAN per fornire aggiornamenti firmware al gateway dove gli aggiornamenti possono anche essere firmati. Per aggiornare il firmware del gateway, è possibile utilizzare l'SDK o la CLI ma non la console.

Il completamento del processo può richiedere fino a 45 minuti. Può richiedere più tempo se si configura il gateway per la prima volta per connettersi ad AWS IoT Core per LoRaWAN. I produttori di gateway di solito forniscono i propri file di aggiornamento del firmware e le firme in modo da poterli utilizzare e procedere a Caricare il file del firmware in un bucket S3 e aggiungere un ruolo IAM.

Se non disponi dei file di aggiornamento del firmware, consulta Genera il file di aggiornamento del firmware e la firma per un esempio che è possibile utilizzare per adattarsi alla propria applicazione.

Per eseguire l'aggiornamento del firmware del gateway:

- Genera il file di aggiornamento del firmware e la firma
- Caricare il file del firmware in un bucket S3 e aggiungere un ruolo IAM
- Pianifica ed esegui l'aggiornamento del firmware utilizzando una definizione di processo

Genera il file di aggiornamento del firmware e la firma

I passaggi descritti in questa procedura sono facoltativi e dipendono dal gateway utilizzato.
I produttori di gateway forniscono il proprio aggiornamento del firmware sotto forma di file di aggiornamento o script e Basics Station esegue questo script in background. In questo caso, molto probabilmente troverai il file di aggiornamento del firmware nelle note di rilascio del gateway che stai utilizzando. È quindi possibile utilizzare il file o lo script di aggiornamento e procedere a Caricare il file del firmware in un bucket S3 e aggiungere un ruolo IAM.

Se non si dispone di questo script, di seguito vengono mostrati i comandi da eseguire per la generazione del file di aggiornamento del firmware. Gli aggiornamenti possono anche essere firmati per garantire che il codice non sia stato alterato o danneggiato e che i dispositivi eseguano codici pubblicati solo da autori attendibili.

In questa procedura, potrai:

- Generare il file di aggiornamento del firmware
- Generare firma per l'aggiornamento del firmware
- Esamina i passaggi successivi

Generare il file di aggiornamento del firmware

Il software LoRa Basics Station in esecuzione sul gateway è in grado di ricevere aggiornamenti firmware nella risposta CUPS. Se non disponi di uno script fornito dal produttore, fai riferimento al seguente script di aggiornamento del firmware scritto per il gateway RAKWireless basato su Raspberry Pi. Abbiamo uno script di base e la nuova stazione binaria, il file di versione, e `station.conf` sono collegati ad esso.

> **Note**
>
> Lo script è specifico del gateway RAKWireless, quindi dovrai adattarlo alla tua applicazione in base al gateway che stai utilizzando.

Script di base

Di seguito uno script di base di esempio per il gateway RAKWireless basato su Raspberry Pi. È possibile salvare i seguenti comandi in un file `base.sh` e quindi eseguire lo script nel terminale sul browser web di 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
```

Aggiungere script payload

Allo script di base, aggiungiamo il binario Basics Station, il version.txt che identifichi la versione a cui aggiornare, e `station.conf` in uno script chiamato `addpayload.sh`. Quindi, esegui questo 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
```

Dopo aver eseguito questi script, è possibile eseguire il seguente comando nel terminale per generare il file di aggiornamento del firmware, `fwstation`.

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

Generare firma per l'aggiornamento del firmware

Il software LoRa Basics Station fornisce aggiornamenti firmware firmati con firme ECDSA. Per supportare gli aggiornamenti firmati, è necessario:

- La firma che deve essere generata da una chiave privata ECDSA e meno di 128 byte.
- La chiave privata utilizzata per la firma e che deve essere memorizzata nel gateway con il nome file del formato `sig-%d.key`. Si consiglia di utilizzare il nome del file `sig-0.key`.
- Un CRC a 32 bit sulla chiave privata.

La firma e il CRC saranno passati alle API AWS IoT Core per LoRaWAN. Per generare i file precedenti, è possibile utilizzare il seguente script `gen.sh` che si ispira all'esempio basicstation nel repository 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
```

La chiave privata generata dallo script dovrebbe essere salvata nel gateway. Il file chiave è in formato binario.

```
./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/p2ssgXIPNCOgZr+NzeTLpX+WfBo5tYWbh5pQWN3AiBROen+XlIdMScv
AsfVfU/ZScJCalkVNZh4esyS8mNIgA==

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

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

Esamina i passaggi successivi

Ora che hai generato il firmware e la firma, vai all'argomento successivo per caricare il file del firmware `fwstation` per un bucket Amazon S3. Il bucket è un container che memorizza il file di aggiornamento del firmware come oggetto. È possibile aggiungere un ruolo IAM che consentirà al server CUPS l'autorizzazione per leggere il file di aggiornamento del firmware nel bucket S3.

Caricare il file del firmware in un bucket S3 e aggiungere un ruolo IAM

Puoi utilizzare Amazon S3 per creare un bucket, che è un container in grado di archiviare il file di aggiornamento del firmware. È possibile caricare il file nel bucket S3 e aggiungere un ruolo IAM che permette al server CUPS di leggere il file di aggiornamento dal bucket. Per ulteriori informazioni su Amazon S3, consulta Nozioni di base su Amazon S3.

Il file di aggiornamento del firmware che si desidera caricare dipende dal gateway in uso. Se è stata eseguita una procedura simile a quella descritta in Genera il file di aggiornamento del firmware e la firma, caricherai il `fwstation` generato eseguendo gli script.

Questa procedura dura circa 20 minuti.

Per caricare il file del firmware:

- Crea un bucket Amazon S3 e carica il file di aggiornamento
- Crea un ruolo IAM con autorizzazioni per leggere il bucket S3
- Esamina i passaggi successivi

Crea un bucket Amazon S3 e carica il file di aggiornamento

Creerai un bucket Amazon S3 utilizzando la AWS Management Console, quindi caricherai il file di aggiornamento del firmware nel bucket.

Creare un bucket S3

Per creare un bucket S3, apri la Amazon S3 console. Accedi se non lo hai già fatto e quindi esegui il passaggio seguente:

1. Seleziona Crea bucket.
2. Inserisci un nome univoco e significativo per il Nome bucket, (ad esempio, `iotwirelessfwupdate`). Per la convenzione di denominazione consigliata per il bucket, consulta https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucketnamingrules.html.
3. Assicurati di aver selezionato Regione AWS come quello usato per creare il gateway e il dispositivo LoRaWAN, e che l'impostazione Block all public access (Blocca tutti gli accessi pubblici) sia selezionata in modo che il bucket utilizzi le autorizzazioni predefinite.
4. Scegli Enable (Abilita) per Bucket versioning (Controllo delle versioni bucket) che ti aiuterà a mantenere più versioni del file di aggiornamento firmware nello stesso bucket.
5. Conferma che Server-side encryption (Crittografia lato server) è impostato su Disable (Disabilita) e scegli Create bucket (Crea bucket).

Carica il file di aggiornamento del firmware

Ora puoi visualizzare il bucket nell'elenco dei bucket visualizzato nella AWS Management Console. Scegli il tuo bucket e completa i seguenti passaggi per caricare il file.

1. Scegli il bucket e poi Upload (Carica).

2. Scegli Add file (Aggiungi file) e carica il file di aggiornamento del firmware. Se hai seguito la procedura descritta in Genera il file di aggiornamento del firmware e la firma, caricherai il `fwstation`, altrimenti carica il file fornito dal produttore del gateway.
3. Assicurati che tutte le impostazioni siano impostate sul valore predefinito. Assicurati che Predefined ACLs (ACL predefiniti) sia impostato su private (privato) e scegli Upload (Caricamento) per caricare il file.
4. Copia l'URI S3 del file caricato. Scegli il tuo bucket e vedrai il file che hai caricato visualizzato nell'elenco di Objects (Oggetti). Scegli il file e poi Copy S3 URI (Copiare URI S3). L'URI sarà: `s3://iotwirelessfwupdate/fwstation` se hai chiamato il tuo bucket in modo simile all'esempio descritto in precedenza (`fwstation`). Utilizza l'URI S3 durante la creazione del ruolo IAM.

Crea un ruolo IAM con autorizzazioni per leggere il bucket S3

Verrà ora creato un ruolo e una policy IAM che darà a CUPS l'autorizzazione a leggere il file di aggiornamento del firmware dal bucket S3.

Creare una policy IAM per il tuo ruolo

Per creare una policy IAM per il tuo ruolo di destinazione AWS IoT Core per LoRaWAN, apri Hub policy della console IAM) quindi completa questi passaggi:

1. Scegli Create policy (Crea policy), quindi scegli la scheda JSON.
2. Elimina qualsiasi contenuto dall'editor e incolla il documento relativo alla policy. La policy fornisce le autorizzazioni per accedere al bucket `iotwireless` e il file di aggiornamento del firmware `fwstation` memorizzato all'interno di un oggetto.

```
{
    "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. Scegli Review policy (Rivedi la policy) e in Name (Nome), inserisci un nome per questa policy (ad esempio, `IoTWirelessFwUpdatePolicy`). Dovrai utilizzare questo nome nella procedura successiva.
4. Scegli Crea policy.

Creare un ruolo IAM e collegarvi la policy

Ora creerai un ruolo IAM e lo collegherai alla policy creata in precedenza per accedere al bucket S3. Apri Roles hub of the IAM console (Hub ruoli della console IAM) e completa la procedura seguente:

1. Scegli Crea ruolo.
2. In Seleziona tipo di entità attendibile, scegli Altro Account AWS.
3. In Account ID (ID account), inserisci il tuo account Account AWS ID, quindi scegli Next: Permissions (Successivo: autorizzazioni).
4. Nella casella di ricerca, immetti il nome della policy IAM creata nella procedura precedente. Controlla la policy IAM (ad esempio, `IoTWirelessFwUpdatePolicy`) creata in precedenza nei risultati della ricerca e sceglila.
5. Scegliere Next: Tags (Successivo: Tag), quindi Next: Review (Successivo: Verifica).
6. Per Role Name (Nome ruolo), immetti un nome per il ruolo, ad esempio `IoTWirelessFwUpdateRole`, quindi scegli Create role (Crea ruolo).

Modifica la relazione di fiducia per il ruolo IAM

Nel messaggio di conferma visualizzato dopo avere eseguito il passaggio precedente, scegli il nome del ruolo creato per modificarlo. Modificherai il ruolo per aggiungere la seguente relazione di trust.

1. Nella sezione Summary (Riepilogo) del ruolo creato in precedenza, scegli la scheda Trust Relationships (Relazioni di trust), quindi scegli Edit Trust Relationship (Modifica relazione di trust).

2. In Policy Document (Documento policy), modifica la proprietà di `Principal` affinché appaia come il seguente esempio.

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

   Dopo aver modificato la proprietà `Principal`, il documento completo di policy dovrebbe essere simile al seguente.

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

3. Per salvare le modifiche e uscire, scegli Update Trust Policy (Aggiorna policy di attendibilità).
4. Ottieni l'ARN per il tuo ruolo. Scegli il tuo ruolo IAM e nella sezione Riepilogo vedrai un ARN ruolo, ad esempio `arn:aws:iam::123456789012:role/IoTWirelessFwUpdateRole`. Copia questo ARN Ruolo.

Esamina i passaggi successivi

Dopo aver creato il bucket S3 e un ruolo IAM che consente al server CUPS di leggere il bucket S3, passa all'argomento successivo per pianificare ed eseguire l'aggiornamento del firmware. Mantieni S3 URI e ARN ruolo che hai copiato in precedenza, in modo da poterli immettere per creare una definizione di attività che verrà eseguita per eseguire l'aggiornamento del firmware.

Pianifica ed esegui l'aggiornamento del firmware utilizzando una definizione di processo

È possibile utilizzare una definizione di processo per includere dettagli sull'aggiornamento del firmware e definire l'aggiornamento. AWS IoT Core per LoRaWAN fornisce un aggiornamento del firmware basato sulle informazioni dei seguenti tre campi associati al gateway.

- Station

  La versione e il tempo di compilazione del software Basics Station. Per identificare queste informazioni, è inoltre possibile generarle utilizzando il software Basics Station che viene eseguito dal gateway (ad esempio, `2.0.5(rpi/std) 2021-03-09 03:45:09`).
- PackageVersion

  La versione del firmware, specificata dal file `version.txt` nel gateway. Anche se queste informazioni potrebbero non essere presenti nel gateway, è consigliabile utilizzarle come metodo per definire la versione del firmware (ad esempio, `1.0.0`).
- Modello

  La piattaforma o il modello utilizzato dal gateway (ad esempio, Linux).

Questa procedura richiede 20 minuti.

Per completare questa procedura:

- Scarica la versione corrente in esecuzione sul tuo gateway
- Creare una definizione di attività Wireless gateway
- Esegui il processo di aggiornamento del firmware e monitora l'avanzamento

Scarica la versione corrente in esecuzione sul tuo gateway

Per determinare l'idoneità del gateway per un aggiornamento del firmware, il server CUPS controlla tutti e tre i campi `Station`, `PackageVersion` e `Model`, per una corrispondenza quando il gateway li presenta durante una richiesta CUPS. Quando si utilizza una definizione di attività, questi campi vengono memorizzati come parte del campo `CurrentVersion`.

Puoi utilizzare l'API AWS IoT Core per LoRaWAN o AWS CLI per ottenere il `CurrentVersion` per il gateway. I comandi seguenti mostrano come ottenere queste informazioni utilizzando la CLI.

1. Se è già stato eseguito il provisioning di un gateway, è possibile ottenere informazioni sul gateway utilizzando il comando get-wireless-gateway.

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

   L'esempio seguente mostra un output di esempio per questo 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. Utilizzando l'ID del gateway wireless riportato dal comando `get-wireless-gateway`, puoi utilizzare il comando get-wireless-gateway-firmware-informazioni per ottenere `CurrentVersion`.

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

   Di seguito viene mostrato un output di esempio per il comando, con le informazioni provenienti da tutti e tre i campi visualizzati dal `CurrentVersion`.

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

Creare una definizione di attività Wireless gateway

Quando si crea la definizione dell'attività, si consiglia di specificare la creazione automatica delle attività utilizzando il parametro AutoCreateTasks. `AutoCreateTasks` si applica a qualsiasi gateway che abbia una corrispondenza per tutti e tre i parametri menzionati in precedenza. Se questo parametro è disabilitato, i parametri devono essere assegnati manualmente al gateway.

È possibile creare la definizione del processo del gateway wireless utilizzando l'API AWS IoT Core per LoRaWAN o AWS CLI. I comandi seguenti mostrano come creare la definizione di processo utilizzando la CLI.

1. Crea un file, `input.json`, che conterrà le informazioni da passare all'API `CreateWirelessGatewayTaskDefinition`. Nel file `input.json`, fornisci le informazioni riportate di seguito:
   - UpdateDataSource

     Fornisci il collegamento all'oggetto contenente il file di aggiornamento del firmware caricato nel bucket S3. (ad esempio, `s3://iotwirelessfwupdate/fwstation`).
   - UpdateDataRole

     Fornisci il collegamento al ruolo ARN del ruolo IAM creato, che fornisce le autorizzazioni per leggere il bucket S3. (ad esempio, `arn:aws:iam::123456789012:role/IoTWirelessFwUpdateRole`).
   - SigKeyCRC e UpdateSignature

     Queste informazioni potrebbero essere fornite dal produttore del gateway, ma se è stata eseguita la procedura descritta in Genera il file di aggiornamento del firmware e la firma, queste informazioni si trovano quando si genera la firma.
   - CurrentVersion

     Fornisci il `CurrentVersion` che è stato ottenuto in precedenza eseguendo il comando `get-wireless-gateway-firmware-information` .

     ```
     cat input.json
     ```

     Di seguito viene mostrato il contenuto del file `input.json`.

     ```
     {
         "AutoCreateTasks": true,
     ```

```
    "Name": "FirmwareUpdate",
    "Update":
    {
        "UpdateDataSource" : "s3://iotwirelessfwupdate/fwstation",
        "UpdateDataRole" : "arn:aws:iam::123456789012:role/
IoTWirelessFwUpdateRole",
        "LoRaWAN" :
        {
            "SigKeyCrc": 3434210794,
            "UpdateSignature": "MEQCIDPY/p2ssgXIPNCOgZr+NzeTLpX
+WfBo5tYWbh5pQWN3AiBROen+XlIdMScvAsfVfU/ZScJCalkVNZh4esyS8mNIgA==",
            "CurrentVersion" :
            {
            "PackageVersion": "1.0.0",
            "Model": "rpi",
            "Station": "2.0.5(rpi/std) 2021-03-09 03:45:09"
            }
        }
    }
}
```

2. Passa il file `input.json` nel comando create-wireless-gateway-task-definition per creare la definizione dell'attività.

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

Di seguito viene mostrato l'output del comando.

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

Esegui il processo di aggiornamento del firmware e monitora l'avanzamento

Il gateway è pronto per ricevere l'aggiornamento del firmware e, una volta acceso, si connette al server CUPS. Quando il server CUPS trova una corrispondenza nella versione del gateway, pianifica un aggiornamento del firmware.

Un processo è una definizione di processo in corso. Una volta specificata la creazione automatica delle attività impostando `AutoCreateTasks` a `True`, l'attività di aggiornamento del firmware viene avviata non appena viene trovato un gateway corrispondente.

È possibile tenere traccia dello stato di avanzamento dell'attività utilizzando l'API `GetWirelessGatewayTask`. Quando si esegue il comando get-wireless-gateway-task per la prima volta, mostrerà lo stato dell'attività come `IN_PROGRESS`.

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

Di seguito viene mostrato l'output del 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 si esegue il comando la volta successiva, se l'aggiornamento del firmware ha effetto, mostrerà i campi aggiornati `Package`, `Version` e `Model` e lo stato dell'attività cambia in `COMPLETED`.

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

Di seguito viene mostrato l'output del 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"
}
```

In questo esempio, abbiamo mostrato l'aggiornamento del firmware utilizzando il gateway RAKWireless basato su Raspberry Pi. Lo script di aggiornamento del firmware interrompe la

BasicStation in esecuzione per archiviare l'aggiornamento `Package`, `Version` e i campi `Model` in modo che BasicStation debba essere riavviato.

```
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 l'aggiornamento del firmware non riesce, viene visualizzato lo stato `FIRST_RETRY` dal server CUPS e il gateway invia la stessa richiesta. Se il server CUPS non è in grado di connettersi al gateway dopo un `SECOND_RETRY`, mostrerà uno stato di `FAILED`.

Dopo l'attività precedente è stata `COMPLETED` o `FAILED`, elimina la vecchia attività utilizzando il comando delete-wireless-gateway-task prima di avviarne uno nuovo.

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

Scelta dei gateway per ricevere il traffico dati in downlink LoRaWAN

Quando si invia un messaggio di downlink da AWS IoT Core per LoRaWAN al dispositivo, è possibile scegliere i gateway che si desidera utilizzare per il traffico di dati in downlink. Per ricevere il traffico in downlink è possibile specificare un singolo gateway o scegliere da un elenco di gateway.

Come specificare l'elenco dei gateway

È possibile specificare un singolo gateway o l'elenco dei gateway da utilizzare per inviare un messaggio in downlink da AWS IoT Core per LoRaWAN sul proprio dispositivo utilizzando l'operazione API `SendDataToWirelessDevice`. Quando si richiama l'operazione API, specificare i seguenti parametri utilizzando l'oggetto `ParticipatingGateways` per i gateway.

> **Note**
>
> L'elenco dei gateway che si desidera utilizzare non è disponibile nella console AWS IoT. È possibile specificare questo elenco di gateway da utilizzare solo quando si utilizza l'operazione API `SendDataToWirelessDevice` o la CLI.

- `DownlinkMode`: indica se inviare il messaggio di downlink in modalità sequenziale o simultanea. Per i dispositivi di classe A, specificare `UsingUplinkGateway` per utilizzare solo i gateway scelti dalla precedente trasmissione di messaggi di uplink.
- `GatewayList`: l'elenco dei gateway che si desidera usare per inviare il traffico dati in downlink. Il payload del downlink verrà inviato ai gateway specificati con la frequenza specificata. Ciò è indicato mediante un elenco di oggetti `GatewayListItem`, formati da coppie `GatewayId` e `DownlinkFrequency`.
- `TransmissionInterval`: il tempo che AWS IoT Core per LoRaWAN attenderà prima di trasmettere il payload al gateway successivo.

> **Note**
>
> È possibile specificare questo elenco di gateway da utilizzare solo quando si invia il messaggio di downlink a un dispositivo wireless di classe B o C. Se si utilizza un dispositivo di classe A, il gateway scelto per l'invio del messaggio di uplink verrà utilizzato quando viene inviato un messaggio di downlink al dispositivo.

L'esempio seguente mostra come specificare tali parametri per il gateway. Il file `input.json` conterrà ulteriori dettagli. Per ulteriori informazioni sull'invio di un messaggio di downlink mediante l'operazione API `SendDataToWirelessDevice`, consulta Eseguire operazioni di accodamento dei messaggi di downlink utilizzando l'API.

> **Note**
>
> I parametri per specificare l'elenco dei gateway partecipanti non sono disponibili quando si invia un messaggio di downlink da AWS IoT Core per LoRaWANmediante la 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
```

Nell'esempio seguente viene mostrato il contenuto del file `input.json`.

Contenuto di 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
                    }
                ]
            }
        }
    }
}
```

L'output dell'esecuzione di questo comando genera un `MessageId` per il messaggio di downlink. In alcuni casi, anche se ricevi il `MessageId`, i pacchetti possono essere eliminati. Per ulteriori informazioni su come risolvere l'errore, consulta la sezione Risoluzione dei problemi relativi alla coda dei messaggi di downlink.

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

Ottenimento delle informazioni sull'elenco dei gateway partecipanti

È possibile ottenere informazioni sull'elenco dei gateway che partecipano alla ricezione del messaggio di downlink elencando i messaggi nella coda di downlink. Per elencare i messaggi, utilizzare l'API `ListQueuedMessages`.

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

L'esecuzione di questo comando restituisce informazioni sui messaggi in coda e sui relativi parametri.

Gestione di dispositivi con AWS IoT Core per LoRaWAN

Di seguito sono riportate alcune considerazioni importanti quando si utilizzano i dispositivi con AWS IoT Core per LoRaWAN. Per informazioni su come aggiungere un dispositivo a AWS IoT Core per LoRaWAN, consulta Integra i tuoi dispositivi su AWS IoT Core per LoRaWAN.

Considerazioni sui dispositivi

Quando si seleziona un dispositivo da utilizzare per comunicare con AWS IoT Core per LoRaWAN, considera quanto segue.

- Sensori disponibili
- Capacità della batteria
- Consumo energetico
- Costo
- Tipo di antenna e campo di trasmissione

Utilizzo di dispositivi con gateway qualificati per AWS IoT Core per LoRaWAN

I dispositivi utilizzati possono essere associati a gateway wireless qualificati per l'utilizzo con AWS IoT Core per LoRaWAN. Puoi trovare questi gateway e kit di sviluppo nel Catalogo dei dispositivi dei partner dei servizi AWS. Ti consigliamo inoltre di considerare la vicinanza di questi dispositivi ai gateway. Per ulteriori informazioni, consultare Utilizzo di gateway qualificati dal Catalogo dei dispositivi dei partner di AWS.

Versione di LoRaWAN

AWS IoT Core per LoRaWAN supporta tutti i dispositivi conformi alle specifiche LoRaWAN 1.0.x o 1.1, standardizzate da LoRa Alliance.

Modalità di attivazione

Prima che il tuo dispositivo LoRaWAN possa inviare dati uplink, devi completare un processo chiamato attivazione o procedura join. Per attivare il dispositivo, è possibile utilizzare OTAA (attivazione per via etere) o ABP (Attivazione per personalizzazione). Si consiglia di utilizzare OTAA per attivare il dispositivo in quanto vengono generate nuove chiavi di sessione per ogni attivazione, così da renderlo più sicuro.

Le specifiche del dispositivo wireless si basano sulla versione e sulla modalità di attivazione di LoRaWAN, che determina le chiavi root e le chiavi di sessione generate per ogni attivazione. Per ulteriori informazioni, consultare Aggiungi le specifiche del dispositivo wireless ad AWS IoT Core per LoRaWAN utilizzando la console.

Classi di dispositivi

I dispositivi LoRaWAN possono inviare messaggi di uplink in qualsiasi momento. L'ascolto dei messaggi di downlink consuma la capacità della batteria e riduce la durata della batteria. Il protocollo LoRaWAN specifica tre classi di dispositivi LoRaWAN.

- I dispositivi di classe A sono in modalità sleep per la maggior parte del tempo e ascoltano i messaggi di downlink solo per un breve periodo di tempo. Questi dispositivi sono per lo più sensori alimentati a batteria con durata fino a 10 anni.
- I dispositivi di classe B possono ricevere messaggi negli slot downlink pianificati. Questi dispositivi sono principalmente attuatori alimentati a batteria.
- I dispositivi di classe C non sono mai in modalità sleep e ascoltano continuamente i messaggi in arrivo, il che non causa molto ritardo nella ricezione dei messaggi. Questi dispositivi sono principalmente attuatori alimentati dalla rete.

Per ulteriori informazioni su queste considerazioni sui dispositivi wireless, fare riferimento alle risorse menzionate in Ulteriori informazioni su LoRaWAN.

Argomenti

Esecuzione della velocità di trasmissione dati adattiva (ADR) con AWS IoT Core per LoRaWAN

Per ottimizzare il consumo di energia di trasmissione del dispositivo e garantire al contempo che i messaggi dei dispositivi finali vengano ricevuti dai gateway, AWS IoT Core per LoRaWAN utilizza una velocità di trasmissione dati adattiva. La velocità di trasmissione dati adattiva indica ai dispositivi finali di ottimizzare la velocità dei dati, la potenza di trasmissione e il numero di ritrasmissioni, cercando di ridurre la percentuale di errori dei pacchetti ricevuti dai gateway. Ad esempio, se il dispositivo finale si trova vicino ai gateway, la velocità di trasmissione dati adattiva riduce la potenza di trasmissione e aumenta la velocità di trasmissione.

Argomenti

Come funziona la velocità di trasmissione dati adattiva (ADR)

Per abilitare l'ADR, il dispositivo deve impostare il bit ADR nell'intestazione del frame. Una volta impostato il bit ADR, AWS IoT Core per LoRaWAN invia il comando `LinkADRReq` MAC e i dispositivi rispondono con il comando `LinkADRAns` che include lo stato ACK del comando ADR. Una volta ricevuto l'ACK del comando ADR, il dispositivo seguirà le istruzioni ADR da AWS IoT Core per LoRaWAN e regolerà i valori dei parametri di trasmissione per ottenere la velocità di trasmissione ottimale.

L'algoritmo AWS IoT Core per LoRaWAN ADR utilizza le informazioni SINR nella cronologia dei metadati di uplink per determinare la potenza di trasmissione e la velocità di trasmissione dati ottimali da utilizzare per i dispositivi. L'algoritmo utilizza i 20 messaggi uplink più recenti che vengono avviati una volta impostato il bit ADR nell'intestazione del frame. Per determinare il numero di ritrasmissioni, l'algoritmo utilizza la percentuale di errore dei pacchetti (PER), che è una percentuale del numero totale di pacchetti persi. Quando si utilizza questo algoritmo, è possibile controllare solo l'intervallo delle velocità di trasmissione dati, ovvero i limiti minimo e massimo per le velocità di trasmissione dati.

Configurazione dei limiti di velocità dati (CLI)

Per impostazione predefinita, AWS IoT Core per LoRaWAN eseguirà l'ADR quando imposti il bit ADR nell'intestazione del frame del tuo dispositivo LoRaWAN. È possibile controllare i limiti minimi e massimi per la velocità di trasmissione dati durante la creazione di un profilo di servizio per i dispositivi LoRaWAN utilizzando l'operazione API AWS IoT Wireless `CreateServiceProfile` o il comando AWS CLI, `create-service-profile`.

> **Note**
>
> Non è possibile specificare i limiti massimi e minimi di velocità di trasmissione dati quando si crea un profilo di servizio dalla AWS Management Console. Può essere abilitato solo utilizzando l'API AWS IoT Wireless o la AWS CLI.

Per specificare i limiti minimo e massimo per la velocità dei dati, utilizza i parametri `DrMin` e `DrMax` con l'operazione API `CreateServiceProfile`. I limiti di velocità dati minimo e massimo predefiniti sono 0 e 15. Ad esempio, il seguente comando CLI imposta un limite minimo di velocità dati di 3 e un limite massimo di 12.

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

L'esecuzione di questo comando genera un ID e un nome della risorsa Amazon (ARN) per il profilo del servizio.

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

È possibile ottenere i valori dei parametri specificati utilizzando l'operazione API AWS IoT Wireless `GetServiceProfile` o il comando AWS CLI, `get-service-profile`.

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

L'esecuzione di questo comando genera i valori per i parametri del profilo di servizio.

```
{
    "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 hai creato più profili, puoi utilizzare l'operazione API, `ListServiceProfiles`, o il comando AWS CLI, `list-service-profiles`, per elencare i profili di servizio nel tuo Account AWS, quindi utilizzare l'API `GetServiceProfile` o il comando CLI `get-service-profile` per recuperare il profilo di servizio per il quale hai personalizzato i limiti di velocità dei dati.

Gestione della comunicazione tra i dispositivi LoRaWAN e AWS IoT

Dopo aver collegato il tuo dispositivo LoRaWAN a AWS IoT Core per LoRaWAN, i dispositivi possono iniziare a inviare messaggi al cloud. Si definiscono messaggi di uplink i messaggi inviati dal dispositivo e ricevuti da AWS IoT Core per LoRaWAN. I dispositivi LoRaWAN possono inviare in qualsiasi momento messaggi di uplink, che vengono successivamente inoltrati ad altri Servizio AWS e applicazioni ospitate nel cloud. I messaggi inviati da AWS IoT Core per LoRaWAN e altri applicazioni e Servizio AWS ai tuoi dispositivi sono chiamati messaggi di downlink.

Di seguito viene illustrato come visualizzare e gestire i messaggi di uplink e downlink inviati tra i dispositivi e il Cloud. Puoi mantenere una coda dei messaggi di downlink e inviare questi messaggi ai dispositivi nell'ordine in cui sono stati aggiunti alla coda.

Argomenti

Visualizza il formato dei messaggi di uplink inviati dai dispositivi LoRaWAN

Dopo aver collegato il dispositivo LoRaWAN ad AWS IoT Core per LoRaWAN, potrai visualizzare il formato del messaggio di uplink che riceverai dal tuo dispositivo wireless.

Prima di poter visualizzare i messaggi di uplink

È necessario aver inserito il dispositivo wireless e collegato il dispositivo ad AWS IoT in modo che possa trasmettere e ricevere dati. Per informazioni su come eseguire l'onboarding del dispositivo per AWS IoT Core per LoRaWAN, consulta Integra i tuoi dispositivi su AWS IoT Core per LoRaWAN.

Cosa contengono i messaggi di uplink?

Dispositivi LoRaWAN connessi ad AWS IoT Core per LoRaWAN attraverso i gateway LoRaWAN. Il messaggio di uplink ricevuto dal dispositivo conterrà le seguenti informazioni.

- Dati di payload corrispondenti al messaggio di payload crittografato inviato dal dispositivo wireless.
- Metadati wireless che includono:
  - Informazioni sul dispositivo, ad esempio DevEui, la velocità dati e il canale di frequenza in cui il dispositivo è in funzione.
  - Parametri aggiuntivi opzionali e informazioni sul gateway per i gateway connessi al dispositivo. I parametri del gateway includono EUI del gateway, SNR e RSSi.

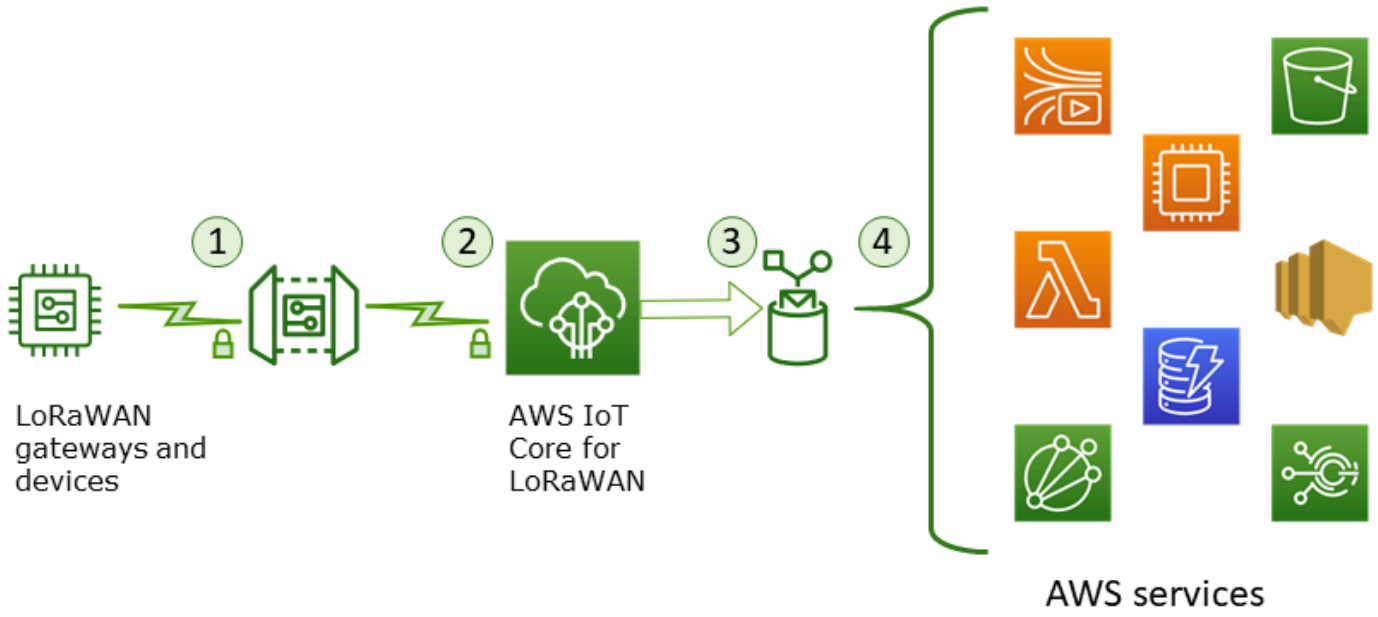
  Utilizzando i metadati wireless, è possibile ottenere informazioni utili sul dispositivo wireless e sui dati trasmessi tra il dispositivo e AWS IoT. Ad esempio, puoi utilizzare il parametro `AckedMessageId` per verificare se l'ultimo messaggio downlink confermato è stato ricevuto dal dispositivo. Facoltativamente, se si sceglie di includere le informazioni sul gateway, è possibile stabilire se si desidera passare a un canale gateway più potente e più vicino al dispositivo.

Come visualizzare i messaggi di uplink?

Dopo aver effettuato l'onboarding del dispositivo, è possibile utilizzare il Client di prova MQTT sulla pagina Test della console AWS IoT per sottoscrivere l'argomento specificato durante la creazione

della destinazione. Potrai iniziare a visualizzare messaggi dopo che il dispositivo sarà connesso e avrà iniziato ad inviare i dati di payload.

Questo diagramma individua gli elementi chiave di un sistema LoRaWAN connesso ad AWS IoT Core per LoRaWAN, che mostra il piano dati primario e il modo in cui i dati fluiscono attraverso il sistema.



Quando il dispositivo wireless inizia a inviare dati di uplink, AWS IoT Core per LoRaWAN avvolge le informazioni dei metadati wireless con il payload, inviandole quindi alle tue applicazioni AWS.

Esempio di messaggio di uplink

Nell'esempio seguente viene illustrato il formato del messaggio di uplink ricevuto dal dispositivo.

```
{
    "WirelessDeviceId": "5b58245e-146c-4c30-9703-0ca942e3ff35",
    "PayloadData": "Cc48AAAAAAAAAAA=",
    "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": "80029cfffe5cf1cc",
                    "Snr": -29,
                    "Rssi": 9.75
             }
             ],
            "MIC": "7255cb07",
            "MType": "UnconfirmedDataUp",
            "Major": "LoRaWANR1",
            "Modulation": "LORA",
            "PolarizationInversion": false,
            "SpreadingFactor": 12,
            "Timestamp": "2021-05-03T03:24:29Z"

        }
    }
}
```

Esclusione dei metadati gateway dai metadati uplink

Se desideri escludere le informazioni relative ai metadati del gateway dai metadati dell'uplink, disabilita il parametro AddGwMetadata quando crei il profilo di servizio. Per informazioni sulla disattivazione di questo parametro, consulta Aggiungi profili di servizio.

In questo caso, non verrà visualizzata la sezione `Gateways` nei metadati uplink, come illustrato nell'esempio seguente.

```
{
    "WirelessDeviceId": "0d9a439b-e77a-4573-a791-49d5c0f4db95",
    "PayloadData": "AAAAAAAA//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"
    }
  }
}
```

Accodamento dei messaggi di downlink da inviare ai dispositivi LoRaWAN

Le applicazioni ospitate su cloud e altri Servizio AWS possono inviare messaggi di downlink ai tuoi dispositivi wireless. Si definiscono messaggi di downlink i messaggi inviati da AWS IoT Core per LoRaWAN sul tuo dispositivo wireless. Puoi pianificare e inviare i messaggi di downlink per ogni dispositivo che hai inserito in AWS IoT Core per LoRaWAN.

Se vuoi inviare un messaggio di downlink a molteplici dispositivi, puoi utilizzare un gruppo multicast. I dispositivi di un gruppo multicast condividono lo stesso indirizzo multicast, che viene quindi distribuito a un intero gruppo di dispositivi destinatari. Per ulteriori informazioni, consultare Creazione di gruppi multicast per inviare un payload di downlink a più dispositivi.

Come funziona una coda di messaggi di downlink

La classe del dispositivo LoRaWAN determina il modo in cui i messaggi nella coda vengono inviati al dispositivo. I dispositivi di classe A inviano un messaggio di uplink a AWS IoT Core per LoRaWAN per indicare che il dispositivo è disponibile alla ricezione di messaggi di downlink. I dispositivi di classe B possono ricevere messaggi negli slot di downlink pianificati. I dispositivi di classe C possono ricevere messaggi di downlink in qualsiasi momento. Per ulteriori informazioni sulle classi dei dispositivi, consulta la sezione Classi di dispositivi.

Di seguito viene illustrato come i messaggi vengono accodati e inviati ai dispositivi di classe A.

1. AWS IoT Core per LoRaWAN esegue il buffer del messaggio di downlink aggiunto alla coda con la porta frame, i dati di payload e i parametri della modalità di ricevuta specificati utilizzando la console AWS IoT o l'API AWS IoT Wireless.
2. Il dispositivo LoRaWAN invia un messaggio di uplink per indicare che è online e può iniziare a ricevere messaggi di downlink.
3. Se hai aggiunto più di un messaggio di downlink alla coda, AWS IoT Core per LoRaWAN invia il primo messaggio di downlink presente nella coda al dispositivo con il flag di ricevuta (ACK) impostato.

4. Il dispositivo invia un messaggio di uplink a AWS IoT Core per LoRaWAN immediatamente oppure rimane in sospeso fino al successivo messaggio di uplink e include il flag ACK nel messaggio.
5. Quando riceve il messaggio di uplink con il flag ACK, AWS IoT Core per LoRaWAN cancella il messaggio di downlink dalla coda, indicando che il dispositivo ha ricevuto correttamente il messaggio di downlink. Se dopo tre verifiche il flag ACK non è presente nel messaggio di uplink, il messaggio viene eliminato.

Eseguire operazioni di accodamento dei messaggi di downlink utilizzando la console

Puoi utilizzare la AWS Management Console per accodare i messaggi di downlink e cancellare i singoli messaggi o l'intera coda, secondo necessità. Per i dispositivi di classe A, dopo che il dispositivo invia un messaggio di uplink per indicare che è online, i messaggi in coda vengono inviati al dispositivo. Dopo l'invio, il messaggio viene automaticamente cancellato dalla coda.

Accodamento dei messaggi di downlink

Per creare una coda di messaggi di downlink

1. Accedi all'hub dei dispositivi della console AWS IoT e scegli il dispositivo per il quale desideri accodare i messaggi di downlink.
2. Nella sezione Downlink messages (Messaggi di downlink) della pagina dei dettagli del dispositivo, scegli Queue downlink messages (Accoda messaggi di downlink).
3. Per configurare il messaggio di downlink, specifica i seguenti parametri:
   - FPort: scegli la porta frame per la comunicazione tra il dispositivo e AWS IoT Core per LoRaWAN.
   - Payload: specifica il messaggio di payload che desideri inviare al dispositivo. La dimensione massima del payload è di 242 byte. Se la velocità dati adattiva (ADR) è abilitata, AWS IoT Core per LoRaWAN la utilizza per scegliere la velocità dati ottimale per le dimensioni del payload. Puoi ottimizzare ulteriormente la velocità dati in base alle tue esigenze.
   - Modalità ricevuta: conferma se il dispositivo ha ricevuto il messaggio di downlink. Se un messaggio richiede questa modalità, verrà visualizzato un messaggio di uplink con il flag ACK nel flusso dei dati e il messaggio verrà cancellato dalla coda.
4. Per aggiungere il messaggio di downlink alla coda, scegli Submit (Invia).

Ora il messaggio di downlink è stato aggiunto alla coda. Se non visualizzi il messaggio o si verifica un errore, puoi risolvere il problema come descritto in Risoluzione dei problemi relativi alla coda dei messaggi di downlink.

> **Note**
>
> Dopo che il messaggio di downlink è stato aggiunto alla coda, i parametri FPort, Payload e Acknowledge mode (Modalità ricevuta) non possono più essere modificati. Se vuoi inviare un messaggio di downlink con valori diversi per questi parametri, devi eliminare il messaggio e accodare un nuovo messaggio di downlink con i valori dei parametri aggiornati.

La coda elenca i messaggi di downlink aggiunti. Per visualizzare il payload per i messaggi di uplink e downlink scambiati tra i dispositivi e AWS IoT Core per LoRaWAN, puoi utilizzare l'analizzatore di rete. Per ulteriori informazioni, consultare Monitoraggio del parco istanze di risorse wireless in tempo reale utilizzando l'analizzatore di rete.

Elenco dei messaggi di downlink in coda

Il messaggio di downlink che hai creato viene aggiunto alla coda. Ogni successivo messaggio di downlink viene aggiunto alla coda dopo questo messaggio. Puoi visualizzare un elenco dei messaggi di downlink nella sezione Downlink messages (Messaggi di downlink) della pagina dei dettagli del dispositivo. Dopo avere ricevuto un messaggio di uplink, i messaggi vengono inviati al dispositivo. Dopo che un messaggio di downlink è stato ricevuto dal dispositivo, verrà rimosso dalla coda. Il messaggio successivo si sposta quindi verso l'alto nella coda dei messaggi da inviare al dispositivo.

Eliminazione di singoli messaggi di downlink o cancellazione dell'intera coda

Ogni messaggio di downlink viene cancellato automaticamente dalla coda dopo che è stato inviato al dispositivo. Puoi anche eliminare singoli messaggi o cancellare l'intera coda dei messaggi di downlink. Queste operazioni non possono essere annullate.

- Se nella coda trovi messaggi che non vuoi inviare, selezionali e scegli Delete (Elimina).
- Se non vuoi inviare alcuno dei messaggi in coda al tuo dispositivo, puoi cancellare l'intera coda scegliendo Clear downlink queue (Cancella coda di downlink).

Eseguire operazioni di accodamento dei messaggi di downlink utilizzando l'API

Puoi utilizzare l'API AWS IoT Wireless per accodare i messaggi di downlink e cancellare i singoli messaggi o l'intera coda, secondo necessità.

Accodamento dei messaggi di downlink

Per creare una coda di messaggi di downlink tramite l'API, utilizza l'operazione API `SendDataToWirelessDevice` o il comando della CLI `send-data-to-wireless-device`.

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

L'output dell'esecuzione di questo comando genera un `MessageId` per il messaggio di downlink. In alcuni casi, anche se ricevi il `MessageId`, i pacchetti possono essere eliminati. Per ulteriori informazioni su come risolvere l'errore, consulta la sezione Risoluzione dei problemi relativi alla coda dei messaggi di downlink.

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

Elenco dei messaggi di downlink in coda

Per elencare tutti i messaggi di downlink presenti nella coda, utilizza l'operazione API `ListQueuedMessages` o il comando della CLI `list-queued-messages`.

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

Per impostazione predefinita, durante l'esecuzione di questo comando vengono visualizzati un massimo di 10 messaggi di downlink.

Rimozione di singoli messaggi di downlink o cancellazione dell'intera coda

Per rimuovere singoli messaggi dalla coda o per cancellare l'intera coda, utilizza l'operazione API `DeleteQueuedMessages` o il comando della CLI `delete-queued-messages`.

- Per rimuovere i singoli messaggi, fornisci il `messageID` dei messaggi che desideri rimuovere per il dispositivo wireless, specificato dal `wirelessDeviceId`.
- Per cancellare l'intera coda di downlink, specifica il `messageID` come `*` per il dispositivo wireless, specificato dal `wirelessDeviceId`.

Risoluzione dei problemi relativi alla coda dei messaggi di downlink

Ecco alcune cose da controllare se i risultati che vedi sono diversi da quelli che ti aspetti.

- I messaggi di downlink non vengono visualizzati nella console AWS IoT

  Se non visualizzi un messaggio di downlink nella coda dopo averlo aggiunto come descritto in Eseguire operazioni di accodamento dei messaggi di downlink utilizzando la console, potrebbe dipendere dal fatto che il dispositivo non ha completato un processo chiamato procedura di attivazione o congiungimento. Questa procedura viene completata quando il dispositivo viene inserito in AWS IoT Core per LoRaWAN. Per ulteriori informazioni, consultare Aggiungi le specifiche del dispositivo wireless ad AWS IoT Core per LoRaWAN utilizzando la console.

  Dopo avere inserito il dispositivo in AWS IoT Core per LoRaWAN, puoi monitorarlo per verificare se l'accesso e il congiungimento sono riusciti utilizzando l'analizzatore di rete o Amazon CloudWatch. Per ulteriori informazioni, consultare Strumenti di monitoraggio.
- Pacchetti di messaggi di downlink mancanti quando si utilizza l'API

  Quando utilizzi l'operazione API `SendDataToWirelessDevice`, l'API restituisce un `MessageId` univoco. Tuttavia, non puoi verificare se il dispositivo LoRaWAN abbia ricevuto il messaggio di downlink. I pacchetti di downlink possono essere eliminati se, ad esempio, il dispositivo non ha completato la procedura di congiungimento. Per ulteriori informazioni su come risolvere questo errore, consulta la sezione precedente.
- Errore ARN mancante durante l'invio del messaggio di downlink

  Quando invii un messaggio di downlink dalla coda al dispositivo, potresti ricevere un errore di Amazon Resource Name (ARN) mancante. L'errore potrebbe verificarsi perché non è stata specificata correttamente la destinazione per il dispositivo che riceve il messaggio di downlink. Per risolvere questo errore, controlla i dettagli di destinazione del dispositivo.

Gestione del traffico LoRaWAN da reti di dispositivi LoRaWAN pubbliche (Everynet)

Puoi connettere i tuoi dispositivi LoRaWAN al cloud in pochi minuti utilizzando reti LoRaWAN disponibili pubblicamente. AWS IoT Core per LoRaWAN ora supporta la copertura di rete di Everynet negli Stati Uniti e nel Regno Unito. Quando utilizzi la rete pubblica, per ogni dispositivo ti verrà addebitato mensilmente un costo per la connessione alla rete pubblica. Il prezzo si applica a tutte le Regioni AWS in cui è disponibile la connettività di rete pubblica. Per ulteriori informazioni sui prezzi di questa funzionalità, consulta la pagina dei prezzi di AWS IoT Core.

> **Important**
>
> La rete pubblica è gestita e fornita come servizio direttamente da Everynet. Prima di utilizzare questa funzionalità, consulta i termini del servizio AWS applicabili. Inoltre, se utilizzi una rete pubblica tramite AWS IoT Core per LoRaWAN, alcune informazioni sul dispositivo LoRaWAN, come `DevEUI` e `JoinEUI`, verranno replicate nelle regioni in cui AWS IoT Core per LoRaWAN è disponibile.

AWS IoT Core per LoRaWAN supporta la rete LoRaWAN pubblica in base alle specifiche LoRa Alliance per il roaming, come descritto nel documento LoRaWAN Backend Interfaces 1.0 Specification. È possibile utilizzare la funzionalità di rete pubblica per connettere i dispositivi terminali che si trovano all'esterno della rete privata. Per supportare questa funzionalità, AWS IoT Core per LoRaWAN collabora con EveryNet per offrire una copertura radio estesa.

Vantaggi dell'utilizzo di una rete LoRaWAN pubblica

I dispositivi LoRaWAN possono utilizzare una rete pubblica per connettersi al cloud, con conseguente riduzione dei tempi di implementazione e dei tempi e costi necessari per mantenere una rete LoRaWAN privata.

L'utilizzo di una rete LoRaWAN pubblica offre vantaggi come l'estensione della copertura, l'esecuzione core senza rete radio e la densificazione della copertura. È possibile utilizzare questa funzionalità per:

- Fornire copertura ai dispositivi quando si spostano all'esterno della rete privata, ad esempio Dispositivo A nella figura mostrata nella sezione Architettura del supporto della rete LoRaWAN pubblica.

- Estendere la copertura ai dispositivi che non dispongono di un gateway LoRa a cui connettersi, come Dispositivo B nella figura mostrata nella sezione Architettura del supporto della rete LoRaWAN pubblica. Il dispositivo può quindi utilizzare il gateway fornito dal partner per connettersi alla rete privata.

I dispositivi LoRaWAN possono utilizzare una rete pubblica per connettersi al cloud utilizzando la funzionalità di roaming, con conseguente riduzione dei tempi di implementazione e dei tempi e costi necessari per mantenere una rete LoRaWAN privata.

Le sezioni seguenti descrivono l'architettura di supporto della rete pubblica, come funziona il supporto della rete LoRaWAN pubblica e come utilizzare questa funzionalità.

Argomenti

Funzionamento del supporto della rete pubblica LoRaWAN

AWS IoT Core per LoRaWAN supporta la funzionalità di roaming passivo, in base alle specifiche di LoRa Alliance. Con il roaming passivo, il processo di roaming è completamente trasparente per il dispositivo finale. I dispositivi finali che funzionano in roaming al di fuori della rete privata possono connettersi ai gateway di tale rete e scambiare dati di uplink e downlink utilizzando il server di applicazioni. I dispositivi rimangono connessi alla rete privata durante l'intero processo di roaming.

> **Note**
>
> AWS IoT Core per LoRaWAN supporta solo la funzionalità stateless del roaming passivo. La modalità handover roaming non è supportata. In modalità handover roaming, il dispositivo passerà a un operatore differente quando si sposta all'esterno della rete privata.

Argomenti

Concetti relativi alla rete LoRaWAN pubblica

I seguenti concetti sono utilizzati dalla funzione di rete pubblica supportata da AWS IoT Core per LoRaWAN.

LoRaWAN Network Server (LNS)

Un LNS è un server privato autonomo che può essere eseguito in locale o configurato come un servizio basato sul cloud. AWS IoT Core per LoRaWAN è un LNS che offre servizi sul cloud.

Home network server (hNS)

La rete privata è la rete a cui appartiene il dispositivo. L'home network server (hNS) è un LNS in cui AWS IoT Core per LoRaWAN archivia i dati di provisioning del dispositivo, come `DevEUI`, `AppEUI` e le chiavi di sessione.

Visited network server (vNS)

La rete visitata è la rete da cui il dispositivo riceve la copertura quando abbandona la rete privata. Il visited network server (vNS) è un LNS che dispone di un accordo commerciale e tecnico con hNS per essere in grado di servire il dispositivo finale. Il partner AWS, Everynet, funge da rete visitata per fornire copertura.

Serving network server (sNS)

Il serving network server (sNS) è un LNS che gestisce i comandi MAC per il dispositivo. Per ciascuna sessione LoRa può esserci un solo sNS.

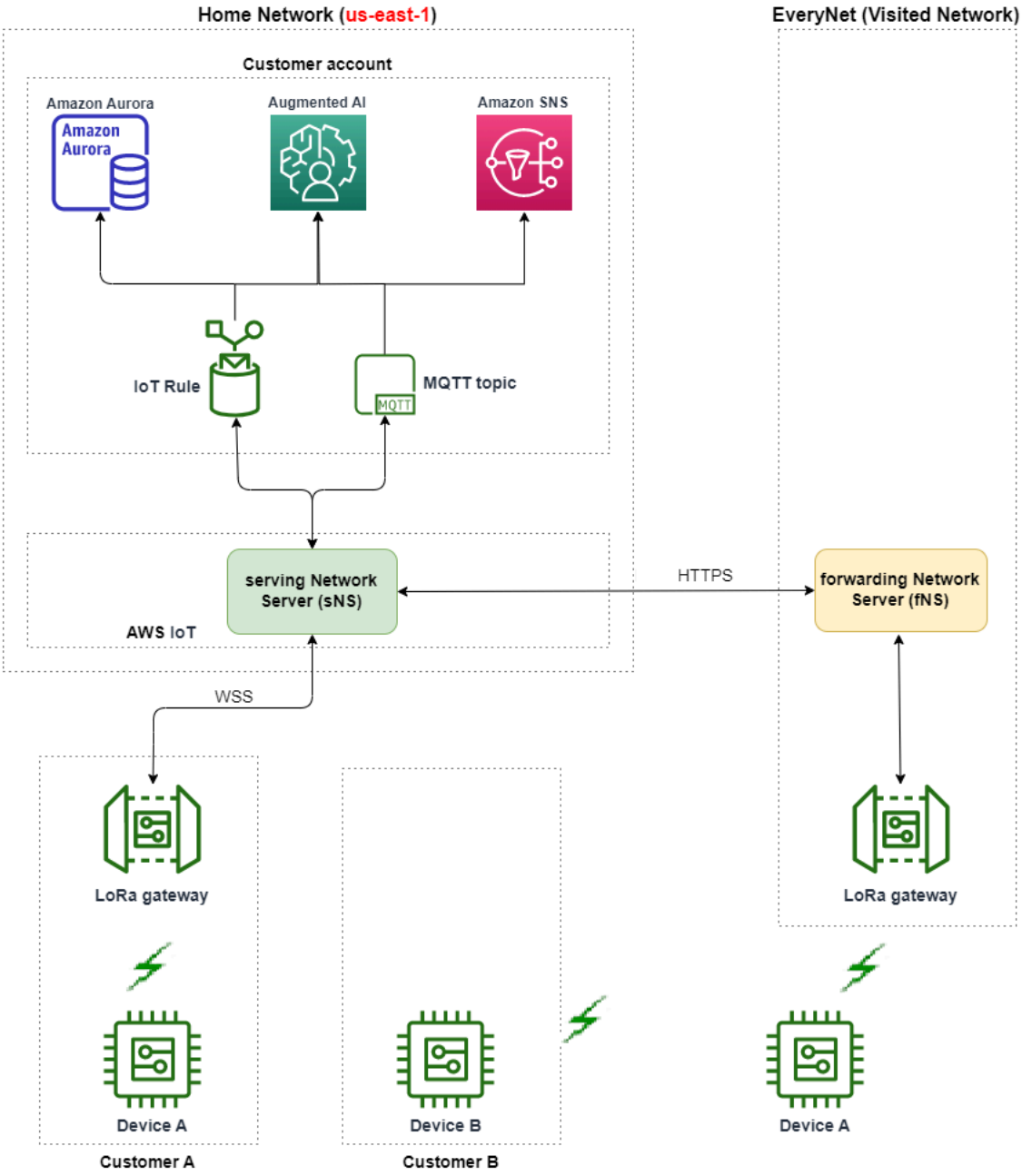
Forwarding network server (fNS)

Il forwarding network server (fNS) è un LNS che gestisce i gateway radio. In una sessione LoRa possono essere coinvolti zero o più fNS. Questo server di rete gestisce l'inoltro dei pacchetti di dati ricevuti dal dispositivo nella rete privata.

Architettura del supporto della rete LoRaWAN pubblica

Il seguente diagramma dell'architettura mostra come AWS IoT Core per LoRaWAN collabora con Everynet per fornire la connettività della rete pubblica. In questo caso, Dispositivo A è connesso ad hNS (home network server) fornito da AWS IoT Core per LoRaWAN tramite un gateway LoRa. Quando Dispositivo A si sposta all'esterno della rete privata, accede a una rete visitata ed è coperto dal visited network server (vNS) fornito da Everynet. Il vNS estende anche la copertura a Dispositivo B che non dispone di un gateway LoRa a cui connettersi.

Puoi visualizzare le informazioni sulla copertura della rete pubblica nella console AWS IoT come descritto nella sezione seguente.



AWS IoT Core per LoRaWAN utilizza una funzionalità hub roaming, in conformità con la LoRa Alliance LoRaWAN Roaming Hub Technical Recommendation. L'hub roaming fornisce un endpoint per Everynet per instradare il traffico ricevuto dal dispositivo finale. In questo caso, Everynet funge da forwarding network server (fNS) per inoltrare il traffico ricevuto dal dispositivo. Utilizza un'API RESTful HTTP, come definito dalle specifiche LoRa Alliance.

> **Note**
>
> Se il dispositivo si sposta dalla rete privata ed entra in una località in cui sia la rete privata sia Everynet possono offrire copertura, utilizzerà una policy first-come-first-serve per determinare se connettersi al gateway LoRa o al gateway di Everynet.

Quando si visita una rete pubblica, hNS e serving network server (sNS) sono separati. I pacchetti in uplink e in downlink vengono quindi scambiati tra sNS e hNS.

Come utilizzare il supporto della rete pubblica

Per abilitare il supporto della rete pubblica di Everynet, devi abilitare determinati parametri di roaming durante la creazione di un profilo del servizio. In questa versione beta, questi parametri sono disponibili quando si utilizza l'API AWS IoT Wireless o AWS CLI. Nelle sezioni seguenti vengono illustrati i parametri che occorre abilitare e viene descritto come abilitare la rete pubblica utilizzando AWS CLI.

> **Note**
>
> È possibile abilitare il supporto della rete pubblica solo durante la creazione di un nuovo profilo del servizio. Non è possibile aggiornare un profilo esistente per abilitare la rete pubblica utilizzando questi parametri.

Argomenti

Parametri di roaming

Specifica i seguenti parametri durante la creazione di un profilo del servizio per il dispositivo. Specifica questi parametri durante l'aggiunta di un profilo del servizio dall'hub Profili della console AWS IoT o l'utilizzo dell'operazione API AWS IoT Wireless, `CreateServiceProfile` o del comando AWS CLI, `create-service-profile`.

> **Note**
>
> AWS IoT Core per LoRaWAN non supporta la modalità handover roaming. Durante la creazione del profilo del servizio, non è possibile abilitare il parametro `HrAllowed` che specifica se utilizzare handover roaming.

- Attivazione del roaming consentita (`RaAllowed`): questo parametro specifica se abilitare l'attivazione del roaming. L'attivazione del roaming consente a un dispositivo finale di attivarsi sotto la copertura di un vNS. Quando si utilizza la funzionalità di roaming, `RaAllowed` deve essere impostato su `true`.
- Roaming passivo consentito (`PrAllowed`): questo parametro specifica se abilitare il roaming passivo. Quando si utilizza la funzionalità di roaming, `PrAllowed` deve essere impostato su `true`.

Abilitazione del supporto della rete pubblica per i dispositivi

Per abilitare il supporto della rete pubblica LoRaWAN sui tuoi dispositivi, esegui la seguente procedura.

> **Note**
>
> Puoi abilitare la funzionalità della rete pubblica solo per i dispositivi OTAA. Questa funzionalità non è supportata per i dispositivi che utilizzano ABP come metodo di attivazione.

1. Creazione del profilo del servizio con parametri di roaming

   Crea un profilo del servizio abilitando i parametri di roaming.

   > **Note**
   >
   > Quando crei un profilo per il dispositivo che assocerai a questo profilo del servizio, ti consigliamo di specificare un valore elevato per il parametro `RxDelay1`, almeno superiore a 2 secondi.

   - Utilizzo della console di AWS IoT

Vai all'hub Profili della console AWS IoT e scegli Aggiungi profilo del servizio. Quando crei il profilo, scegli Abilita rete pubblica.

- Utilizzo dell'API AWS IoT Wireless

  Per abilitare il roaming durante la creazione di un profilo del servizio, utilizza l'operazione API CreateServiceProfile o il comando dell'interfaccia a riga di comando `create-service-profile`, come mostrato nell'esempio seguente.

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

  L'esecuzione di questo comando restituisce l'ARN e l'ID del profilo del servizio come output.

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

2. Verifica dei parametri di roaming nel profilo del servizio

Per controllare i parametri di roaming specificati, è possibile visualizzare il profilo del servizio nella console o utilizzare il comando dell'interfaccia a riga di comando `get-service-profile`, come mostrato nell'esempio seguente.

- Utilizzo della console di AWS IoT

  Passa all'hub Profili della console AWS IoT e scegli il profilo creato. Nella scheda Configurazione del profilo della pagina dei dettagli, i parametri RAAllowed e PRAllowed sono impostati su `true`.

- Utilizzo dell'API AWS IoT Wireless

  Per visualizzare i parametri di roaming abilitati, utilizza l'operazione API GetServiceProfile o il comando dell'interfaccia a riga di comando `get-service-profile`, come mostrato nell'esempio seguente.

```
aws iotwireless get-service-profile \
```

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

L'esecuzione di questo comando restituisce i dettagli del profilo del servizio come output, inclusi i valori per i parametri di 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. Collegamento del profilo del servizio ai dispositivi

   Collega il profilo del servizio creato con i parametri di roaming ai dispositivi finali. Puoi anche creare un profilo del dispositivo e aggiungere una destinazione per i dispositivi wireless. Utilizza questa destinazione per instradare i messaggi in uplink inviati dal dispositivo. Per ulteriori informazioni sulla creazione di profili del dispositivo e di una destinazione, consultare Aggiungi profili di dispositivo e Aggiunta di destinazioni a AWS IoT Core per LoRaWAN.

   - Onboarding di nuovi dispositivi

     Se non hai già eseguito l'onboarding di nuovi dispositivi, specifica il profilo del servizio da utilizzare durante l'aggiunta del dispositivo ad AWS IoT Core per LoRaWAN. Nel comando

seguente viene illustrato come utilizzare il comando dell'interfaccia a riga di comando `create-wireless-device` per aggiungere un dispositivo utilizzando l'ID del profilo del servizio creato. Per informazioni sull'aggiunta del profilo del servizio mediante la console, consultare Aggiungi le specifiche del dispositivo wireless ad AWS IoT Core per LoRaWAN utilizzando la console.

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

Nell'esempio seguente viene mostrato il contenuto del file *createdevice.json*.

Contenuto di 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"
    },
}
```

L'output dell'esecuzione di questo comando produce l'ARN e l'ID del dispositivo wireless.

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

- Aggiornamento di dispositivi esistenti

  Se hai già eseguito l'onboarding dei dispositivi, puoi aggiornare i dispositivi wireless esistenti per utilizzare questo profilo del servizio. Nel comando seguente viene illustrato come utilizzare

il comando dell'interfaccia a riga di comando `update-wireless-device` per aggiornare un dispositivo utilizzando l'ID del profilo del servizio creato.

```
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"
```

Il comando non produce output. Puoi utilizzare l'API `GetWirelessDevice` o il comando dell'interfaccia a riga di comando `get-wireless-device` per ottenere le informazioni aggiornate.

4. Collegamento del dispositivo al cloud mediante Everynet

Poiché il roaming è stato abilitato, il dispositivo deve ora eseguire un join per ottenerne un nuovo `DevAddr`. Se utilizzi OTAA, il dispositivo LoRaWAN invia una richiesta di join e il server di rete può consentire la richiesta. Può quindi connettersi al Cloud AWS utilizzando la copertura di rete fornita da Everynet. Per istruzioni su come eseguire la procedura di attivazione o il join per il dispositivo, consultare la documentazione del dispositivo.

> **Note**
>
> - Puoi attivare la funzionalità di roaming e connetterti alla rete pubblica solo per i dispositivi che utilizzano OTAA come metodo di attivazione. I dispositivi ABP non sono supportati. Per istruzioni su come eseguire la procedura di attivazione o il join per il dispositivo, consultare la documentazione del dispositivo. Per informazioni, consulta Modalità di attivazione.
> - Per disattivare la funzionalità di roaming per i dispositivi, puoi scollegare i dispositivi da questo profilo di servizio e associarli a un altro profilo di servizio con i parametri di roaming impostati su `false`. Dopo il passaggio a questo profilo di servizio, i dispositivi devono eseguire un'altra associazione per evitare che continuino a funzionare sulla rete pubblica.

5. Messaggi in uplink e in downlink di Exchange

Dopo che è stato eseguito il join del dispositivo ad AWS IoT Core per LoRaWAN, è possibile avviare lo scambio di messaggi tra il dispositivo e il cloud.

- Visualizzazione di messaggi in uplink

Quando si inviano messaggi in uplink dai dispositivi, AWS IoT Core per LoRaWAN consegna questi messaggi a Account AWS utilizzando la destinazione configurata in precedenza. Questi messaggi verranno inviati dal dispositivo al cloud sulla rete di Everynet.

È possibile visualizzare i messaggi utilizzando il nome della regola AWS IoT o utilizzare il client MQTT per effettuare la sottoscrizione all'argomento MQTT specificato durante la creazione della destinazione. Per ulteriori informazioni sul nome della regola e altri dettagli di destinazione specificati, consultare Aggiunta di una destinazione tramite la console.

Per ulteriori informazioni sulla visualizzazione del messaggio in uplink e il formato, consultare Visualizza il formato dei messaggi di uplink inviati dai dispositivi LoRaWAN.

- Invio di messaggi in downlink

  È possibile accodare e inviare messaggi in downlink ai dispositivi dalla console o utilizzando il comando API AWS IoT Wireless, `SendDataToWirelessDevice`, o il comando AWS CLI, `send-data-to-wireless-device`. Per ulteriori informazioni sull'accodamento e l'invio di messaggi in downlink, consultare Accodamento dei messaggi di downlink da inviare ai dispositivi LoRaWAN.

  Nel codice seguente viene illustrato un esempio di come inviare un messaggio in downlink utilizzando il comando dell'interfaccia a riga di comando `send-data-to-wireless-device`. Viene specificato l'ID del dispositivo wireless per ricevere i dati, il payload, se utilizzare la modalità di riconoscimento e i metadati wireless.

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

  L'output dell'esecuzione di questo comando genera un `MessageId` per il messaggio di downlink.

> **Note**
>
> In alcuni casi, anche se ricevi il `MessageId`, i pacchetti possono essere eliminati. Per informazioni sulla risoluzione dei problemi di tali scenari, consultare Risoluzione dei problemi relativi alla coda dei messaggi di downlink.

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

- Visualizzazione delle informazioni sulla copertura

  Dopo aver abilitato la rete pubblica, puoi visualizzare le informazioni sulla copertura di rete nella console AWS IoT. Vai all'hub Copertura della console AWS IoT, quindi cerca le posizioni per visualizzare le informazioni sulla copertura dei tuoi dispositivi sulla mappa.

  > **Note**
  >
  > Questa funzionalità utilizza il servizio di posizione Amazon per visualizzare le informazioni sulla copertura dei tuoi dispositivi su una mappa di posizione Amazon. Prima di utilizzare le mappe del servizio di posizione Amazon, consulta i relativi termini e condizioni. Tieni presente che AWS potrebbe trasmettere le query API al provider di dati di terze parti prescelto, che potrebbe trovarsi all'esterno della Regione AWS attualmente utilizzata. Per ulteriori informazioni, consultare Termini del servizio AWS.

Firmware update over-the-air (FUOTA) per dispositivi LoRaWAN e gruppi multicast

È possibile eseguire FUOTA per aggiornare il firmware del dispositivo di un singolo dispositivo LoRaWAN o di un gruppo di dispositivi. Per aggiornare il firmware del dispositivo o per inviare un carico utile in downlink a più dispositivi, crea un gruppo multicast. Utilizzando il multicast, una sorgente può inviare dati a un singolo gruppo multicast, che viene quindi distribuito a un gruppo di dispositivi destinatari.

Il supporto di AWS IoT Core per LoRaWAN per i gruppi FUOTA e multicast si basa sulle seguenti specifiche di LoRa Alliance:

- Specifiche di configurazione multicast remota LoRaWAN, TS005-2.0.0
- Specifiche di trasporto frammentate del blocco dati LoRaWAN, TS004-2.0.0
- Specifiche di sincronizzazione dell'orologio a livello applicativo LoRaWAN, TS003-2.0.0

> **Note**
>
> AWS IoT Core per LoRaWAN esegue automaticamente la sincronizzazione dell'orologio secondo le specifiche LoRa Alliance. Utilizza la funzione `AppTimeReq` per rispondere all'orario lato server per i dispositivi che lo richiedono, utilizzando la segnalazione ClockSync.

Di seguito sono riportati argomenti che mostrano come creare gruppi multicast ed eseguire FUOTA.

Argomenti

Preparazione dei dispositivi per la configurazione multicast e FUOTA

Quando aggiungi il tuo dispositivo wireless a AWS IoT Core per LoRaWAN, è possibile preparare il dispositivo wireless per la configurazione multicast e FUOTA utilizzando la console o la CLI. Se utilizzi questa configurazione per la prima volta, consigliamo di utilizzare la console. Per gestire il gruppo multicast e aggiungere o rimuovere un certo numero di dispositivi dal gruppo, si consiglia di utilizzare la CLI per gestire un numero elevato di risorse.

GenAppKey e FPort

Quando si aggiunge il dispositivo wireless, prima di poter aggiungere i dispositivi a gruppi multicast o eseguire FUOTA, configura i seguenti parametri. Prima di configurare questi parametri, assicurarsi che i dispositivi supportino FUOTA e multicast e che le specifiche del dispositivo wireless siano `0TAA v1.1` o `0TAAv1.0.x`.

- `GenAppKey`: per i dispositivi che supportano LoRaWAN versione 1.0.x e per l'utilizzo di gruppi multicast, `GenAppKey` è la chiave radice specifica del dispositivo da cui derivano le chiavi di sessione per il gruppo multicast.

  > **Note**
  >
  > Per i dispositivi LoRaWAN che utilizzano le specifiche wireless `OTAA v1.1`, `AppKey` viene utilizzato per lo stesso scopo nel caso di `GenAppKey`.

  Per impostare i parametri utili ad avviare il trasferimento dei dati, AWS IoT Core per LoRaWAN distribuisce le chiavi di sessione con i dispositivi finali. Per ulteriori informazioni sulle versioni di LoRaWAN, consulta Versione di LoRaWAN.

  > **Note**
  >
  > AWS IoT Core per LoRaWAN memorizza le informazioni `GenAppKey` fornite in formato crittografato.

- `FPorts`: secondo le specifiche LoRaWAN per i gruppi FUOTA e multicast, AWS IoT Core per LoRaWAN assegna i valori predefiniti per i seguenti campi del parametro `FPorts`. Se hai già assegnato uno dei seguenti valori `FPort`, è possibile scegliere un valore disponibile diverso, da 1 a 223.
  - `Multicast`: 200

    Questo valore `FPort` viene utilizzato per i gruppi multicast.
  - `FUOTA`: 201

    Questo valore `FPort` è usato per FUOTA.
  - `ClockSync`: 202

    Questo valore `FPort` viene utilizzato per la sincronizzazione dell'orologio.

Profili di dispositivo per multicast e FUOTA

All'inizio di una sessione multicast, viene utilizzata una finestra di distribuzione di classe B o di classe C per inviare il messaggio di downlink ai dispositivi del gruppo. I dispositivi aggiunti per multicast e FUOTA devono supportare le modalità operative di classe B o di classe C. A seconda della classe

supportata dal dispositivo, scegliere un profilo per il dispositivo che abbia entrambe le modalità di classe B o classe C.

Per ulteriori informazioni sui profili, consulta Aggiungi profili a AWS IoT Core per LoRaWAN.

Preparazione dei dispositivi per multicast e FUOTA utilizzando la console

Per specificare i parametri FPorts e GenAppKey per la configurazione multicast e FUOTA utilizzando la console:

1. Passare alla Device hub (Hub dei dispositivi) della console AWS IoT e scegliere Add wireless device (Aggiungi dispositivo wireless).
2. Seleziona Wireless device specification (Specifiche del dispositivo wireless). Il dispositivo deve utilizzare OTAA per l'attivazione del dispositivo. Quando si sceglie OTAA v1.0.x o OTAA v1.1, viene visualizzata una sezione di FUOTA configuration-Optional (Configurazione FUOTA - opzionale).
3. Inserisci i parametri dell'Identificatore univoco esteso (EUI) per il dispositivo wireless.
4. Espandi la sezione FUOTA configuration-Optional (Configurazione FUOTA - opzionale) e quindi scegli This device supports firmware updates over the air (FUOTA) (Questo dispositivo supporta gli aggiornamenti firmware in onda (FUOTA)). È ora possibile inserire i valori FPort per multicast, FUOTA e sincronizzazione orologio. Se hai scelto `OTAA v1.0.x` per le specifiche del dispositivo wireless, inserisci il GenAppKey.
5. Aggiungi il tuo dispositivo a AWS IoT Core per LoRaWAN scegliendo i profili e una destinazione per l'instradamento dei messaggi. Per il profilo del dispositivo connesso al dispositivo, assicurati di selezionare una o entrambe le modalità Supporta classe B e Supporta classe C.

> **Note**
>
> Per specificare i parametri di configurazione FUOTA, devi utilizzare la Hub dei dispositivi della console AWS IoT. Questi parametri non vengono visualizzati se si esegue l'onboarding dei dispositivi utilizzando la pagina Intro (Introduzione) della console AWS IoT.

Per ulteriori informazioni sulle specifiche del dispositivo wireless e sull'onboarding del dispositivo, consulta Aggiungi il dispositivo wireless ad AWS IoT Core per LoRaWAN.

> **Note**
>
> Puoi specificare questi parametri solo quando crei il dispositivo wireless. Non è possibile modificare o specificare i parametri quando si aggiorna un dispositivo esistente.

Preparazione dei dispositivi per multicast e FUOTA utilizzando l'operazione API

Per utilizzare gruppi multicast o per eseguire FUOTA, configura questi parametri utilizzando l'operazione API `CreateWirelessDevice` o il comando CLI `create-wireless-device`. Oltre a specificare la chiave dell'applicazione e i parametri FPorts, assicurarsi che il profilo del dispositivo connesso al dispositivo supporti una o entrambe le modalità di classe B o classe C.

È possibile fornire questo file `input.json` come input per il comando `create-wireless-device`.

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

dove:

Contenuti di 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
```

```
}
```

Per informazioni sulle CLI utilizzabili, consulta AWS CLI reference (Riferimento alla).

> **Note**
>
> Dopo aver specificato i valori di questi parametri, non è possibile aggiornarli tramite l'operazione API `UpdateWirelessDevice`. Al contrario, è possibile creare un nuovo dispositivo con i valori dei parametri `GenAppKey` e `FPorts`.

Per ottenere informazioni sui valori specificati per questi parametri, è possibile utilizzare l'operazione API `GetWirelessDevice` o il comando CLI `get-wireless-device`.

Passaggi successivi

Dopo aver configurato i parametri, è possibile creare gruppi multicast e attività FUOTA per inviare payload di downlink o aggiornare il firmware dei dispositivi LoRaWAN.

- Per ulteriori informazioni sulla creazione di gruppi multicast, consulta Crea gruppi multicast e aggiungi dispositivi al gruppo.
- Per ulteriori informazioni sulla creazione di una attività FUOTA, consulta Creazione di attività FUOTA e dotazione dell'immagine del firmware.

Creazione di gruppi multicast per inviare un payload di downlink a più dispositivi

Per inviare un payload di downlink a più dispositivi, crea un gruppo multicast. Utilizzando il multicast, una sorgente può inviare dati a un singolo indirizzo multicast, che viene quindi distribuito a un intero gruppo di dispositivi destinatari.

I dispositivi di un gruppo multicast condividono lo stesso indirizzo multicast, chiavi di sessione e contatore di frame. Utilizzando le stesse chiavi di sessione, i dispositivi di un gruppo multicast possono decrittare il messaggio quando viene avviata una trasmissione downlink. Un gruppo multicast supporta solo downlink. Non dà conferma della ricezione del payload di downlink da parte dei dispositivi.

Con i gruppi multicast di AWS IoT Core per LoRaWAN, è possibile:

- Filtrare l'elenco di dispositivi utilizzando il profilo del dispositivo, RFRegion o la classe del dispositivo, e quindi aggiungere questi dispositivi a un gruppo multicast.
- Pianificare e inviare uno o più messaggi payload di downlink ai dispositivi di un gruppo multicast, all'interno di una finestra di distribuzione pari a 48 ore.
- Chiedere ai dispositivi di passare temporaneamente alla modalità Classe B o classe C all'inizio della sessione multicast per ricevere il messaggio downlink.
- Monitorare la configurazione del gruppo multicast e lo stato dei dispositivi e risolvere, inoltre, eventuali problemi.
- Usare gli aggiornamenti Firmware Over-The-Air (FUOTA) per distribuire in sicurezza gli aggiornamenti del firmware su dispositivi di un gruppo multicast.

Il seguente video descrive come creare gruppi multicast AWS IoT Core per LoRaWAN e ti guiderà attraverso il processo di aggiunta di un dispositivo al gruppo e di pianificazione di un messaggio di downlink per il gruppo.

Di seguito viene illustrato come creare il gruppo multicast e come pianificare un messaggio di downlink.

Argomenti

Crea gruppi multicast e aggiungi dispositivi al gruppo

È possibile creare gruppi multicast utilizzando la console o la CLI. Se stai creando il tuo gruppo multicast per la prima volta, ti consigliamo di utilizzare la console per aggiungere il gruppo multicast. Quando si desidera gestire il gruppo multicast e aggiungere o rimuovere dispositivi dal gruppo, è possibile utilizzare la CLI.

Dopo aver scambiato la segnalazione con i dispositivi finali aggiunti, AWS IoT Core per LoRaWAN stabilisce le chiavi condivise con i dispositivi finali e imposta i parametri per il trasferimento dei dati.

Prerequisiti

Prima di procedere con la creazione di gruppi multicast e l'aggiunta di dispositivi al gruppo:

- Preparare i dispositivi per la configurazione multicast e FUOTA, specificando i parametri di configurazione FUOTA `GenAppKey` e `FPorts`. Per ulteriori informazioni, consultare Preparazione dei dispositivi per la configurazione multicast e FUOTA.
- Verificare se i dispositivi supportano le modalità operative di classe B o di classe C. A seconda della classe supportata dal dispositivo, scegliere un profilo per il dispositivo che abbia entrambe le modalità Supporta Classe B o Supporta Classe C. Per ulteriori informazioni sui profili, consulta Aggiungi profili a AWS IoT Core per LoRaWAN.

  All'inizio della sessione multicast, viene utilizzata una finestra di distribuzione di classe B o di classe C per inviare messaggi di downlink ai dispositivi del gruppo.

Creazione di gruppi multicast utilizzando la console

Per creare gruppi multicast utilizzando la console, vai alla pagina Multicast groups (Gruppi multicast) della console AWS IoT e scegli Create multicast group (Crea gruppo multicast).

1. Creazione di un gruppo multicast

   Per creare il gruppo multicast, specificare le proprietà e i tag multicast per il gruppo.

   1. Specificazione delle proprietà multicast

      Per specificare le proprietà multicast, inserire le seguenti informazioni per il gruppo multicast.

      - Nome: inserire un nome univoco per il gruppo multicast. Il nome può includere solo lettere, numeri, trattini e caratteri di sottolineatura. Non può contenere spazi.
      - Descrizione: puoi fornire una descrizione per il gruppo multicast. Una descrizione può essere lunga fino a 2.048 caratteri.

   2. Tag per gruppo multicast

      È inoltre possibile fornire qualsiasi coppia chiave-valore come Tag per il tuo gruppo multicast. Per proseguire nella creazione del tuo gruppo multicast, scegli Successivo.

2. Aggiungere dispositivi a un gruppo multicast

   È possibile aggiungere singoli dispositivi o un gruppo di dispositivi al gruppo multicast. Per aggiungere dispositivi:

   1. Specifica RFRegion

Specifica il valore di RFRegion o la banda di frequenza per il tuo gruppo multicast. La RFRegion per il tuo gruppo multicast deve corrispondere a RFRegion di dispositivi aggiunti al gruppo multicast. Per ulteriori informazioni su RFRegion, vedi Considerate la selezione delle bande di frequenza LoRa per i gateway e la connessione del dispositivo.

2. Seleziona una classe di dispositivi multicast

   Scegliere se si desidera che i dispositivi del gruppo multicast passino a una modalità di classe B o classe C all'inizio della sessione multicast. Una sessione di classe B può ricevere messaggi di downlink nei normali slot downlink e una sessione di classe C può ricevere messaggi downlink in qualsiasi momento.

3. Scegli i dispositivi da aggiungere al gruppo

   Scegli se desideri aggiungere dispositivi al gruppo multicast singolarmente o in blocco.

   - Per aggiungere dispositivi singolarmente, inserire l'ID di ciascun di dispositivo wireless che si desidera aggiungere al gruppo.
   - Per aggiungere dispositivi in blocco, è possibile filtrare i dispositivi che si desidera aggiungere per profilo o tag. Filtrando in base al profilo del dispositivo, è possibile aggiungere dispositivi con un profilo che supporta la classe di dispositivo B, C o entrambe.

4. Per creare un nuovo gruppo, selezionare Create (Crea).

   I dettagli del gruppo multicast e i dispositivi aggiunti compaiono nel gruppo. Per informazioni sullo stato del gruppo multicast, dei dispositivi e per la risoluzione di eventuali problemi, consultare Monitora e risolvi lo stato del gruppo multicast e dei dispositivi del gruppo.

Dopo aver creato un gruppo multicast, puoi scegliere Action (Azione) per modificare, eliminare o aggiungere dispositivi al gruppo multicast. Dopo aver aggiunto i dispositivi, è possibile pianificare una sessione per l'invio del payload di downlink ai dispositivi del gruppo.

Creazione di gruppi multicast utilizzando l'API

Per creare gruppi multicast e aggiungere dispositivi al gruppo utilizzando l'API:

1. Creazione di un gruppo multicast

   Per creare il tuo gruppo multicast, usa l'operazione API `CreateMulticastGroup` o il comando CLI `create-multicast-group`. È possibile fornire questo file `input.json` come input per il comando `create-multicast-group`.

```
aws iotwireless create-multicast-group \
    --cli-input-json file://input.json
```

dove:

Contenuti di input.json

```
{
   "Description": "Multicast group to send downlink payload and perform FUOTA.",
   "LoRaWAN": {
      "DlClass": "ClassB",
      "RfRegion": "US915"
   },
   "Name": "MC_group_FUOTA"
}
```

Dopo aver creato il gruppo multicast, è possibile utilizzare le seguenti operazioni API o comandi CLI per aggiornare, eliminare o ottenere informazioni sui gruppi multicast.

- `UpdateMulticastGroup` o `update-multicast-group`
- `GetMulticastGroup` o `get-multicast-group`
- `ListMulticastGroups` o `list-multicast-groups`
- `DeleteMulticastGroup` o `delete-multicast-group`

2. Aggiungere dispositivi a un gruppo multicast

   È possibile aggiungere dispositivi al gruppo multicast singolarmente o in blocco.

   - Per creare il tuo gruppo multicast, usa l'operazione API `StartBulkAssociateWirelessDeviceWithMulticastGroup` o il comando CLI `start-bulk-associate-wireless-device-with-multicast-group`. Per filtrare i dispositivi che si desidera associare in blocco al gruppo multicast, fornisci una stringa di query. Di seguito viene illustrato come aggiungere un gruppo di dispositivi con un profilo dispositivo a cui è collegato un ID specificato.

     ```
     aws iotwireless start-bulk-associate-wireless-device-with-multicast-group \
         --id "12abd34e-5f67-89c2-9293-593b1bd862e0" \
         --cli-input-json file://input.json
     ```

dove:

Contenuti di input.json

```
{
     "QueryString": "DeviceProfileName: MyWirelessDevice AND DeviceProfileId:
 d6d8ef8e-7045-496d-b3f4-ebcaa1d564bf",
     "Tags": [
        {
            "Key": "Multicast",
            "Value": "ClassB"
        }
    ]
}
```

Qui, `multicast-groups/d6d8ef8e-7045-496d-b3f4-ebcaa1d564bf/bulk` è l'URL utilizzato per associare dispositivi al gruppo.

- Per creare il tuo gruppo multicast, usa l'operazione API `AssociateWirelessDeviceWithMulticastGroup` o il comando CLI `associate-wireless-device-with-multicast-group`. Fornisci l'ID del dispositivo wireless per ogni dispositivo che desideri aggiungere al tuo gruppo.

```
aws iotwireless associate-wireless-device-with-multicast-group \
    --id "12abd34e-5f67-89c2-9293-593b1bd862e0" \
    --wireless-device-id "ab0c23d3-b001-45ef-6a01-2bc3de4f5333"
```

Dopo aver creato il gruppo multicast, è possibile utilizzare le seguenti operazioni API o comandi CLI per ottenere informazioni sul gruppo multicast o per disassociare i dispositivi.

- `DisassociateWirelessDeviceFromMulticastGroup` o `disassociate-wireless-device-from-multicast-group`
- `StartBulkDisassociateWirelessDeviceFromMulticastGroup` o `start-bulk-disassociate-wireless-device-from-multicast-group`
- `ListWirelessDevices` o `list-wireless-devices`

> **Note**
>
> L'operazione API `ListWirelessDevices` può essere utilizzata per creare elenchi di dispositivi wireless in generale, o di dispositivi wireless associati a un gruppo multicast o a un'attività FUOTA.
>
> - Per elencare i dispositivi wireless associati a un gruppo multicast, utilizzare l'operazione API `ListWirelessDevices` con `MulticastGroupID` come filtro.
> - Per elencare i dispositivi wireless associati a un'attività processo FUOTA, utilizzare l'operazione API `ListWirelessDevices` con `FuotaTaskID` come filtro.

Passaggi successivi

Dopo aver creato un gruppo multicast e aggiunto dispositivi, è possibile continuare ad aggiungere dispositivi e monitorare lo stato sia del gruppo multicast che dei dispositivi. Se i dispositivi sono stati aggiunti correttamente al gruppo, puoi configurare e pianificare un messaggio di downlink da inviare ai dispositivi. Prima di poter inviare un messaggio di downlink, lo stato del dispositivo deve essere Multicast setup ready (Configurazione multicast pronta). Dopo aver pianificato un messaggio downlink, lo stato cambia in Session attempting (Tentativo di sessione). Per ulteriori informazioni, consultare Pianifica un messaggio di downlink da inviare ai dispositivi del gruppo multicast.

Se si desidera aggiornare il firmware dei dispositivi nel gruppo multicast, è possibile eseguire aggiornamenti Firmware Over-The-Air (FUOTA) con AWS IoT Core per LoRaWAN. Per ulteriori informazioni, consultare Aggiornamenti Firmware Over-The-Air (FUOTA) per dispositivi AWS IoT Core per LoRaWAN.

Se i dispositivi non sono stati aggiunti o se viene visualizzato un errore nel gruppo multicast o nello stato del dispositivo, puoi passare il mouse sopra l'errore per ottenere ulteriori informazioni e risolverlo. Se viene ancora visualizzato un errore, consultare Monitora e risolvi lo stato del gruppo multicast e dei dispositivi del gruppo per informazioni su come risolvere il problema.

Monitora e risolvi lo stato del gruppo multicast e dei dispositivi del gruppo

Dopo aver aggiunto dispositivi e creato il gruppo multicast, apri la AWS Management Console. Consulta la pagina Multicast groups (Gruppi multicast) della console AWS IoT e scegli il gruppo multicast creato per visualizzarne i dettagli. Vedrai informazioni sul gruppo multicast, sul numero di dispositivi aggiunti e dettagli sullo stato del dispositivo. È possibile utilizzare le informazioni sullo stato per monitorare l'avanzamento della sessione multicast e risolvere eventuali errori.

Stato del gruppo multicast

I dispositivi del gruppo multicast trovarsi in uno dei seguenti messaggi di stato, visibili nella AWS Management Console.

- In attesa

  Questo stato indica che hai creato un gruppo multicast ancora sprovvisto di sessione multicast. Verrà visualizzato questo messaggio di stato quando il gruppo è stato creato. Intanto, è possibile aggiornare il gruppo multicast e associare o disassociare i dispositivi al gruppo. Dopo che lo stato è cambiato da Pending (In attesa), non è possibile aggiungere al gruppo altri dispositivi.

- Session attempting (Tentativo di sessione)

  Dopo che i tuoi dispositivi sono stati aggiunti con successo al gruppo multicast, verrà mostrato questo messaggio di stato quando il gruppo ha una sessione multicast pianificata. Nel frattempo, non è possibile aggiornare o aggiungere dispositivi al gruppo multicast. Se annulli la sessione multicast, lo stato del gruppo cambia in Pending (In attesa).

- In session (In sessione)

  Nei primi istanti della sessione multicast, verrà mostrato questo messaggio di stato. Anche un gruppo multicast continua a trovarsi in questo stato quando è associato a un'attività FUOTA con una sessione di aggiornamento firmware in corso.

  Se non si dispone di un'attività FUOTA associata nella sessione, e se la sessione multicast viene annullata perché il tempo di sessione ha superato il timeout, o la sessione multicast è stata annullata, lo stato del gruppo cambia in Pending (In attesa).

- Delete waiting (Eliminazione attesa)

  Se elimini il gruppo multicast, lo stato del gruppo cambia in Delete waiting (Eliminazione attesa). Le eliminazioni sono permanenti e non possono essere annullate. Questa operazione può richiedere tempo e lo stato del gruppo sarà Delete_Waiting fino a quando il gruppo multicast non sarà eliminato. Dopo che l'attività FUOTA passa a questo stato, non potrà passare in uno degli altri stati.

Stato dei dispositivi nel gruppo multicast

I dispositivi del gruppo multicast possono avere uno dei seguenti messaggi di stato, visibili nella AWS Management Console. È possibile passare il mouse su ciascun messaggio di stato per ottenere ulteriori informazioni su ciò che indica.

- Package attempting (Tentativo di avvio pacchetto)

  Dopo che i dispositivi sono stati associati al gruppo multicast, lo stato del dispositivo è Package attempting (Tentativo di avvio pacchetto). Quando compare questo stato, significa che AWS IoT Core per LoRaWAN non ha ancora confermato se il dispositivo supporta la configurazione e il funzionamento multicast.

- Package unsupported (Pacchetto non supportato)

  Dopo che i dispositivi sono stati associati al gruppo multicast, AWS IoT Core per LoRaWAN verifica se il firmware del dispositivo è in grado di eseguire la configurazione e il funzionamento multicast. Se sul dispositivo non è disponibile il pacchetto multicast supportato, lo stato è Package unsupported (Pacchetto non supportato). Per risolvere l'errore, verificare se il firmware del dispositivo è in grado di eseguire la configurazione e il funzionamento multicast.

- Multicast setup attempting (Tentativo di configurazione multicast)

  Se i dispositivi associati al gruppo multicast sono in grado di configurare e funzionare multicast, lo stato è Multicast setup attempting (Tentativo di configurazione multicast). Questo stato indica che il dispositivo non ha ancora completato la configurazione multicast.

- Multicast setup ready (Configruazione multicast pronta)

  Il dispositivo ha completato la configurazione multicast ed è stato aggiunto al gruppo multicast. Questo stato indica che i dispositivi sono pronti per una sessione multicast e che un messaggio di downlink può essere inviato a tali dispositivi. Lo stato indica anche quando è possibile utilizzare FUOTA per aggiornare il firmware dei dispositivi del gruppo.

- Session attempting (Tentativo di sessione)

  È stata pianificata una sessione multicast per i dispositivi del gruppo multicast. All'inizio di una sessione di gruppo multicast, lo stato del dispositivo è Session attempting (Tentativo di sessione) e richieste vengono inviate per sapere se è possibile avviare una finestra di distribuzione di classe B o di classe C per la sessione. Se il tempo necessario per configurare la sessione multicast supera il timeout o se si annulla la sessione multicast, lo stato cambia in Multicast setup done (Configurazione multicast completa).

- In session (In sessione)

  Questo stato indica che è stata avviata una finestra di distribuzione di classe B o di classe C e che il dispositivo ha una sessione multicast in corso. Durante questo periodo, è possibile inviare messaggi downlink da AWS IoT Core per LoRaWAN ai dispositivi del gruppo multicast. Se si

aggiorna l'ora della sessione, la sessione corrente viene sostituita e lo stato cambia in Session attempting (Tentativo di sessione). Quando il tempo di sessione termina o se si annulla la sessione multicast, lo stato cambia in Multicast setup ready (Configurazione multicast pronta).

Passaggi successivi

Ora che hai appreso i diversi stati del tuo gruppo multicast e dei dispositivi del gruppo, e sai come risolvere eventuali problemi (ad esempio quando un dispositivo non è in grado di configurare il multicast), puoi pianificare un messaggio downlink da inviare ai dispositivi e il tuo gruppo multicast si troverà nello stato In session (In sessione). Per ulteriori informazioni sulla pianificazione di un messaggio di downlink, consulta Pianifica un messaggio di downlink da inviare ai dispositivi del gruppo multicast.

Pianifica un messaggio di downlink da inviare ai dispositivi del gruppo multicast

Dopo aver aggiunto correttamente i dispositivi al gruppo multicast, è possibile avviare una sessione multicast e configurare un messaggio di downlink da inviare ai dispositivi. Il messaggio di downlink deve essere pianificato entro 48 ore e l'ora di inizio per il multicast deve essere pianificata almeno 30 minuti dopo l'ora corrente.

> **Note**
>
> I dispositivi di un gruppo multicast non possono identificare il momento in cui viene ricevuto un messaggio di downlink.

Prerequisiti

Prima di poter inviare un messaggio di downlink, è necessario aver creato un gruppo multicast e aver aggiunto correttamente i dispositivi al gruppo per il quale si desidera inviare un messaggio di downlink. Non è possibile aggiungere altri dispositivi dopo che è stato pianificato un orario di inizio per la sessione multicast. Per ulteriori informazioni, consultare Crea gruppi multicast e aggiungi dispositivi al gruppo.

Se uno dei dispositivi non è stato aggiunto correttamente, il gruppo multicast e lo stato del dispositivo conterranno informazioni per aiutarti a risolvere gli errori. Se gli errori persistono, consultare Monitora e risolvi lo stato del gruppo multicast e dei dispositivi del gruppo per informazioni sulla risoluzione di questi errori.

Pianificazione di un messaggio di downlink utilizzando la console

Per inviare un messaggio di downlink utilizzando la console, vai alla pagina Multicast groups (Gruppi multicast) della console AWS IoT e scegli il gruppo multicast creato. Nella pagina dei dettagli gruppo multicast, scegli Schedule downlink message (Pianifica il messaggio di downlink) e quindi Schedule downlink session (Pianifica una sessione downlink).

1. Pianificazione della finestra del messaggio di downlink

   È possibile impostare una finestra temporale per l'invio di un messaggio di downlink ai dispositivi del gruppo multicast. Il messaggio di downlink deve essere programmato entro 48 ore.

   Per pianificare la sessione multicast, specificare i seguenti parametri:

   - Start date (Data di inizio) e Start time (Ora di inizio):: la data e l'ora di inizio devono essere successive di almeno 30 minuti e 48 ore prima rispetto all'ora corrente.

     > **Note**
     >
     > L'ora specificata è in UTC, considera quindi di verificare la differenza di fuso orario con la tua area geografica al momento della pianificazione della finestra di downlink.

   - Session timeout (Timeout della sessione): il tempo trascorso il quale la sessione multicast verrà interrotta se non è stato ricevuto alcun messaggio di downlink. Il timeout minimo ammesso è di 60 secondi. Il valore massimo di timeout è di 2 giorni per i gruppi multicast di classe B e 18 ore per i gruppi multicast di classe C.
2. Configurazione del messaggio di downlink

   Per configurare il messaggio di downlink, specificare i seguenti parametri:

   - Data rate (Velocità dati): Scegli una velocità dati per il tuo messaggio downlink. La velocità dati dipende dalla RFRegion e dalle dimensioni del payload. La velocità dati predefinita è 8 per la regione US915 e 0 per la regione EU868.
   - Frequency (Frequenza): scegli una frequenza per l'invio del tuo messaggio di downlink. Per evitare conflitti di messaggistica, scegli una frequenza disponibile a seconda della regione.
   - FPort: Scegli una porta di frequenza disponibile per l'invio del messaggio di downlink ai tuoi dispositivi.
   - Payload: specifica la dimensione massima del payload in base alla velocità dati. Utilizzando la velocità dati predefinita, è possibile avere una dimensione massima del payload di 33 byte

nella RfRregion US915 e 51 byte nella RfRegion EU868. Utilizzando velocità dati più elevate, è possibile trasferire fino a una dimensione massima del payload di 242 byte.

Per pianificare il tuo messaggio di downlink, scegli Schedule (Pianifica).

Pianificazione di un messaggio di downlink utilizzando l'API

Per pianificare un messaggio di downlink utilizzando l'API, utilizzare l'operazione API `StartMulticastGroupSession` o il comando CLI `start-multicast-group-session`.

È possibile utilizzare le seguenti operazioni API o comandi CLI per ottenere informazioni ed eliminare un gruppo multicast.

- `GetMulticastGroupSession` o `get-multicast-group-session`
- `DeleteMulticastGroupSession` o `delete-multicast-group-session`

Per inviare dati a un gruppo multicast dopo l'avvio della sessione, utilizzare l'operazione API `SendDataToMulticastGroup` o il comando CLI `send-data-to-multicast-group`.

Passaggi successivi

Dopo aver configurato un messaggio di downlink da inviare ai dispositivi, il messaggio viene inviato all'inizio della sessione. I dispositivi di un gruppo multicast non possono confermare che il messaggio sia stato ricevuto.

Configurazione di ulteriori messaggi di downlink

È inoltre possibile configurare ulteriori messaggi di downlink da inviare ai dispositivi del gruppo multicast:

- Per configurare ulteriori messaggi di downlink dalla console:
  1. Passare alla pagina Multicast groups (Gruppi multicast) della console AWS IoT e scegli il gruppo multicast creato.
  2. Nella pagina dei dettagli gruppo multicast, scegli Schedule downlink message (Pianifica il messaggio downlink) e quindi Configure additional downlink message (Configura ulteriori messaggi di downlink).
  3. Specifica i parametri Data rate (Velocità dati), Frequency(Frequenza), FPort e Payload come hai fatto per il primo messaggio di downlink.

- Per configurare ulteriori messaggi di downlink utilizzando l'API o la CLI, chiamare l'operazione API `SendDataToMulticastGroup` o il comando CLI `send-data-to-multicast-group` per ogni messaggio di downlink aggiuntivo.

Aggiornamento della pianificazione delle sessioni

È inoltre possibile aggiornare la pianificazione della sessione per utilizzare una nuova data e ora di inizio della la sessione multicast. Con la pianificazione di una nuova sessione, la sessione precedentemente pianificata verrà sostituita.

> **Note**
>
> Aggiorna la sessione multicast solo quando necessario. Questi aggiornamenti possono far sì che un gruppo di dispositivi si riattivi per una lunga durata e scarichi la batteria.

- Per aggiornare la pianificazione della sessione dalla console:
  1. Passare alla pagina Multicast groups (Gruppi multicast) della console AWS IoT e scegli il gruppo multicast creato.
  2. Nella pagina dei dettagli gruppo multicast, scegliere Schedule downlink message (Pianifica il messaggio downlink) e quindi Update session schedule (Aggiorna pianificazione sessione).
  3. Specifica i parametri State date (Data dello stato), Start time (Ora di inizio), e Timeout session (Timeout della sessione), in modo analogo a quanto fatto per il primo messaggio di downlink.
- Per aggiornare la pianificazione della sessione dall'API o dalla CLI, utilizzare l'operazione API `StartMulticastGroupSession` o il comando CLI `start-multicast-group-session`.

Aggiornamenti Firmware Over-The-Air (FUOTA) per dispositivi AWS IoT Core per LoRaWAN

Usa gli aggiornamenti Firmware Over-The-Air (FUOTA) per distribuire gli aggiornamenti del firmware su dispositivi AWS IoT Core per LoRaWAN.

Utilizzando FUOTA, è possibile inviare aggiornamenti firmware a singoli dispositivi o a un gruppo di dispositivi. È inoltre possibile inviare aggiornamenti firmware a più dispositivi creando un gruppo multicast. Per prima cosa aggiungi i tuoi dispositivi al gruppo multicast, quindi invia l'immagine di aggiornamento del firmware a tutti i dispositivi. Si consiglia di firmare digitalmente le immagini del

firmware, in modo che i dispositivi che ricevono le immagini possano verificare che provengano dalla sorgente corretta.

Con i FUOTA di AWS IoT Core per LoRaWAN, puoi:

- Distribuire le nuove immagini del firmware o immagini delta a un solo dispositivo o ad un gruppo di dispositivi.
- Verificare l'autenticità e l'integrità del nuovo firmware dopo che è stato distribuito ai dispositivi.
- Monitora l'avanzamento di un'implementazione e i problemi di debug in caso di distribuzione non riuscita.

Il supporto di AWS IoT Core per LoRaWAN per i gruppi FUOTA e multicast si basa sulle seguenti specifiche di LoRa Alliance:

- Specifiche di configurazione multicast remota LoRaWAN, TS005-2.0.0
- Specifiche di trasporto frammentate del blocco dati LoRaWAN, TS004-2.0.0
- Specifiche di sincronizzazione dell'orologio a livello applicativo LoRaWAN, TS003-2.0.0

> **Note**
>
> AWS IoT Core per LoRaWAN esegue automaticamente la sincronizzazione dell'orologio secondo le specifiche LoRa Alliance. Utilizza la funzione `AppTimeReq` per rispondere all'orario lato server per i dispositivi che lo richiedono, utilizzando la segnalazione ClockSync.

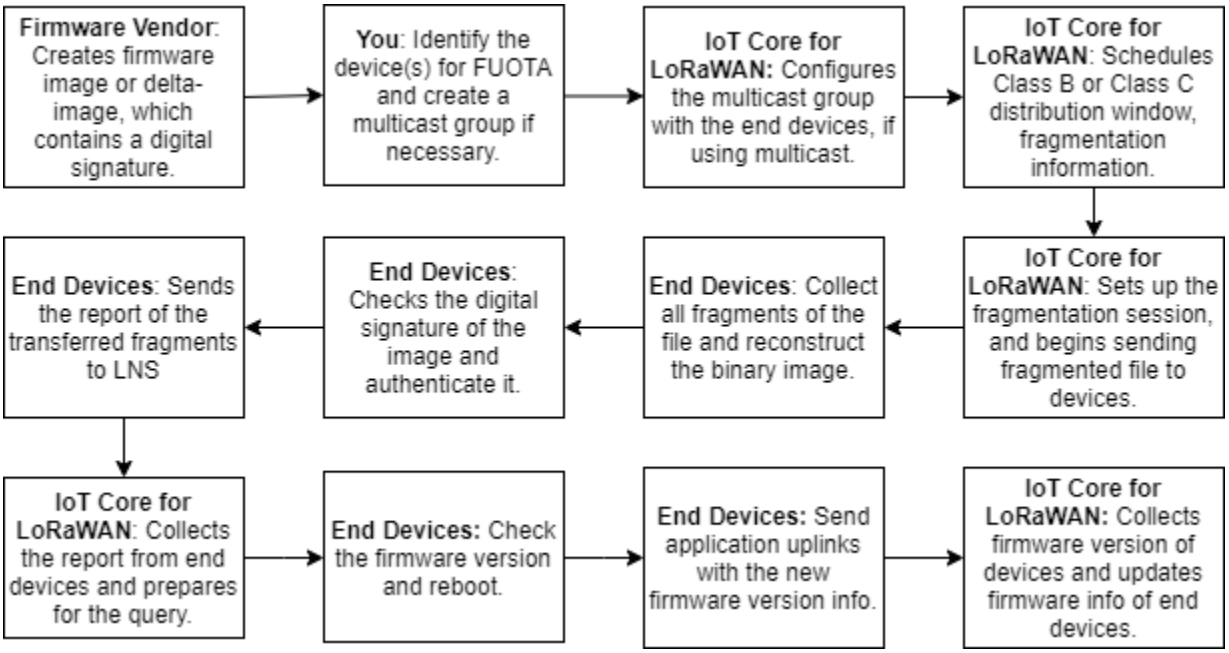
Il seguente video descrive come creare attività FUOTA AWS IoT Core per LoRaWAN e ti guida attraverso il processo di aggiunta di dispositivi all'attività e di pianificazione di un'attività FUOTA.

I seguenti argomenti illustrano come eseguire gli aggiornamenti FUOTA.

- Panoramica del processo FUOTA
- Creazione di attività FUOTA e dotazione dell'immagine del firmware
- Aggiunta di dispositivi e gruppi multicast per un'attività FUOTA e pianificazione di una sessione FUOTA
- Monitoraggio e risoluzione dello stato dell'attività FUOTA e dei dispositivi aggiunti all'attività

Panoramica del processo FUOTA

Il seguente diagramma mostra come AWS IoT Core per LoRaWAN esegue il processo FUOTA per i tuoi dispositivi finali. Se stai aggiungendo singoli dispositivi alla sessione FUOTA, puoi saltare i passaggi per creare e configurare il tuo gruppo multicast. Puoi aggiungere i tuoi dispositivi direttamente a una sessione FUOTA, poi AWS IoT Core per LoRaWAN avvierà il processo di aggiornamento del firmware.



Per eseguire i FUOTA per i tuoi dispositivi, prima di tutto crea l'immagine del firmware con firma digitale, poi configura i dispositivi e i gruppi multicast che desideri aggiungere all'attività FUOTA. Dopo aver avviato una sessione FUOTA, i dispositivi finali raccolgono tutti i frammenti, da cui ricostruiscono l'immagine, riportano lo stato a AWS IoT Core per LoRaWAN, e applicano la nuova immagine del firmware.

Di seguito sono illustrati i diversi passaggi del processo FUOTA:

1. Crea un'immagine firmware o un'immagine delta con una firma digitale

   Affinché AWS IoT Core per LoRaWAN possa eseguire i FUOTA per i tuoi dispositivi LoRaWAN, ti consigliamo di firmare digitalmente l'immagine del firmware o l'immagine delta quando invii gli aggiornamenti del firmware via etere (OTA). I dispositivi che ricevono le immagini possono quindi verificare che questa provenga dalla sorgente giusta.

   L'immagine del firmware non deve avere dimensioni superiori a 1 megabyte. Maggiore è la dimensione del firmware, maggiore sarà il tempo necessario per completare il processo di

aggiornamento. Per un trasferimento dati più rapido o se la nuova immagine è più grande di 1 Megabyte, utilizza un'immagine delta, che è parte della nuova immagine e rappresenta il delta tra la nuova immagine del firmware e l'immagine precedente.

> **Note**
>
> AWS IoT Core per LoRaWAN non fornisce lo strumento di generazione della firma digitale e il sistema di gestione delle versioni del firmware. È possibile utilizzare qualsiasi strumento di terze parti per generare la firma digitale per l'immagine del firmware. Si consiglia di utilizzare uno strumento di firma digitale come quello incorporato in ARM Mbed GitHub repository (Repository GitHub ARM Mbed), che include anche strumenti per la generazione dell'immagine delta e per i dispositivi per l'utilizzo di tale immagine.

2. Identificazione e configurazione dei dispositivi per FUOTA

   Dopo aver identificato i dispositivi per FUOTA, inviare gli aggiornamenti del firmware a dispositivi singoli o multipli.

   - Per inviare gli aggiornamenti del firmware a più dispositivi, crea un gruppo multicast e configuralo con i dispositivi finali. Per ulteriori informazioni, consultare Creazione di gruppi multicast per inviare un payload di downlink a più dispositivi.
   - Per inviare aggiornamenti firmware a singoli dispositivi, aggiungi tali dispositivi alla sessione FUOTA e quindi esegui l'aggiornamento del firmware.

3. Pianificazione di una finestra di distribuzione e configurazione della sessione di frammentazione

   Se è stato creato un gruppo multicast, è possibile specificare la finestra di distribuzione di classe B o di classe C, per determinare quando i dispositivi possono ricevere i frammenti da AWS IoT Core per LoRaWAN. I dispositivi potrebbero funzionare in classe A, prima di passare alla modalità di classe B o classe C. È inoltre necessario specificare l'ora di inizio della sessione.

   I dispositivi di classe B o di classe C si riattivano alla finestra di distribuzione specificata e iniziano a ricevere i pacchetti di downlink. I dispositivi che funzionano in modalità classe C possono consumare più energia rispetto ai dispositivi di classe B. Per ulteriori informazioni, consultare Classi di dispositivi.

4. I dispositivi finali segnalano lo stato a AWS IoT Core per LoRaWAN, e aggiornano l'immagine firmware

   Dopo aver configurato una sessione di frammentazione, i dispositivi finali e AWS IoT Core per LoRaWAN eseguono la procedura seguente per aggiornare il firmware del dispositivo.

   1. Poiché i dispositivi LoRaWAN hanno una bassa velocità di dati, per avviare il processo FUOTA, AWS IoT Core per LoRaWAN imposta una sessione di frammentazione per frammentare l'immagine del firmware. Poi invia questi frammenti ai dispositivi finali.
   2. Dopo che AWS IoT Core per LoRaWAN invia i frammenti di immagine, i dispositivi finali LoRaWAN eseguono le seguenti attività.
      a. Raccolgono i frammenti e, successivamente, ricostruiscono i l'immagine binaria da questi frammenti.
      b. Controllano la firma digitale dell'immagine ricostruita per autenticare l'immagine e verificano che provenga dalla sorgente giusta.
      c. Confrontano la versione del firmware da AWS IoT Core per LoRaWAN con la versione corrente.
      d. Segnalano lo stato delle immagini frammentate trasferite in AWS IoT Core per LoRaWAN, quindi applicano la nuova immagine del firmware.

      > **Note**
      >
      > In alcuni casi, i dispositivi finali riportano lo stato delle immagini frammentate trasferite in AWS IoT Core per LoRaWAN prima di controllare la firma digitale dell'immagine del firmware.

Ora che conosci il processo FUOTA, è possibile creare l'attività FUOTA e aggiungere dispositivi all'attività per aggiornare il firmware. Per ulteriori informazioni, consultare Creazione di attività FUOTA e dotazione dell'immagine del firmware.

Creazione di attività FUOTA e dotazione dell'immagine del firmware

Per aggiornare il firmware dei dispositivi LoRaWAN, creare innanzitutto un'attività FUOTA e fornire l'immagine del firmware, provvista di firma digitale, che si desidera utilizzare per l'aggiornamento. È quindi possibile aggiungere dispositivi e gruppi multicast all'attività e pianificare una sessione FUOTA. All'inizio della sessione, AWS IoT Core per LoRaWAN imposta una sessione di frammentazione e i

dispositivi finali raccolgono i frammenti, ricostruiscono l'immagine e applicano il nuovo firmware. Per ulteriori informazioni sul processo FUOTA, consulta Panoramica del processo FUOTA.

Di seguito viene illustrato come creare un'attività FUOTA e caricare l'immagine del firmware o l'immagine delta che verrà memorizzata in un bucket S3.

Prerequisiti

Prima di poter eseguire i FUOTA, l'immagine del firmware deve essere firmata digitalmente in modo che i dispositivi finali possano verificare l'autenticità dell'immagine al momento dell'applicazione. È possibile utilizzare qualsiasi strumento di terze parti per generare la firma digitale per l'immagine del firmware. Si consiglia di utilizzare uno strumento di firma digitale come quello incorporato in ARM Mbed GitHub repository (Repository GitHub ARM Mbed), che include anche strumenti per la generazione dell'immagine delta e per i dispositivi per l'utilizzo di tale immagine.

Creazione di un'attività FUOTA e caricamento dell'immagine del firmware utilizzando la console

Per creare un'attività FUOTA e caricare l'immagine del firmware utilizzando la console, vai alla scheda FUOTA tasks (Attività FUOTA) della console e quindi scegli Create FUOTA task (Crea attività FUOTA).

1. Creazione di un'attività FUOTA

   Per creare l'attività FUOTA, specificare le proprietà e i tag dell'attività.

   1. Specificazione proprietà delle attività FUOTA

      Per specificare le proprietà delle attività FUOTA, immettere le seguenti informazioni.

      - Name (Nome): Inserire un nome univoco per l'attività FUOTA. Il nome può includere solo lettere, numeri, trattini e caratteri di sottolineatura. Non può contenere spazi.
      - Descrizione: puoi fornire una descrizione per il gruppo multicast. La descrizione può contenere fino a 2.048 caratteri.
      - RFRegion: imposta la banda di frequenza per l'attività FUOTA. La banda di frequenza deve corrispondere a quella utilizzata per effettuare il provisioning dei dispositivi wireless o dei gruppi multicast.

   2. Tag per attività FUOTA

      È inoltre possibile fornire qualsiasi coppia chiave-valore come Tag per la tua attività FUOTA. Scegliere Next (Successivo) per continuare la creazione dell'immagine.

2. Caricamento dell'immagine del firmware

   Scegliere il file immagine del firmware che si desidera utilizzare per aggiornare il firmware dei dispositivi da aggiungere all'attività FUOTA. Il file di immagine del firmware è archiviato in un bucket S3. È possibile fornire a AWS IoT Core per LoRaWAN le autorizzazioni per accedere all'immagine del firmware per tuo conto. Si consiglia di firmare digitalmente le immagini del firmware in modo da verificarne l'autenticità quando viene eseguito l'aggiornamento del firmware.

   1. Scelta del file immagine del firmware

      È possibile caricare un nuovo file immagine del firmware in un bucket S3 o scegliere un'immagine esistente già caricata in un bucket S3.

      > **Note**
      >
      > Il file di immagine del firmware non deve avere dimensioni superiori a 1 megabyte. Maggiore è la dimensione del firmware, maggiore sarà il tempo necessario per completare il processo di aggiornamento.

      - Per utilizzare un'immagine esistente, scegli Select an existing firmware image (Seleziona un'immagine firmware esistente), scegli Browse S3 (Sfoglia S3) e quindi scegli il file immagine del firmware che desideri utilizzare.

        AWS IoT Core per LoRaWAN popola l'URL S3, ovvero il percorso del file immagine del firmware nel bucket S3. Il formato del percorso è `s3://bucket_name/file_name`. Per visualizzare il file nella console Amazon Simple Storage Service, scegli View (Visualizza).
      - Per caricare una nuova immagine firmware.

        a. Scegliere Upload a new firmware image (Carica una nuova immagine del firmware) e caricare l'immagine del firmware. Il file immagine non deve essere superiore a 1 megabyte.

        b. Per creare un bucket S3 e inserire un Bucket name (Nome bucket) per memorizzare il file immagine del firmware, scegliere Create S3 bucket (Crea bucket S3).

   2. Autorizzazioni per accedere al bucket

      Puoi creare un nuovo ruolo di servizio o scegliere un ruolo esistente per permettere a AWS IoT Core per LoRaWAN di accedere al file immagine del firmware nel bucket S3 per tuo conto. Seleziona Avanti.

Per creare un nuovo ruolo, è possibile inserire un nome di ruolo o lasciarlo vuoto per generare automaticamente un nome casuale. Per visualizzare le autorizzazioni della policy che consentono l'accesso al bucket S3, scegliere View policy permissions (Visualizza le autorizzazioni della policy).

Per ulteriori informazioni sull'utilizzo di un bucket S3 per archiviare l'immagine e concedere a AWS IoT Core per LoRaWAN le autorizzazioni per l'accesso, vedi Caricare il file del firmware in un bucket S3 e aggiungere un ruolo IAM.

3. Rivedi e crea

   Per creare l'attività FUOTA, esaminare i dettagli di configurazione e attività FUOTA specificati e scegliere Create task (Crea attività).

Creazione di attività FUOTA e caricamento dell'immagine del firmware utilizzando l'API

Per creare un'attività FUOTA e specificare il file immagine del firmware utilizzando l'API, utilizzare l'operazione API `CreateFuotaTask` o il comando CLI `create-fuota-task`. È possibile fornire questo file `input.json` come input per il comando `create-fuota-task`. Quando si utilizza l'API o la CLI, il file immagine del firmware fornito come input deve essere già caricato in un bucket S3. È inoltre possibile specificare il ruolo IAM che fornisce a AWS IoT Core per LoRaWAN l'accesso all'immagine del firmware nel bucket S3.

```
aws iotwireless create-fuota-task \
    --cli-input-json file://input.json
```

dove:

Contenuti di 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"
}
```

Dopo aver creato l'attività FUOTA, è possibile utilizzare le seguenti operazioni API o comandi CLI per aggiornare, eliminare o ottenere informazioni sull'attività FUOTA.

- `UpdateFuotaTask` o `update-fuota-task`
- `GetFuotaTask` o `get-fuota-task`
- `ListFuotaTasks` o `list-fuota-tasks`
- `DeleteFuotaTask` o `delete-fuota-task`

Passaggi successivi

Dopo aver creato un'attività FUOTA e fornito l'immagine del firmware, è possibile aggiungere dispositivi all'attività per aggiornare il firmware. È possibile aggiungere singoli dispositivi o gruppi multicast all'attività. Per ulteriori informazioni, consultare Aggiunta di dispositivi e gruppi multicast per un'attività FUOTA e pianificazione di una sessione FUOTA.

Aggiunta di dispositivi e gruppi multicast per un'attività FUOTA e pianificazione di una sessione FUOTA

Dopo aver creato un'attività FUOTA, è possibile aggiungere dispositivi all'attività per cui si desidera aggiornare il firmware. Dopo aver aggiunto correttamente i dispositivi all'attività FUOTA, è possibile pianificare una sessione FUOTA per aggiornare il firmware del dispositivo.

- Se si dispone di un numero limitato di dispositivi, è possibile aggiungere questi dispositivi direttamente all'attività FUOTA.
- Se si dispone di un numero elevato di dispositivi per cui si desidera aggiornare il firmware, è possibile aggiungere questi dispositivi ai gruppi multicast e in seguito aggiungere i gruppi multicast all'attività FUOTA. Per ulteriori informazioni sulla creazione di gruppi multicast, consulta Creazione di gruppi multicast per inviare un payload di downlink a più dispositivi.

> **Note**
>
> È possibile aggiungere singoli dispositivi o gruppi multicast all'attività FUOTA. Non è possibile aggiungere sia dispositivi che gruppi multicast all'attività.

Dopo aver aggiunto i dispositivi o i gruppi multicast, è possibile avviare una sessione di aggiornamento firmware. AWS IoT Core per LoRaWAN raccoglie l'immagine del firmware, frammenta

le immagini e quindi memorizza i frammenti in un formato crittografato. I dispositivi finali raccolgono i frammenti e applicano la nuova immagine del firmware. Il tempo necessario per l'aggiornamento del firmware dipende dalle dimensioni dell'immagine e dalla frammentazione delle immagini. Al termine dell'aggiornamento del firmware, i frammenti crittografati dell'immagine del firmware memorizzati da AWS IoT Core per LoRaWAN vengono eliminati. È ancora possibile trovare l'immagine del firmware nel bucket S3.

Prerequisiti

Prima di poter aggiungere dispositivi o gruppi multicast all'attività FUOTA, procedere come segue.

- Devi aver già creato l'attività FUOTA e aver fornito l'immagine del firmware. Per ulteriori informazioni, consultare Creazione di attività FUOTA e dotazione dell'immagine del firmware.
- Effettua il provisioning dei dispositivi wireless per cui desideri aggiornare il firmware del dispositivo. Per informazioni su come eseguire l'onboarding del dispositivo, consulta Integra i tuoi dispositivi su AWS IoT Core per LoRaWAN.
- Per aggiornare il firmware di più dispositivi, è possibile aggiungerli a un gruppo multicast. Per ulteriori informazioni, consultare Creazione di gruppi multicast per inviare un payload di downlink a più dispositivi.
- Quando si esegue l'onboarding dei dispositivi in AWS IoT Core per LoRaWAN, specificare il parametro `FPorts` della configurazione FUOTA. Se utilizzi un dispositivo LoRaWan v1.0.x, devi anche specificare il `GenAppKey`. Per maggiori informazioni sulla denominazione dei parametri di configurazione, vedere Preparazione dei dispositivi per la configurazione multicast e FUOTA.

Aggiunta di dispositivi a un'attività FUOTA e pianificazione di una sessione FUOTA utilizzando la console

Per aggiungere dispositivi o gruppi multicast e pianificare una sessione FUOTA utilizzando la console, vai alla sezione FUOTA tasks (Attività FUOTA) della console. Quindi, scegli l'attività FUOTA a cui desideri aggiungere i dispositivi ed esegui l'aggiornamento del firmware.

Aggiunta di dispositivi e gruppi multicast

1. È possibile aggiungere singoli dispositivi o gruppi multicast all'attività FUOTA. Non è possibile aggiungere sia dispositivi che gruppi multicast alla stessa attività FUOTA. Per aggiungere dispositivi utilizzando la console, esegui queste operazioni.

    1. In FUOTA task details (Dettagli attività FUOTA), scegli Add device(Aggiungi dispositivo).

2. Scegli la banda di frequenza o RFRegion per i dispositivi aggiunti all'attività. Questo valore deve corrispondere al RFRegion che hai scelto per l'attività FUOTA.
3. Scegli se desideri aggiungere singoli dispositivi o gruppi multicast all'attività.
   - Per aggiungere singoli dispositivi, scegli Add individual devices (Aggiunta di dispositivi individuali) e inserisci l'ID di ciascun dispositivo che desideri aggiungere all'attività FUOTA.
   - Per aggiungere gruppi multicast, scegli Add multicast groups (Aggiungi gruppi multicast) e aggiungi i tuoi gruppi multicast all'attività. È possibile filtrare i gruppi multicast che si desidera aggiungere all'attività in base al profilo o ai tag del dispositivo. Quando si filtra in base al profilo del dispositivo, è possibile scegliere gruppi multicast con dispositivi con un profilo con l'opzione Supporta classe B o Supporta la classe C abilitata.

2. Pianificazione della sessione FUOTA

   Dopo aver aggiunto correttamente i dispositivi o i gruppi multicast, è possibile pianificare una sessione FUOTA. Per pianificare una sessione, esegui le operazioni descritte di seguito.

   1. Scegliere l'attività FUOTA per cui si desidera aggiornare il firmware del dispositivo, quindi scegliere Schedule FUOTA session (Pianifica sessione FUOTA).
   2. Specifica una Start date (Data di inizio) e una Start time (Ora di inizio) per la tua sessione FUOTA. Assicurati che l'ora di inizio sia posticipata di 30 o più minuti rispetto all'ora corrente.

Aggiunta di dispositivi a un'attività FUOTA e pianificazione di una sessione FUOTA utilizzando l'API

Puoi utilizzare l'API AWS IoT Wireless o la CLI per aggiungere dispositivi wireless o gruppi multicast all'attività FUOTA. È quindi possibile pianificare una sessione FUOTA.

1. Aggiunta di dispositivi e gruppi multicast

   È possibile associare dispositivi wireless o gruppi multicast all'attività FUOTA.

   - Per associare singoli dispositivi all'attività FUOTA, utilizza l'operazione API `AssociateWirelessDeviceWithFuotaTask` o il comando della CLI `associate-wireless-device-with-fuota-task` e inserisci `WirelessDeviceID` come input.

     ```
     aws iotwireless associate-wireless-device-with-fuota-task \
         --id "01a23cde-5678-4a5b-ab1d-33456808ecb2"
         --wireless-device-id "ab0c23d3-b001-45ef-6a01-2bc3de4f5333"
     ```

- Per associare gruppi multicast all'attività FUOTA, utilizza l'operazione API `AssociateMulticastGroupWithFuotaTask` o il comando della CLI `associate-multicast-group-with-fuota-task` e inserisci `MulticastGroupID` come input.

```
aws iotwireless associate-multicast-group-with-FUOTA-task \
    --id 01a23cde-5678-4a5b-ab1d-33456808ecb2"
    --multicast-group-id
```

Dopo aver associato i dispositivi wireless o il gruppo multicast all'attività FUOTA, utilizzare le seguenti operazioni API o comandi CLI per creare un elenco dei dispositivi o dei gruppi multicast, o per dissociarli dall'attività.

- `DisassociateWirelessDeviceFromFuotaTask` o `disassociate-wireless-device-from-fuota-task`
- `DisassociateMulticastGroupFromFuotaTask` o `disassociate-multicast-group-from-fuota-task`
- `ListWirelessDevices` o `list-wireless-devices`
- `ListMulticastGroups` o `list-multicast-groups-by-fuota-task`

> **Note**
>
> L'API:
>
> - `ListWirelessDevices` può fornire un elenco dei dispositivi wireless in generale e dei dispositivi associati a un gruppo multicast, quando `MulticastGroupID` viene utilizzato come filtro. L'API fornisce un elenco dei dispositivi wireless associati a un'attività FUOTA quando `FuotaTaskID` viene utilizzato come filtro.
> - `ListMulticastGroups` può fornire un elenco dei gruppi multicast in generale e dei gruppi multicast associati a un'attività FUOTA quando `FuotaTaskID` viene utilizzato come filtro.

2. Pianificazione della sessione FUOTA

Dopo aver aggiunto correttamente i dispositivi o i gruppi multicast all'attività FUOTA, è possibile avviare una sessione FUOTA per aggiornare il firmware del dispositivo. L'ora di inizio deve essere posticipata di 30 o più minuti rispetto all'ora corrente. Per pianificare una sessione

FUOTA utilizzando l'API o la CLI, utilizzare l'operazione API `StartFuotaTask` o il comando CLI `start-fuota-task`.

Dopo aver avviato una sessione FUOTA, non è più possibile aggiungere dispositivi o gruppi multicast all'attività. Puoi ottenere informazioni sullo stato della sessione FUOTA utilizzando l'operazione API `GetFuotaTask` o il comando CLI `get-fuota-task`.

Monitoraggio e risoluzione dello stato dell'attività FUOTA e dei dispositivi aggiunti all'attività

Dopo aver eseguito il provisioning dei dispositivi wireless e creato quanti gruppi multicast si desiderino utilizzare, è possibile avviare una sessione FUOTA eseguendo la procedura seguente.

Stato dell'attività FUOTA

L'attività FUOTA può mostrare nella AWS Management Console uno dei seguenti messaggi di stato.

- In attesa

  Questo stato indica che hai creato un'attività FUOTA, ma che l'attività è ancora sprovvista di una sessione di aggiornamento del firmware. Verrà visualizzato questo messaggio di stato quando il gruppo è stato creato. Nel frattempo, è possibile aggiornare l'attività FUOTA e associare o disassociare i dispositivi dal gruppo multicast o dall'attività. Dopo che lo stato è cambiato da Pending (In attesa), non possono essere aggiunti ulteriori dispositivi al gruppo.
- In attesa di sessione FUOTA

  Dopo che i tuoi dispositivi sono stati aggiunti con successo nell'attività FUOTA, quando l'attività ha una sessione di aggiornamento firmware pianificata verrà visualizzato questo messaggio di stato. Non è possibile, nel frattempo, aggiornare o aggiungere dispositivi alla sessione FUOTA. Se annulli la sessione FUOTA, lo stato del gruppo cambia in Pending (In attesa).
- In FUOTA session (In sessione FUOTA)

  All'inizio della sessione FUOTA, verrà visualizzato questo messaggio di stato. La sessione di frammentazione inizia e i dispositivi finali raccolgono i frammenti, ricostruiscono l'immagine del firmware, confrontano la nuova versione del firmware con la versione originale, e applicano la nuova immagine.
- Sessione FUOTA completata

Dopo che i dispositivi finali hanno segnalato a AWS IoT Core per LoRaWAN che è stata applicata la nuova immagine del firmware o, quando la sessione scade, la sessione FUOTA è contrassegnata come completata e il seguente stato sarà visibile.

Questo stato compare anche in uno dei seguenti casi, quindi assicurati di verificare se l'aggiornamento del firmware sia stato applicato correttamente ai dispositivi.

- Quando lo stato dell'attività FUOTA era FUOTA session waiting (In attesa di sessione FUOTA) e c'è un errore del bucket S3, ad esempio il collegamento al file immagine nel bucket S3 non è corretto o AWS IoT Core per LoRaWAN non dispone di autorizzazioni sufficienti per accedere al file nel bucket.
- Quando lo stato dell'attività FUOTA era FUOTA session waiting (In attesa di sessione FUOTA) e c'è una richiesta per avviare una sessione FUOTA, ma non viene ricevuta una risposta dai dispositivi o dai gruppi multicast nell'attività FUOTA.
- Quando lo stato dell'attività FUOTA era In FUOTA session (Sessione FUOTA in corso) e i dispositivi o i gruppi multicast non hanno inviato alcun frammento per un certo periodo di tempo, il che comporta il timeout della sessione.

- Delete waiting (Eliminazione attesa)

  Se elimini l'attività FUOTA che si trova in uno degli altri stati, verrà visualizzato questo stato. Un'operazione di eliminazione è permanente e non può essere annullata. Questa operazione può richiedere tempo e lo stato del gruppo sarà Delete Waiting (Eliminazione dell'attesa) fino a quando l'attività FUOTA non sarà eliminata. Dopo che l'attività FUOTA entra in questo stato, non può passare a uno degli altri stati.

Stato dei dispositivi in un'attività FUOTA

L'attività FUOTA può mostrare nella AWS Management Console uno dei seguenti messaggi di stato. È possibile passare il mouse su ciascun messaggio di stato per ottenere ulteriori informazioni su ciò che indica.

- Initial

  Quando è l'ora di inizio della sessione FUOTA, AWS IoT Core per LoRaWAN verifica che il dispositivo sia provvisto del pacchetto supportato per l'aggiornamento del firmware. Se il dispositivo è provvisto del pacchetto supportato, viene avviata la sessione FUOTA per il dispositivo.

L'immagine del firmware è frammentata e i frammenti vengono inviati al dispositivo. Quando viene visualizzato questo stato, significa che la sessione FUOTA per il dispositivo non è ancora iniziata.

- Package unsupported (Pacchetto non supportato)

  Se il dispositivo non dispone del pacchetto FUOTA supportato, verrà mostrato questo stato. Se il pacchetto di aggiornamento del firmware non è supportato, la sessione FUOTA del dispositivo non può essere avviata. Per risolvere questo errore, verifica che il firmware del dispositivo possa ricevere aggiornamenti firmware utilizzando FUOTA.

- Algoritmo di frammentazione non supportato

  All'inizio della sessione FUOTA, AWS IoT Core per LoRaWAN configura una sessione di frammentazione per il tuo dispositivo. Se viene visualizzato questo stato, significa che il tipo di algoritmo di frammentazione utilizzato non può essere applicato per l'aggiornamento del firmware del dispositivo. L'errore si verifica perché il dispositivo non dispone del pacchetto FUOTA supportato. Per risolvere questo errore, verifica che il firmware del dispositivo possa ricevere aggiornamenti firmware utilizzando FUOTA.

- Memoria insufficiente

  Dopo che AWS IoT Core per LoRaWAN invia i frammenti di immagine, i tuoi dispositivi finali li raccolgono e ricostruiscono l'immagine binaria da questi frammenti. Questo stato viene visualizzato quando il dispositivo non dispone di memoria sufficiente per assemblare i frammenti dell'immagine del firmware in arrivo, il che può comportare l'interruzione prematura della sessione di aggiornamento del firmware. Per risolvere l'errore, verificare che l'hardware del dispositivo possa ricevere questo aggiornamento. Se il dispositivo non è in grado di ricevere questo aggiornamento, utilizzare un'immagine delta per aggiornare il firmware.

- Indice di frammentazione non supportato

  L'indice di frammentazione identifica una delle quattro sessioni di frammentazione possibili eseguibili contemporaneamente. Se il dispositivo non supporta il valore dell'indice di frammentazione indicato, viene visualizzato questo stato. Per risolvere il problema, procedi in uno dei seguenti modi.

  - Avvia una nuova attività FUOTA per il dispositivo.
  - Se l'errore persiste, passa dalla modalità unicast a multicast.
  - Se l'errore non viene ancora risolto, controllare il firmware del dispositivo.

- Errori di memoria

Questo stato indica che il dispositivo ha riscontrato un errore di memoria durante la ricezione dei frammenti in arrivo da AWS IoT Core per LoRaWAN. Se si verifica questo errore, il dispositivo potrebbe non essere in grado di ricevere questo aggiornamento. Per risolvere l'errore, verificare che l'hardware del dispositivo possa ricevere questo aggiornamento. Se necessario, utilizzare un'immagine delta per aggiornare il firmware del dispositivo.

- Descrittore errato

  Il dispositivo non supporta il descrittore indicato. Il descrittore è un campo che descrive il file che verrà trasportato durante la sessione di frammentazione. Se vedi questo errore, contatta AWS Support Center.

- Replay conteggio sessioni

  Questo stato indica che il dispositivo ha precedentemente utilizzato questo conteggio di sessioni. Per risolvere il problema, avviare una nuova attività FUOTA per il dispositivo.

- Frammenti mancanti

  Mentre il dispositivo raccoglie i frammenti di immagine da AWS IoT Core per LoRaWAN, ricostruisce la nuova immagine del firmware da frammenti indipendenti e codificati. Se il dispositivo non ha ricevuto tutti i frammenti, la nuova immagine non potrà essere ricostruita e comparirà questo stato. Per risolvere il problema, avviare una nuova attività FUOTA per il dispositivo.

- MIC error (Errore MIC)

  Quando il dispositivo ricostruisce la nuova immagine del firmware dai frammenti raccolti, esegue un Message Integrity Check (MIC, Controllo Integrità Messaggi) per verificare l'autenticità dell'immagine e se quest'ultima proviene dalla sorgente corretta. Se il dispositivo rileva una mancata corrispondenza nel MIC dopo aver riassemblato i frammenti, viene mostrato il seguente stato. Per risolvere il problema, avviare una nuova attività FUOTA per il dispositivo.

- Successful (Riuscito)

  La sessione FUOTA per il tuo dispositivo ha avuto successo.

> **Note**
>
> Mentre questo messaggio di stato indica che i dispositivi hanno ricostruito l'immagine dai frammenti e l'hanno verificata, il firmware del dispositivo potrebbe non essere stato

aggiornato quando il dispositivo segnala lo stato a AWS IoT Core per LoRaWAN. Verificare se il firmware del dispositivo è stato aggiornato.

Passaggi successivi

Hai appreso i diversi stati dell'attività FUOTA e dei relativi dispositivi e come risolvere eventuali problemi. Per ulteriori informazioni su ciascuno di questi stati, consulta le Specifiche di trasporto frammentate del blocco dati LoRaWAN, TS004-1.0.0.

Monitoraggio del parco istanze di risorse wireless in tempo reale utilizzando l'analizzatore di rete

L'analizzatore di rete utilizza una connessione WebSocket di default per ricevere i registri dei messaggi di traccia in tempo reale per le risorse di connettività wireless. Utilizzando l'analizzatore di rete, è possibile aggiungere le risorse che si desidera monitorare, attivare una sessione di messaggistica di traccia e iniziare a ricevere messaggi di traccia in tempo reale.

Per monitorare le risorse, puoi utilizzare Amazon CloudWatch. Per utilizzare CloudWatch, è necessario impostare un ruolo IAM per configurare la registrazione e quindi attendere che le voci di registro vengano visualizzate nella console. L'analizzatore di rete riduce significativamente il tempo necessario per configurare una connessione e iniziare a ricevere messaggi di traccia, fornendo informazioni di registro just-in-time per il tuo parco istanze di risorse. Per informazioni sul monitoraggio usando CloudWatch, consulta Monitoraggio delle risorse AWS IoT Wireless con i file di log Amazon CloudWatch.

Riducendo i tempi di configurazione e utilizzando le informazioni dei messaggi di traccia, puoi monitorare le tue risorse in modo più efficace, ottenere informazioni significative e risolvere gli errori. È possibile monitorare sia i dispositivi LoRaWAN che i gateway LoRaWAN. Ad esempio, puoi identificare rapidamente un errore di adesione durante l'onboarding di uno dei tuoi dispositivi LoRaWAN. Per eseguire il debug dell'errore, utilizza le informazioni nel registro dei messaggi di traccia fornito.

Come usare l'analizzatore di rete

Per monitorare il parco istanze della risorsa e iniziare a ricevere messaggi di traccia, attenersi ai seguenti passaggi

1. Crea la configurazione dell'analizzatore di rete e aggiungi le risorse

Prima di poter attivare la messaggistica di traccia, crea una configurazione dell'analizzatore di rete e aggiungi le risorse alla configurazione. Innanzitutto, specifica le impostazioni di configurazione che includono i livelli di registro e le informazioni sul frame del dispositivo wireless. Quindi, aggiungi le risorse che vuoi monitorare utilizzando il gateway wireless e gli identificatori del dispositivo wireless.

2. Trasmetti i messaggi di traccia con WebSockets

   È possibile generare un URL di richiesta preimpostato utilizzando le credenziali per il ruolo IAM per trasmettere i messaggi di traccia dell'analizzatore di rete utilizzando il protocollo WebSocket.

3. Attiva la sessione di messaggistica di traccia e monitora i messaggi di traccia

   Per iniziare a ricevere messaggi di traccia, attiva la sessione di messaggistica di traccia. Per evitare costi aggiuntivi, è possibile disattivare o chiudere la sessione di messaggistica di traccia dell'analizzatore di rete.

Il seguente video descrive come lavora l'analizzatore di rete AWS IoT Core per LoRaWAN e ti guida attraverso il processo di aggiunta di risorse e di tracciamento delle attività congiunte utilizzando l'analizzatore di rete stesso.

Gli argomenti seguenti illustrano come creare la configurazione, aggiungere le risorse e attivare la sessione di messaggistica di traccia.

Argomenti

- Aggiunta del ruolo IAM necessario per l'analizzatore di rete
- Creazione di una configurazione dell'analizzatore di rete e aggiunta delle risorse
- Trasmetti messaggi di traccia dell'analizzatore di rete con WebSockets
- Visualizzazione e monitoraggio in tempo reale dei registri dei messaggi di tracciamento dell'analizzatore
- Esegui il debug e la risoluzione dei problemi dei gruppi multicast e delle attività FUOTA utilizzando l'analizzatore di rete

Aggiunta del ruolo IAM necessario per l'analizzatore di rete

Quando si utilizza l'analizzatore di rete, è necessario concedere a un utente l'autorizzazione per utilizzare le operazioni API UpdateNetworkAnalyzerConfiguration e GetNetworkAnalyzerConfiguration

per accedere alle risorse dell'analizzatore di rete. Di seguito vengono illustrate le policy IAM utilizzate per concedere le autorizzazioni.

Policy IAM per l'analizzatore di rete

Usa una delle seguenti opzioni:

- Policy wireless con accesso completo

  Concedi a AWS IoT Core per LoRaWAN la policy di accesso completo collegando la policy AWSIoTWirelessFullAccess al tuo ruolo. Per ulteriori informazioni, consulta la sezione Riepilogo delle policy `AWSIoTWirelessFullAccess`.
- Policy IAM con ambito per le API Get e Update

  Crea la seguente policy IAM nella scheda Visual editor (Editor visivo) della pagina Create policy (Crea policy) della console IAM:

  1. Scegli IoTWireless per Service (Servizio).
  2. In Access level (Livello di accesso) espandi Read (Lettura) e scegli GetNetworkAnalyzerConfiguration, quindi espandi Write (Scrittura) e scegli UpdateNetworkAnalyzerConfiguration.
  3. Scegli Next:Tags (Successivo: Tag) e inserisci un nome per la policy, ad esempio IoTWirelessNetworkAnalyzerPolicy. Scegli Crea policy.

  Di seguito viene illustrata la policy IoTWirelessNetworkAnalyzerPolicy che hai creato. Per ulteriori informazioni sulla creazione di una policy, consulta Creazione di policy IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "iotwireless:GetNetworkAnalyzerConfiguration",
                "iotwireless:UpdateNetworkAnalyzerConfiguration"
            ],
            "Resource": "*"
        }
    ]
}
```

Policy con ambito per accedere a risorse specifiche

Per configurare un controllo degli accessi più granulare, è necessario aggiungere i gateway e i dispositivi wireless al campo Resource (Risorsa). La seguente policy utilizza il carattere jolly per l'ARN per concedere l'accesso a tutti i gateway e i dispositivi. Puoi controllare l'accesso a gateway e dispositivi specifici utilizzando `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/*"
            ]
        }
    ]
}
```

Per concedere a un utente l'autorizzazione per utilizzare l'analizzatore di rete ma non per utilizzare gateway o dispositivi wireless, usa la seguente policy. Se non specificato, le autorizzazioni per l'utilizzo delle risorse sono implicitamente negate.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "iotwireless:GetNetworkAnalyzerConfiguration",
                "iotwireless:UpdateNetworkAnalyzerConfiguration"
            ],
            "Resource": [
                "arn:aws:iotwireless:*:{accountId}:NetworkAnalyzerConfiguration/*"
```

```
            ]
        }
    ]
}
```

Passaggi successivi

Ora che hai creato la policy, puoi aggiungere le risorse alla configurazione dell'analizzatore di rete e ricevere le informazioni della messaggistica di traccia per tali risorse. Per ulteriori informazioni, consultare Creazione di una configurazione dell'analizzatore di rete e aggiunta delle risorse.

Creazione di una configurazione dell'analizzatore di rete e aggiunta delle risorse

Prima di poter eseguire lo streaming dei messaggi di traccia, crea una configurazione dell'analizzatore di rete e aggiungi alla configurazione le risorse che vuoi monitorare. Quando crei una configurazione, puoi:

- Specificare un nome di configurazione e una descrizione facoltativa.
- Personalizzare le impostazioni di configurazione come le informazioni sul frame e il livello di dettaglio dei messaggi di registro.
- Aggiungere le risorse che vuoi monitorare. Le risorse possono essere dispositivi wireless o gateway wireless oppure entrambi.

Le impostazioni di configurazione specificate determinano le informazioni della messaggistica di traccia che ricevi per le risorse aggiunte alla configurazione. Puoi anche creare più configurazioni a seconda del caso d'uso di monitoraggio.

Di seguito viene illustrato come creare una configurazione e aggiungere le risorse.

Argomenti

Creazione di una configurazione dell'analizzatore di rete

Prima di poter monitorare i gateway wireless o i dispositivi wireless, è necessario creare una configurazione dell'analizzatore di rete. Quando crei la configurazione, devi solo specificare un

nome per la configurazione. Puoi personalizzare le impostazioni di configurazione e aggiungere alla configurazione le risorse che vuoi monitorare anche dopo la creazione. Le impostazioni di configurazione determinano le informazioni della messaggistica di traccia che ricevi per tali risorse.

A seconda delle risorse che vuoi monitorare e del livello di informazioni che desideri ricevere, puoi creare più configurazioni. Ad esempio, puoi creare una configurazione che visualizza solo le informazioni di errore per un set di gateway del tuo Account AWS. Puoi anche creare una configurazione che visualizza tutte le informazioni su un dispositivo wireless che vuoi monitorare.

Le sezioni seguenti mostrano le varie impostazioni di configurazione e come creare la configurazione.

Impostazioni di configurazione

Quando crei o aggiorni la configurazione dell'analizzatore di rete, puoi anche personalizzare i seguenti parametri per filtrare le informazioni sul flusso di registro.

- Informazioni sul frame

  Questa impostazione è l'informazione del frame per le risorse del dispositivo wireless per i messaggi di traccia. Le informazioni del frame possono essere utilizzate per eseguire il debug della comunicazione tra il server di rete e i dispositivi finali. È abilitato per impostazione predefinita.

- Livelli di log

  È possibile visualizzare i registri di informazioni o errori oppure disattivare la registrazione.

  - Info

    I registri con un livello di registro Informazioni sono più dettagliati e contengono i flussi di registro che sono informativi e contengono errori. I registri informativi possono essere utilizzati per visualizzare le modifiche allo stato di un dispositivo o di un gateway.

    > **Note**
    >
    > La raccolta di flussi di log più dettagliati può comportare costi aggiuntivi. Per ulteriori informazioni sui prezzi, consulta Prezzi di AWS IoT Core.

  - Errore

    Registri con un livello di log di Errore sono meno dettagliati e mostrano solo le informazioni sugli errori. È possibile utilizzare questi registri quando un'applicazione presenta un errore, ad

esempio un errore di connessione del dispositivo. Utilizzando le informazioni del flusso di log, è possibile identificare e risolvere gli errori relativi alle risorse del parco istanze.

Creazione di una configurazione utilizzando la console

È possibile creare una configurazione dell'analizzatore di rete e personalizzare i parametri opzionali utilizzando la console AWS IoT o l'API AWS IoT Wireless. Inoltre è possibile creare più configurazioni e successivamente eliminare le configurazioni che non vengono più utilizzate.

Creazione di una configurazione dell'analizzatore di rete

1. Apri l'hub dell'analizzatore di rete della console AWS IoT e scegli Crea configurazione.
2. Specifica le impostazioni di configurazione.
   - Nome, descrizione e tag

     Specifica un nome per la configurazione univoco che contenga solo lettere, numeri, trattini o caratteri di sottolineatura. Utilizza il campo Description (Descrizione) per fornire informazioni sulla configurazione e il campo Tags (Tag) per aggiungere coppie chiave-valore di metadati sulla configurazione. Per ulteriori informazioni sulla denominazione e sulla descrizione delle risorse, consulta Descrizione delle risorse AWS IoT Wireless.
   - Impostazioni di configurazione

     Scegli se disabilitare le informazioni del frame e utilizzare Select log levels (Seleziona i livelli di registro) per scegliere i livelli di registro da usare per i registri dei messaggi di traccia. Seleziona Avanti.
3. Aggiungi le risorse alla configurazione. Puoi aggiungere le tue risorse ora o scegliere Create (Crea) e aggiungerle in un secondo momento. Per aggiungere le risorse in un secondo momento, scegli Create (Crea).

   Nella pagina dell'hub dell'analizzatore di rete viene visualizzata la configurazione creata insieme alle relative impostazioni. Per visualizzare i dettagli della nuova configurazione, scegli il nome della configurazione.

Eliminazione della configurazione dell'analizzatore di rete

È possibile creare più configurazioni dell'analizzatore di rete a seconda delle risorse che vuoi monitorare e del livello di informazioni sulla messaggistica di traccia che vuoi ricevere.

Per rimuovere le configurazioni dalla console

1. Apri l'hub dell'analizzatore di rete della console AWS IoT e scegli la configurazione che vuoi rimuovere.
2. Scegli Actions (Operazioni), quindi Delete (Elimina).

Creazione di una configurazione utilizzando l'API

Per creare una configurazione dell'analizzatore di rete con l'API, utilizza l'operazione API CreateNetworkAnalyzerConfiguration o il comando create-network-analyzer-configuration dell'interfaccia a riga di comando.

Quando crei la configurazione, devi solo specificare un nome per la configurazione. Puoi utilizzare questa operazione API anche per specificare le impostazioni di configurazione e aggiungere le risorse durante la creazione della configurazione. In alternativa, puoi specificarle in un secondo momento utilizzando l'operazione API UpdateNetworkAnalyzerConfiguration o il comando update-network-analyzer-configuration dell'interfaccia a riga di comando.

- Creazione di una configurazione

  Quando crei la configurazione, devi specificare un nome. Il comando seguente crea ad esempio una configurazione semplicemente fornendo un nome e una descrizione facoltativa. Per impostazione di default, la configurazione ha le informazioni del frame attivate e utilizza il livello di registro `INFO`.

  ```
  aws iotwireless create-network-analyzer-configuration \
      --configuration-name My_Network_Analyzer_Config \
      --description "My first network analyzer configuration"
  ```

  L'esecuzione di questo comando visualizza l'ARN e l'ID della configurazione dell'analizzatore di rete.

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

- Creazione di una configurazione con le risorse

Per personalizzare queste impostazioni di configurazione, utilizza il parametro `trace-content`. Per aggiungere risorse, utilizza i parametri `WirelessDevices` e `WirelessGateways` per specificare i gateway, i dispositivi oppure entrambi, che vuoi aggiungere alla configurazione. Ad esempio, il seguente comando personalizza le impostazioni di configurazione e aggiunge alla configurazione le risorse wireless, specificate da `WirelessGatewayID` e `WirelessDeviceID`.

```
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"
```

L'esempio seguente mostra l'output dell'esecuzione del comando:

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

Elenco delle configurazioni dell'analizzatore di rete

È possibile creare più configurazioni dell'analizzatore di rete in base alle risorse che vuoi monitorare e al livello di dettaglio delle informazioni sulla messaggistica di traccia che vuoi ricevere per le risorse. Dopo aver creato le configurazioni, puoi utilizzare l'operazione API ListNetworkAnalyzerConfigurations o il comando list-network-analyzer-configuration dell'interfaccia a riga di comando per ottenere l'elenco delle configurazioni.

```
aws iotwireless list-network-analyzer-configurations
```

L'esecuzione di questo comando visualizza tutte le configurazioni dell'analizzatore di rete nel tuo Account AWS. Puoi anche utilizzare il parametro `max-results` per specificare quante configurazioni vuoi visualizzare. L'esempio seguente mostra l'output dell'esecuzione del 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"
      }
   ]
}
```

Eliminazione della configurazione dell'analizzatore di rete

È possibile eliminare una configurazione che non serve più con l'operazione API DeleteNetworkAnalyzerConfiguration o il comando delete-network-analyzer-configuration dell'interfaccia a riga di comando.

```
aws iotwireless delete-network-analyzer-configuration \
    --configuration-name My_NetworkAnalyzer_Config
```

L'esecuzione di questo comando non produce output. Per visualizzare le configurazioni disponibili, puoi utilizzare l'operazione API `ListNetworkAnalyzerConfigurations`.

Passaggi successivi

Ora che hai creato una configurazione dell'analizzatore di rete, puoi aggiungere le risorse alla configurazione o aggiornare le impostazioni di configurazione. Per ulteriori informazioni, consultare Aggiunta di risorse e aggiornamento della configurazione dell'analizzatore di rete.

Aggiunta di risorse e aggiornamento della configurazione dell'analizzatore di rete

Prima di poter attivare la messaggistica di traccia, è necessario aggiungere risorse alla configurazione. È possibile utilizzare solo una singola configurazione predefinita dell'analizzatore di rete. AWS IoT Core per LoRaWAN assegna il nome, NetworkAnalyzerConfig_Default, per questa configurazione e questo campo non può essere modificato. Questa configurazione viene aggiunta automaticamente al tuo Account AWS quando si utilizza l'analizzatore di rete dalla console.

È possibile aggiungere le risorse che desideri monitorare a questa configurazione predefinita. Le risorse possono essere uno o entrambi i dispositivi LoRaWAN e i gateway LoRaWAN. Per

aggiungere ogni singola risorsa alla configurazione, utilizza il gateway wireless e gli identificatori del dispositivo wireless.

Impostazioni di configurazione

Per configurare le impostazioni, aggiungi innanzitutto risorse alla configurazione di default e attiva la messaggistica di traccia. Dopo aver ricevuto i registri dei messaggi di traccia, puoi anche personalizzare i seguenti parametri per aggiornare la configurazione di default e filtrare il flusso di log.

- Informazioni sul frame

  Questa impostazione è l'informazione del frame delle risorse del dispositivo wireless per i messaggi di traccia. Le informazioni sul frame sono abilitate per impostazione predefinita e possono essere utilizzate per eseguire il debug della comunicazione tra il server di rete e i dispositivi finali.

- Livelli di log

  È possibile visualizzare i registri di informazioni o errori oppure disattivare la registrazione.

  - Info

    Registri con un livello di log di Informazioni sono più dettagliati e contengono flussi di log che sono informativi e contengono errori. I log informativi possono essere utilizzati per visualizzare le modifiche allo stato di un dispositivo o di un gateway.

    > **Note**
    >
    > La raccolta di flussi di log più dettagliati può comportare costi aggiuntivi. Per ulteriori informazioni sui prezzi, consulta Prezzi di AWS IoT Core.

  - Errore

    Registri con un livello di log di Errore sono meno dettagliati e mostrano solo le informazioni sugli errori. È possibile utilizzare questi registri quando un'applicazione presenta un errore, ad esempio un errore di connessione del dispositivo. Utilizzando le informazioni del flusso di log, è possibile identificare e risolvere gli errori relativi alle risorse del parco istanze.

Prerequisiti

Prima di poter aggiungere risorse, è necessario aver integrato i gateway e i dispositivi che desideri monitorare a AWS IoT Core per LoRaWAN. Per ulteriori informazioni, consultare Collegamento di gateway e dispositivi ad AWS IoT Core per LoRaWAN.

Aggiungi risorse e aggiorna la configurazione dell'analizzatore di rete utilizzando la console

È possibile aggiungere risorse e personalizzare i parametri opzionali utilizzando la console AWS IoT o l'API AWS IoT Wireless. Oltre alle risorse, puoi anche modificare le impostazioni di configurazione e salvare la configurazione aggiornata.

Per aggiungere risorse alla configurazione (console)

1. Apri l'hub dell'analizzatore di rete della console AWS IoT e scegli la configurazione dell'analizzatore di rete, Network AnalyzerConfig_Default.
2. Scegli Aggiungi risorse.
3. Aggiungi le risorse che vuoi monitorare utilizzando il gateway wireless e gli identificatori del dispositivo wireless. È possibile aggiungere fino a 250 gateway wireless o dispositivi wireless. Per aggiungere la tua risorsa:
   a. Utilizza Visualizza gateway o la scheda Visualizzazione dei dispositivi per visualizzare l'elenco dei gateway e dei dispositivi che hai aggiunto al tuo Account AWS.
   b. Copia il `WirelessDeviceID` o il `WirelessGatewayID` del dispositivo o del gateway che desideri monitorare e inserisci il valore identificativo per la risorsa corrispondente.
   c. Per continuare ad aggiungere risorse, scegli Aggiungi gateway o Aggiungi dispositivo e aggiungi il gateway o il dispositivo wireless. Se hai aggiunto una risorsa che non vuoi più monitorare, scegli Rimozione della risorsa.
4. Dopo aver aggiunto tutte le risorse, scegli Aggiungi.

   Vedrai il numero di gateway e dispositivi che hai aggiunto nella Pagina hub dell'analizzatore di rete. È comunque possibile continuare ad aggiungere gateway e dispositivi fino a quando non si attiva la sessione di messaggistica di traccia. Dopo che la sessione è stata attivata, per aggiungere risorse, dovrai disattivare la sessione.

Per modificare la configurazione dell'analizzatore di rete (console)

È inoltre possibile modificare la configurazione dell'analizzatore di rete e scegliere se disabilitare le informazioni sui frame e il livello di log per i registri dei messaggi di traccia.

1. Apri l'hub dell'analizzatore di rete della console AWS IoT e scegli la configurazione dell'analizzatore di rete, Network AnalyzerConfig_Default.
2. Scegli Modifica.
3. Scegli se disabilitare le informazioni sul fotogramma e utilizzare Seleziona i livelli di log per scegliere i livelli di log da utilizzare per i log dei messaggi di traccia. Selezionare Salva.

   Vedrete le impostazioni di configurazione specificate nella pagina dei dettagli della configurazione dell'analizzatore di rete.

Aggiungi risorse e aggiorna la configurazione dell'analizzatore di rete utilizzando l'API

Puoi utilizzare le operazioni API AWS IoT Wireless o i Comandi della CLI AWS IoT Wireless per aggiungere risorse e aggiornare le impostazioni di configurazione per la configurazione dell'analizzatore di rete.

- Per aggiungere risorse e aggiornare la configurazione dell'analizzatore di rete, utilizzare l'API UpdateNetworkAnalyzerConfiguration o la CLI update-network-analyzer-configuration.
  - Aggiungi risorse

    Per i dispositivi wireless che vuoi aggiungere, usa `WirelessDevicesToAdd` per inserire il `WirelessDeviceID` per i dispositivi come una serie di stringhe. Per i gateway wireless che vuoi aggiungere, usa `WirelessGatewaysToAdd` per inserire il `WirelessGatewayID` per i gateway come una serie di stringhe.
  - Modifica configurazione

    Per modificare la configurazione dell'analizzatore di rete, utilizza il parametro `TraceContent` per specificare se `WirelessDeviceFrameInfo` dovrebbe essere `ENABLED` o `DISABLED`, e se il parametro `LogLevel` dovrebbe essere `INFO`, `ERROR`, oppure `DISABLED`.

```
{
   "TraceContent": {
      "LogLevel": "string",
      "WirelessDeviceFrameInfo": "string"
   },
   "WirelessDevicesToAdd": [ "string" ],
   "WirelessDevicesToRemove": [ "string" ],
```

```
   "WirelessGatewaysToAdd": [ "string" ],
   "WirelessGatewaysToRemove": [ "string" ]
}
```

- Per ottenere informazioni sulla configurazione e sulle risorse che hai aggiunto, usa l'operazione API GetNetworkAnalyzerConfiguration o il comando get-network-analyzer-configuration. Fornire il nome della configurazione dell'analizzatore di rete, `NetworkAnalyzerConfig_Default`, come input.

Passaggi successivi

Dopo aver aggiunto risorse e specificato eventuali impostazioni di configurazione opzionali per la configurazione, è possibile utilizzare il protocollo WebSocket per stabilire una connessione con AWS IoT Core per LoRaWAN per l'utilizzo dell'analizzatore di rete. È quindi possibile attivare la messaggistica di traccia e iniziare a ricevere messaggi di traccia per le risorse. Per ulteriori informazioni, consultare Trasmetti messaggi di traccia dell'analizzatore di rete con WebSockets.

Trasmetti messaggi di traccia dell'analizzatore di rete con WebSockets

Quando si utilizza il protocollo WebSocket, è possibile eseguire lo streaming di messaggi di traccia dell'analizzatore di rete in tempo reale. Quando invii una richiesta, il servizio risponde con una struttura JSON. Dopo aver attivato la messaggistica di traccia, è possibile utilizzare i registri dei messaggi per ottenere informazioni sulle risorse e risolvere gli errori. Per ulteriori informazioni, consulta protocollo WebSocket.

Di seguito viene illustrato come eseguire lo streaming dei messaggi di traccia dell'analizzatore di rete con WebSockets.

Argomenti

- Genera una richiesta prefirmata con la libreria WebSocket
- Messaggi WebSocket e codici di stato

Genera una richiesta prefirmata con la libreria WebSocket

Di seguito viene illustrato come generare una richiesta prefirmata in modo da poter utilizzare la libreria WebSocket per inviare richieste al servizio.

Aggiunta di una policy per le richieste WebSocket al ruolo IAM

Per utilizzare il protocollo WebSocket per chiamare, collegare la seguente policy al ruolo AWS Identity and Access Management (IAM) che effettua la richiesta.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iotwireless:StartNetworkAnalyzerStream",
            "Resource": "*"
        }
    ]
}
```

Creare un URL prefirmato

Crea un URL per la richiesta WebSocket che contiene le informazioni necessarie per configurare le comunicazioni tra l'applicazione e l'analizzatore di rete. Per verificare l'identità della richiesta, lo streaming WebSocket utilizza il processo Amazon Signature Version 4 per la firma delle richieste. Per ulteriori informazioni riguardo Signature Version 4, consulta Firma di richieste API AWS nei Riferimenti generali di Amazon Web Services.

Per chiamare l'analizzatore di rete, utilizzare l'URL della richiesta `StartNetworkAnalyzerStream`. La richiesta verrà firmata utilizzando le credenziali per il ruolo IAM citato in precedenza. L'URL ha il formato seguente con l'aggiunta di interruzioni di riga per la leggibilità.

```
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
```

Utilizza i valori seguenti per i parametri Signature Version 4:

- X-Amz-Algorithm - L'algoritmo utilizzato nel processo di firma. L'unico valore valido è `AWS4-HMAC-SHA256`.

- X-Amz-Credential - Una stringa separata dalle barre ("/") che è formata concatenando i componenti ID chiave di accesso e componenti dell'ambito delle credenziali. L'ambito delle credenziali include la data nel formato AAAAMMGG, la regione AWS, il nome del servizio e una stringa di chiusura speciale (aws4_request).
- X-Amz-Date — La data e l'ora di creazione della firma. Genera la data e l'ora seguendo le istruzioni riportate in Gestione delle date in Signature Version 4 nei Riferimenti generali di Amazon Web Services.
- X-Amz-Expires - L'intervallo di tempo in secondi fino alla scadenza delle credenziali. Il valore massimo è di 300 secondi (5 minuti).
- X-Amz-Security-Token - (opzionale) Un token Signature Version 4 per le credenziali provvisorie. Se specifichi questo parametro, lo devi includere nella richiesta canonica. Per ulteriori informazioni, vedi Richiesta di credenziali di sicurezza temporanee nella Guida per l'utente di AWS Identity and Access Management.
- X-Amz-Signature - La firma Signature Version 4 generata per la richiesta.
- X-Amz-SignedHeaders - Le intestazioni firmate durante la creazione della firma per la richiesta. L'unico valore valido è `host`.

Crea l'URL della richiesta e crea la firma Signature Version 4

Per creare l'URL per la richiesta e creare la firma Signature Version 4, utilizzare la procedura seguente. Gli esempi sono in pseudocodice.

Fase 1. Creazione di una richiesta canonica

Creare una stringa che include informazioni dalla richiesta in un formato standardizzato. In questo modo si ha la certezza che quando AWS riceve la richiesta, può calcolare la stessa firma già calcolata in Task 3: calcolo della firma. Per ulteriori informazioni, consulta Creazione di una richiesta canonica per Signature Version 4 nei Riferimenti generali di Amazon Web Services.

1. Definire le variabili per la richiesta nell'applicazione.

```
# HTTP verb
method = "GET"
# Service name
service = "iotwireless"
# Regione AWS
region = "Regione 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. Crea un URI canonico (identificatore uniforme della risorsa). L'URI canonico è la parte dell'URI tra il dominio e la stringa di query.

```
canonical_uri = "/start-network-analyzer-stream"
```

3. Crea le intestazioni canoniche e le intestazioni firmate. Notare la \n in coda nelle intestazioni canoniche.

   - Aggiungi il nome dell'intestazione in caratteri minuscoli seguito da due punti.
   - Aggiungi un elenco separato da virgole di valori per l'intestazione. Non ordinare i valori nelle intestazioni che presentano più valori.
   - Aggiungi una nuova riga (\n).

```
canonical_headers = "host:" + host + "\n"
signed_headers = "host"
```

4. Eseguire la corrispondenza dell'algoritmo con l'algoritmo hash. È necessario utilizzare SHA-256.

```
algorithm = "AWS4-HMAC-SHA256"
```

5. Creare l'ambito delle credenziali che definisce gli ambiti della chiave derivata per la data, la regione e i servizi per cui è stata effettuata la richiesta.

```
credential_scope = datestamp + "/" + region + "/" + service + "/" + "aws4_request"
```

6. Creare la stringa di query canonica. I valori della stringa di query devono essere codificati in base all'URI e ordinati in base al nome.

   - Organizza i nomi dei parametri per punto di codice carattere in ordine crescente. I parametri con nomi duplicati devono essere ordinati in base al valore. Ad esempio, un nome di

parametro che inizia con la lettera maiuscola F precede un nome di parametro che inizia con la lettera minuscola b.

- Non codificare i caratteri non riservati definiti da RFC 3986: A-Z, a-z, 0-9, trattino (-), trattino basso (_), punto (.), e tilde (~).
- Codifica tutti gli altri caratteri con codifica percentuale con %XY, dove X e Y sono caratteri esadecimali (0-9 e A-F maiuscole). Ad esempio, i caratteri di spaziatura devono essere codificati come %20 (non utilizzando '+', come in alcuni schemi di codifica) e i caratteri UTF-8 estesi devono essere nel formato %XY%ZA%BC.
- Esegui la doppia codifica di qualsiasi carattere uguale (=) nei valori dei parametri.

```
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. Creare un hash di payload. Per una richiesta GET, il payload è una stringa vuota.

```
payload_hash = HashSHA256(("").Encode("utf-8")).HexDigest()
```

8. Combina tutti gli elementi per creare la richiesta canonica.

```
canonical_request = method + '\n'
   + canonical_uri + '\n'
   + canonical_querystring + '\n'
   + canonical_headers + '\n'
   + signed_headers + '\n'
   + payload_hash
```

Fase 2. Creazione della stringa da firmare.

La stringa per la firma contiene le meta informazioni che interessano la richiesta. È possibile utilizzare la stringa per firmare il passaggio successivo quando si calcola la firma della richiesta. Per ulteriori

informazioni, consulta Creazione di una stringa da firmare per Signature Version 4 nei Riferimenti generali di Amazon Web Services.

```
string_to_sign=algorithm + "\n"
   + amz_date + "\n"
   + credential_scope + "\n"
   + HashSHA256(canonical_request.Encode("utf-8")).HexDigest()
```

Task 3: calcolo della firma

Si ricava una chiave di firma dalla chiave di accesso segreta di AWS. La chiave derivata è specifica per la data, il servizio e la Regione AWS per un maggior livello di protezione. È possibile utilizzare la chiave derivata per firmare la richiesta. Per ulteriori informazioni, consulta Calcola la firma per firma per Signature Version 4 di AWS nei Riferimenti generali di Amazon Web Services.

Il codice presuppone che sia stata implementata la funzione `GetSignatureKey` per ottenere una chiave di firma. Per ulteriori informazioni e funzioni di esempio, consulta Esempi di come si ottiene una chiave di firma per Signature Version 4 nei Riferimenti generali di Amazon Web Services.

La funzione `HMAC(key, data)` rappresenta una funzione HMAC-SHA256 che restituisce i risultati in formato binario.

```
#Create the signing key
signing_key = GetSignatureKey(secret_key, datestamp, region, service)

# Sign the string_to_sign using the signing key
signature = HMAC.new(signing_key, (string_to_sign).Encode("utf-8"), Sha256()).HexDigest
```

Processo 4: Aggiunta delle informazioni sulla firma per la richiesta e la creazione della richiesta URL

Dopo aver calcolato la firma, aggiungerla alla stringa di query. Per ulteriori informazioni, consulta Aggiungere la firma alla richiesta nei Riferimenti generali di 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
```

Passaggi successivi

È possibile utilizzare l'URL della richiesta con la libreria WebSocket per effettuare la richiesta al servizio e osservare i messaggi. Per ulteriori informazioni, consultare Messaggi WebSocket e codici di stato.

Messaggi WebSocket e codici di stato

Dopo aver creato una richiesta prefirmata, è possibile utilizzare l'URL della richiesta con la libreria WebSocket, , o una libreria adatta al linguaggio di programmazione, per effettuare richieste al servizio. Per ulteriori informazioni su come generare questa richiesta prefirmata, consulta Genera una richiesta prefirmata con la libreria WebSocket.

Messaggi WebSocket

Stabilire una connessione bidirezionale utilizzando il protocollo WebSocket. I messaggi possono essere trasmessi da client a server e da server a client. Tuttavia, l'analizzatore di rete supporta solo i messaggi inviati dal server al client. Qualsiasi messaggio ricevuto dal client è imprevisto e il server chiuderà automaticamente la connessione WebSocket se un messaggio viene ricevuto dal client.

Quando la richiesta viene ricevuta e viene avviata una sessione di messaggistica di traccia, il server risponde con una struttura JSON, ovvero il payload. Per ulteriori informazioni sul payload e su come attivare i messaggi di traccia dal AWS Management Console, consulta Visualizzazione e monitoraggio in tempo reale dei registri dei messaggi di tracciamento dell'analizzatore.

Codici di stato WebSocket

Di seguito sono riportati i codici di stato WebSocket per la comunicazione dal server al client. I codici di stato WebSocket seguono il RFC Standard di chiusura normale dei collegamenti.

Di seguito sono riportati i codici di stato supportati:

- 1000

  Questo codice di stato indica una chiusura normale, il che significa che la connessione WebSocket è stata stabilita e che la richiesta è stata soddisfatta. Questo stato può essere osservato quando una sessione è inattiva, causando il timeout della connessione.
- 1002

  Questo codice di stato indica che l'endpoint sta terminando la connessione a causa di un errore di protocollo.

- 1003

  Questo codice di stato indica uno stato di errore in cui l'endpoint ha terminato la connessione perché ha ricevuto dati in un formato che non è in grado di accettare. L'endpoint supporta solo i dati di testo e potrebbe visualizzare questo codice di stato se riceve un messaggio binario o un messaggio dal client che utilizza un formato non supportato.

- 1008

  Questo codice di stato indica uno stato di errore in cui l'endpoint ha terminato la connessione perché ha ricevuto un messaggio che viola la policy Questo stato è generico e viene visualizzato quando gli altri codici di stato, come 1003 o 1009, non sono applicabili. Questo stato viene visualizzato anche se è necessario nascondere la policy o quando si verifica un errore di autorizzazione, ad esempio una firma scaduta.

- 1011

  Questo codice di stato indica uno stato di errore in cui il server sta terminando la connessione perché ha riscontrato una condizione imprevista o un errore interno che ha impedito di soddisfare la richiesta.

Passaggi successivi

Ora che hai imparato come generare una richiesta prefirmata e come osservare i messaggi dal server utilizzando la connessione WebSocket, puoi attivare la messaggistica di traccia e iniziare a ricevere i registri dei messaggi per il gateway wireless e le risorse del dispositivo wireless. Per ulteriori informazioni, consultare Visualizzazione e monitoraggio in tempo reale dei registri dei messaggi di tracciamento dell'analizzatore.

Visualizzazione e monitoraggio in tempo reale dei registri dei messaggi di tracciamento dell'analizzatore

Se hai aggiunto risorse alla configurazione dell'analizzatore di rete, puoi attivare la messaggistica di traccia per iniziare a ricevere messaggi di traccia per le tue risorse. È possibile utilizzare il AWS Management Console, l'API AWS IoT Wireless o la AWS CLI.

Prerequisiti

Prima di poter attivare la messaggistica di traccia utilizzando l'analizzatore di rete, devi aver:

- Aggiunto le risorse che vuoi far monitorare alla configurazione predefinita dell'analizzatore di rete. Per ulteriori informazioni, consultare Aggiunta di risorse e aggiornamento della configurazione dell'analizzatore di rete.
- Generato una richiesta prefirmata utilizzando l'URL della richiesta `StartNetworkAnalyzerStream`. La richiesta verrà firmata utilizzando le credenziali per il ruolo AWS Identity and Access Management che fa questa richiesta. Per ulteriori informazioni, consultare Creare un URL prefirmato.

Attiva la messaggistica di traccia utilizzando la console

Per attivare la messaggistica di traccia

1. Apri l'hub dell'analizzatore di rete della console AWS IoT e scegli la configurazione dell'analizzatore di rete, Network AnalyzerConfig_Default.
2. Nella pagina dei dettagli della configurazione dell'analizzatore di rete, scegli Attiva la messaggistica di traccia quindi scegli Attivare.

   Inizierai a ricevere messaggi di traccia in cui viene visualizzato per primo il messaggio di traccia più recente nella console.

   > **Note**
   >
   > Dopo l'avvio della sessione di messaggistica, la ricezione di messaggi di traccia può comportare costi aggiuntivi fino a quando non si disattiva la sessione o si lascia la sessione di traccia. Per ulteriori informazioni sui prezzi, consulta Prezzi di AWS IoT Core.

Visualizza e monitora i messaggi di traccia

Dopo aver attivato la messaggistica di traccia, viene stabilita la connessione WebSocket e i messaggi di traccia iniziano a comparire in tempo reale, prima i più recenti. È possibile personalizzare le preferenze per specificare il numero di messaggi di traccia da visualizzare in ogni pagina e visualizzare solo i campi pertinenti per ciascun messaggio. Ad esempio, è possibile personalizzare il registro dei messaggi di traccia per mostrare solo i registri per le risorse del gateway wireless che hanno Livello di log impostato su `ERROR`, in modo da poter identificare ed eseguire il debug rapidamente degli errori con i gateway. I messaggi di traccia contengono le informazioni seguenti.

- Numero messaggio: un numero univoco che mostra per primo l'ultimo messaggio ricevuto.

- ID risorsa: Il gateway wireless o l'ID del dispositivo wireless della risorsa.
- Timestamp: L'ora in cui il messaggio è stato ricevuto.
- ID messaggio: un identificatore che AWS IoT Core per LoRaWAN assegna a ciascun messaggio ricevuto.
- FPort: La porta di frequenza per comunicare con il dispositivo utilizzando la connessione WebSocket.
- DevEui: Identificatore univoco esteso (EUI) per il dispositivo wireless.
- Risorsa: Se la risorsa monitorata è un dispositivo wireless o un gateway wireless.
- Evento: evento per un messaggio di registro per un dispositivo wireless, che può essere Unisciti, Unisciti di nuovo, Uplink_Data, Downlink_Data, oppure Registrazione.
- Livello di log:Informazioni su flussi di log di `INFO` o `ERROR` per il tuo dispositivo.

Messaggio di log JSON dell'analizzatore di rete

È inoltre possibile scegliere un messaggio di traccia alla volta per visualizzare il payload JSON per quel messaggio. A seconda del messaggio selezionato nei registri dei messaggi di traccia, verranno visualizzate le informazioni nel payload JSON che indica che contiene 2 parti: Customerlog e LoRaFrame.

CustomerLog

La parte CustomerLog del JSON visualizza il tipo e l'identificatore della risorsa che ha ricevuto il messaggio, il livello di registro e il contenuto del messaggio. Nell'esempio seguente viene mostrato un messaggio di log CustomerLog . Puoi utilizzare il campo `message` nel JSON per ottenere ulteriori informazioni sull'errore e su come può essere risolto.

LoRaFrame

La parte LoRaFrame del JSON ha un Messaggio ID e contiene informazioni sul payload fisico per il dispositivo e i metadati wireless.

Il seguente esempio illustra la struttura del messaggio di traccia.

```
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;
  },
};
```

Revisione e passaggi successivi

In questa sezione, hai visualizzato i messaggi di traccia e hai appreso come utilizzare le informazioni per eseguire il debug degli errori. Dopo aver visualizzato tutti i messaggi, è possibile:

- Disattivare i messaggi di traccia

  Per evitare costi aggiuntivi, è possibile disattivare la sessione di messaggistica di traccia. La disattivazione della sessione disconnette la connessione WebSocket in modo da non ricevere alcun messaggio di traccia aggiuntivo. È comunque possibile continuare a visualizzare i messaggi esistenti nella console.
- Modifica le informazioni sul frame per la tua configurazione

  È possibile modificare la configurazione dell'analizzatore di rete e scegliere se disattivare le informazioni sui frame e scegliere i livelli di registro per i messaggi. Prima di aggiornare la configurazione, prendi in considerazione la possibilità di disattivare la sessione di messaggistica di traccia. Per apportare queste modifiche, apri la Pagina dei dettagli dell'analizzatore di rete nella

console AWS IoT e scegli Modificare. È quindi possibile aggiornare la configurazione con le nuove impostazioni di configurazione e attivare la messaggistica di traccia per visualizzare i messaggi aggiornati.

- Aggiungere risorse alla configurazione

  È inoltre possibile aggiungere altre risorse alla configurazione dell'analizzatore di rete e monitorarle in tempo reale. È possibile aggiungere fino a un totale di 250 risorse wireless gateway e dispositivi wireless combinati. Per aggiungere risorse, sulla Pagina dei dettagli dell'analizzatore di reye della console AWS IoT, scegli la scheda Risorse e scegli Aggiungere risorse. È quindi possibile aggiornare la configurazione con le nuove risorse e attivare la messaggistica di traccia per visualizzare i messaggi aggiornati per le risorse aggiuntive.

Per ulteriori informazioni sull'aggiornamento della configurazione dell'analizzatore di rete modificando le impostazioni di configurazione e l'aggiunta di risorse, consultare Aggiunta di risorse e aggiornamento della configurazione dell'analizzatore di rete.

Esegui il debug e la risoluzione dei problemi dei gruppi multicast e delle attività FUOTA utilizzando l'analizzatore di rete

Tra le risorse wireless che puoi monitorare ci sono dispositivi LoRaWAN, gateway LoRaWAN e gruppi multicast. Puoi anche utilizzare l'analizzatore di rete per eseguire il debug e la risoluzione di eventuali problemi che riscontri con la tua attività FUOTA. Puoi anche monitorare e tenere traccia dei messaggi relativi alla configurazione, alla trasmissione dei dati e alle query di stato mentre l'attività FUOTA è in corso.

Se l'attività FUOTA contiene gruppi multicast, per monitorarla è necessario aggiungere alla configurazione dell'analizzatore di rete sia il gruppo multicast sia i dispositivi del gruppo. È inoltre necessario attivare le informazioni sui frame e sui frame multicast per tenere traccia dei messaggi di uplink e downlink unicast e multicast scambiati con il gruppo multicast e i dispositivi mentre l'operazione FUOTA è in corso.

Per monitorare i gruppi multicast, puoi aggiungerli alla configurazione del tuo analizzatore di rete e utilizzare le informazioni sui frame multicast per risolvere i problemi dei messaggi di downlink multicast inviati a questi gruppi. Per la risoluzione dei problemi dei dispositivi che tentano di entrare in un gruppo nel quale viene utilizzata la comunicazione unicast, è necessario includere anche questi dispositivi nella configurazione dell'analizzatore di rete. Per monitorare solo la comunicazione unicast con i dispositivi del gruppo, attiva le informazioni sui frame per i tuoi dispositivi wireless. Questo

approccio garantisce monitoraggio e diagnostica completi sia per i gruppi multicast sia per i dispositivi che vengono aggiunti al gruppo.

Le sezioni seguenti descrivono come eseguire il debug e la risoluzione dei problemi dei gruppi multicast e delle attività FUOTA utilizzando l'analizzatore di rete.

Argomenti

Debug delle attività FUOTA che contengono solo dispositivi

È possibile utilizzare l'analizzatore di rete per eseguire il debug di un'attività FUOTA a cui sono stati aggiunti solo dispositivi LoRaWAN. Per informazioni sull'aggiunta di dispositivi a un'attività FUOTA, consulta Aggiunta di dispositivi e gruppi multicast per un'attività FUOTA e pianificazione di una sessione FUOTA. Per eseguire il debug dell'attività FUOTA, procedi come segue:

1. Crea una configurazione dell'analizzatore di rete attivando le informazioni sui frame per i dispositivi wireless, così da poter monitorare i messaggi di uplink e downlink FUOTA che vengono scambiati con i dispositivi mentre l'attività è in corso.
2. Aggiungi alla configurazione dell'analizzatore di rete i dispositivi nell'attività FUOTA utilizzando i relativi identificatori di dispositivi wireless.
3. Attiva la messaggistica di traccia per iniziare a ricevere messaggi di traccia per i dispositivi presenti nella configurazione dell'analizzatore di rete.

Nella colonna `applicationCommandType` delle informazioni sui messaggi di traccia, inizierai a ricevere messaggi di downlink unicast relativi alla trasmissione e alla configurazione della frammentazione dei dati.

> **Note**
>
> Se non vedi la colonna `applicationCommandType` nella tabella dei messaggi di traccia, modifica le impostazioni per renderla visibile.

Puoi anche vedere il `applicationCommandType` e altri messaggi dettagliati nel messaggio del registro JSON in WirelessMetadata > ApplicationInfo.

Debug delle attività FUOTA con gruppi multicast

È possibile utilizzare l'analizzatore di rete per eseguire il debug di un'attività FUOTA con gruppi multicast e dispositivi LoRaWAN aggiunti al gruppo. Per informazioni sull'aggiunta di dispositivi a un'attività FUOTA, consulta Aggiunta di dispositivi e gruppi multicast per un'attività FUOTA e pianificazione di una sessione FUOTA. Per eseguire il debug dell'attività FUOTA, procedi come segue:

1. Crea una configurazione dell'analizzatore di rete attivando le impostazioni delle informazioni sui frame e delle informazioni sui frame multicast per i dispositivi wireless e i gruppi multicast.
2. Aggiungi il gruppo multicast nell'attività FUOTA alla configurazione dell'analizzatore di rete utilizzando il relativo identificatore di gruppo multicast. Abilita le informazioni sui frame multicast per eseguire il debug dei messaggi di dati del firmware e dei messaggi di query di stato FUOTA inviati al gruppo mentre l'attività FUOTA è in corso.
3. Aggiungi i dispositivi del tuo gruppo multicast alla configurazione dell'analizzatore di rete utilizzando i relativi identificatori di dispositivi wireless. Attiva le informazioni sui frame per monitorare i messaggi di uplink e downlink scambiati direttamente con i dispositivi mentre l'attività FUOTA è in corso.
4. Attiva la messaggistica di traccia per iniziare a ricevere messaggi di traccia per i dispositivi e i gruppi multicast presenti nella configurazione dell'analizzatore di rete.

A questo punto, puoi visualizzare i messaggi di traccia ed eseguirne il debug utilizzando la colonna `applicationCommandType` della tabella dei messaggi di traccia e i dettagli nel messaggio del registro JSON, come descritto in Debug delle attività FUOTA che contengono solo dispositivi.

Debug dei dispositivi che stanno tentando di entrare in un gruppo multicast

Utilizza l'analizzatore di rete per eseguire il debug dei dispositivi che tentano di entrare in un gruppo multicast. Per informazioni sull'aggiunta di dispositivi a un gruppo multicast, consulta Crea gruppi multicast e aggiungi dispositivi al gruppo. Per eseguire il debug del gruppo multicast, procedi come segue:

1. Crea una configurazione dell'analizzatore di rete attivando le informazioni sui frame per i dispositivi wireless.

2. Aggiungi alla configurazione dell'analizzatore di rete i dispositivi che vuoi monitorare utilizzando i relativi identificatori di dispositivi wireless.
3. Attiva la messaggistica di traccia per iniziare a ricevere messaggi di traccia per i dispositivi presenti nella configurazione dell'analizzatore di rete.
4. Inizia ad associare i dispositivi al gruppo multicast dopo aver attivato i messaggi di traccia per i dispositivi del gruppo.

Debug di una sessione di gruppo multicast

Utilizza l'analizzatore di rete per eseguire il debug di una sessione di gruppo multicast. Per ulteriori informazioni, consultare Pianifica un messaggio di downlink da inviare ai dispositivi del gruppo multicast. Per eseguire il debug di una sessione di gruppo multicast, procedi come segue:

1. Crea una configurazione dell'analizzatore di rete attivando le informazioni sui frame multicast per il gruppo multicast.
2. Aggiungi alla configurazione dell'analizzatore di rete il gruppo multicast che desideri monitorare utilizzando il relativo identificatore di gruppi multicast.
3. Attiva la messaggistica di traccia prima dell'inizio della sessione multicast, così da iniziare a ricevere i messaggi di traccia per la sessione del gruppo multicast.
4. Avvia la sessione del gruppo multicast e monitorane lo stato visualizzando i messaggi nella tabella dei messaggi di traccia e nel messaggio del registro JSON.

Nella tabella dei messaggi di traccia, verrà visualizzato `MulticastAddr` nella colonna`DevAddr`. Puoi vedere `MulticastGroupId` e altre informazioni dettagliate nel messaggio del registro JSON in WirelessMetadata > ApplicationInfo.

AWS IoT Core per LoRaWAN ed endpoint VPC dell'interfaccia (AWS PrivateLink)

Puoi connetterti direttamente ad AWS IoT Core per LoRaWAN utilizzando endpoint VPC di interfaccia (AWS PrivateLink) nel tuo Virtual Private Cloud (VPC) invece di connetterti tramite Internet pubblico. Quando utilizzi un endpoint VPC di interfaccia, la comunicazione tra il VPC e AWS IoT Core per LoRaWAN avviene in modo completo e sicuro all'interno della rete AWS.

AWS IoT Core per LoRaWAN supporta endpoint di interfaccia Amazon Virtual Private Cloud che sono supportati da AWS PrivateLink. Ogni endpoint VPC è rappresentato da una o più interfacce di

rete elastiche con indirizzi IP privati nelle sottoreti del tuo VPC. Per ulteriori informazioni, consultare Endpoint VPC di interfaccia (AWS PrivateLink) nella Guida per l'utente di Amazon VPC.

Per ulteriori informazioni su VPC ed endpoint, consulta Cos'è Amazon VPC?.

Per ulteriori informazioni su AWS PrivateLink, consulta AWS PrivateLink ed endpoint VPC.

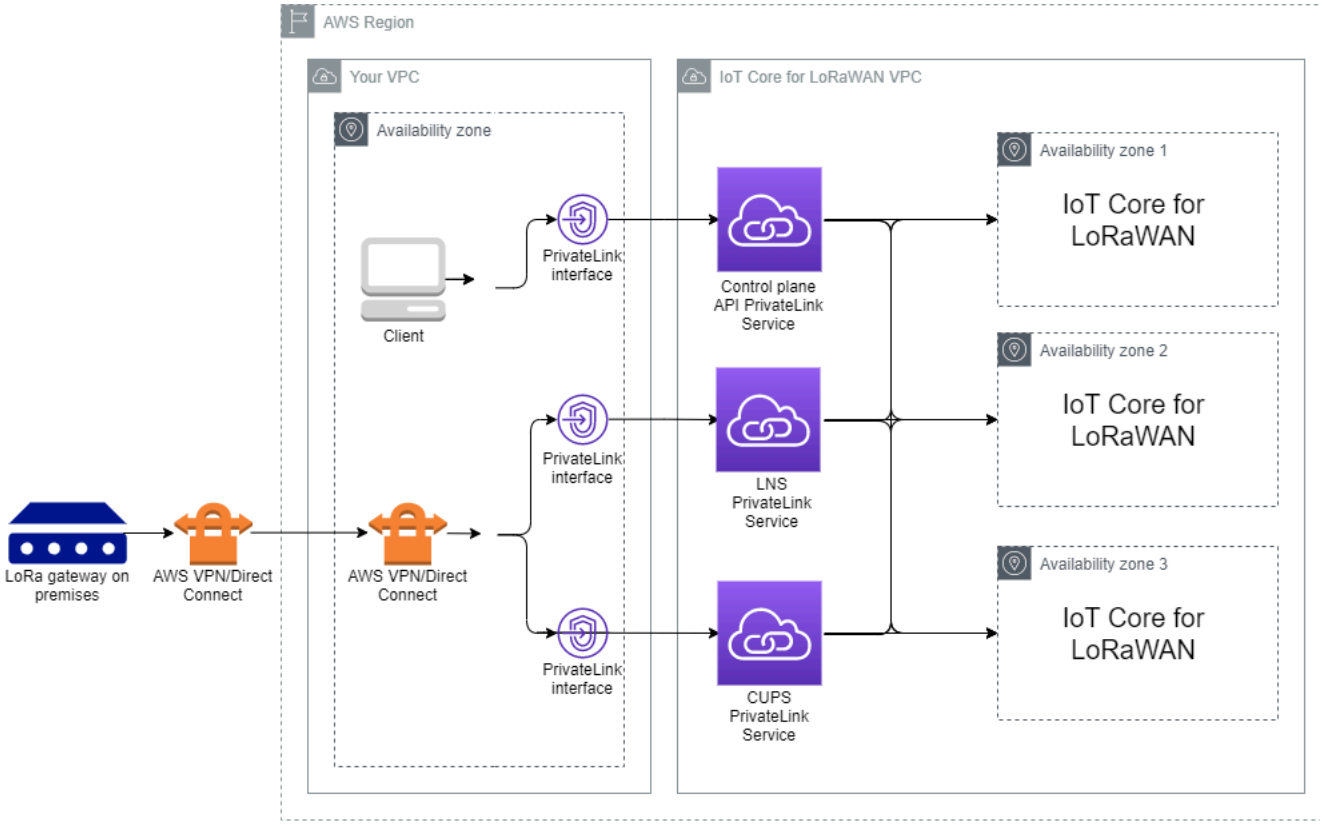
Considerazioni sugli endpoint VPC di AWS IoT

Prima di impostare un endpoint VPC dell'interfaccia per Wireless AWS IoT, assicurati di leggere Interface endpoint properties and limitations nella Guida per l'utente Amazon VPC.

Wireless AWS IoT supporta l'esecuzione di chiamate per tutte le sue operazioni API all'interno del VPC. Le policy endpoint VPC non sono supportate per Wireless AWS IoT. Per impostazione predefinita, l'accesso completo a Wireless AWS IoT è consentito attraverso l'endpoint. Per ulteriori informazioni, consulta Controllo degli accessi ai servizi con endpoint VPC nella Guida per l'utente di Amazon VPC.

architettura privatelink AWS IoT Core per LoRaWAN

Il seguente diagramma mostra l'architettura privatelink di AWS IoT Core per LoRaWAN. L'architettura utilizza un Transit Gateway e un Resolver Route 53 per condividere gli endpoint di interfaccia AWS PrivateLink tra il tuo VPC, il VPC AWS IoT Core per LoRaWAN e un ambiente On-premise. Quando imposti la connessione agli endpoint dell'interfaccia VPC, troverai un diagramma di architettura più dettagliato.



Endpoint AWS IoT Core per LoRaWAN

AWS IoT Core per LoRaWAN ha tre endpoint pubblici. Ogni endpoint pubblico ha un endpoint dell'interfaccia VPC corrispondente. Gli endpoint pubblici possono essere classificati in endpoint del piano di controllo e del piano dati. Per informazioni su questi endpoint, consulta AWS IoT Core per LoRaWAN endpoint API.

- Endpoint API del piano di controllo

  È possibile utilizzare gli endpoint API del piano di controllo per interagire con le API AWS IoT Wireless. È possibile accedere a questi endpoint da un client ospitato nell'Amazon VPC utilizzando AWS PrivateLink.

- Endpoint API del piano dati

  Gli endpoint API del piano dati sono gli endpoint LoRaWAN Network Server (LNS) e Configuration and Update Server (CUPS) che è possibile utilizzare per interagire con gli endpoint AWS IoT Core per LoRaWAN LNS e CUPS. È possibile accedere a questi endpoint dai gateway LoRa On-premise utilizzando AWS VPN o AWS Direct Connect. Questi endpoint si ottengono quando si esegue

l'onboarding del gateway per AWS IoT Core per LoRaWAN. Per ulteriori informazioni, consultare Aggiungi un gateway a AWS IoT Core per LoRaWAN.

Argomenti

Onboarding per l'endpoint API del piano di controllo AWS IoT Core per LoRaWAN

È possibile utilizzare gli endpoint API del piano di controllo AWS IoT Core per LoRaWAN per interagire con le API AWS IoT Wireless. Ad esempio, puoi utilizzare questo endpoint per eseguire l'API SendDataToWirelessDevice per inviare i dati da AWS IoT al dispositivo LoRaWAN. Per ulteriori informazioni, consulta AWS IoT Core per LoRaWAN Endpoint API del piano di controllo.

Puoi utilizzare il client ospitato nel tuo Amazon VPC per accedere agli endpoint del piano di controllo alimentati da AWS PrivateLink. Puoi utilizzare questi endpoint per connetterti all'API AWS IoT Wireless tramite un endpoint di interfaccia nel tuo Virtual Private Cloud (VPC) anziché connetterti tramite Internet pubblico.

Per l’onboarding dell’endpoint del piano di controllo:

- Crea il tuo Amazon VPC e la sottorete
- Avvia un'istanza Amazon EC2 nella sottorete
- Crea un endpoint dell'interfaccia Amazon VPC
- Verifica la connessione all’endpoint dell’interfaccia

Crea il tuo Amazon VPC e la sottorete

Prima di poterti connettere all'endpoint dell'interfaccia, devi creare un VPC e una sottorete. Verrà quindi avviata un'istanza EC2 nella sottorete, che puoi utilizzare per connetterti all'endpoint dell'interfaccia.

Per creare il tuo VPC:

1. Passa alla pagina VPC della console Amazon VPC e scegli Crea VPC.
2. Sulla pagina Create VPC (Crea VPC):

- Inserisci un nome per VPC Name tag (Tag Nome VPC) - facoltativo (ad esempio, **`VPC-A`**).
- Inserisci un intervallo di indirizzi IPv4 per il VPC nel blocco CIDR IPv4 (ad esempio, **`10.100.0.0/16`**).

3. Mantieni i valori predefiniti per gli altri campi e scegli Create VPC (Crea VPC).

Per creare la sottorete:

1. Passa alla pagina Subnets (Sottoreti) della console Amazon VPC e scegli Create subnet (Crea una sottorete).
2. Sulla pagina Create subnet (Crea sottorete):
   - Per VPC ID, scegli il VPC che hai creato in precedenza (ad esempio, `VPC-A`).
   - Inserisci un nome per Subnet name (Nome sottorete) (ad esempio, **`Private subnet`**).
   - Scegli la Availability zone (Zona di disponibilità) per la sottorete.
   - Inserisci il blocco di indirizzi IP della sottorete nella casella IPv4 CIDR block (Blocco CIDR IPv4) in formato CIDR (ad esempio, **`10.100.0.0/24`**).
3. Per creare la sottorete e aggiungerla al VPC, scegli Create subnet (Creare una sottorete).

Per ulteriori informazioni, consulta Work with VPCs and subnets (Uso di VPC e sottoreti).

Avvia un'istanza Amazon EC2 nella sottorete

Avvia la tua istanza EC2:

1. Passa alla console Amazon EC2 e scegli Launch Instance (Avvia istanza).
2. Per AMI, scegli Amazon Linux 2 AMI (HVM), SSD Volume Type e quindi scegli il tipo di istanza t2 micro. Per configurare i dettagli dell'istanza scegli Next (Successivo).
3. Nella pagina Configure Instance Details (Configura i dettagli dell'istanza):
   - Per Network (Rete), scegli il VPC che hai creato in precedenza (per esempio, `VPC-A`).
   - Per Subnet (Sottorete), scegli la sottorete che hai creato in precedenza (ad esempio, **`Private subnet`**).
   - Per Ruolo IAM, scegli il ruolo AWSIoTWirelessFullAccess per garantire a AWS IoT Core per LoRaWAN la policy di accesso completo. Per ulteriori informazioni, consulta la sezione Riepilogo delle policy `AWSIoTWirelessFullAccess`.
   - Per Assume Private IP (Assumere IP privato) utilizza un indirizzo IP, ad esempio, 10.100.0.42.

4. Scegli Next: Add Storage (Successivo: Aggiungi storage) e poi Next: Add tags (Successivo: Aggiungi tag). È possibile aggiungere qualsiasi tag da associare all'istanza EC2. Scegliere Next: Configure Security Group (Fase successiva: configurazione del gruppo di sicurezza).
5. Nella pagina Configure Security Group (Configura il gruppo di sicurezza), configura il gruppo di sicurezza per permettere:
   - Apri All TCP (Tutte le regole TCP) per fonti come `10.200.0.0/16`.
   - Apri All ICMP - IPV4 (Tutti i parametri ICMP - IPV4) per fonti come `10.200.0.0/16`.
6. Per esaminare i dettagli dell'istanza e avviare l'istanza EC2, scegli Review and Launch (Rivedi e avvia).

Per ulteriori informazioni, consulta Nozioni di base sulle istanze Amazon EC2 Linux.

Crea un endpoint dell'interfaccia Amazon VPC

È possibile creare un endpoint VPC per il tuo VPC, a cui è possibile accedere tramite l'API EC2. Per creare l'endpoint:

1. Passa alla console VPC Endpoint e scegli Create Endpoint (Creazione endpoint).
2. Nella pagina Create Endpoint (Crea endpoint), specifica le informazioni riportate di seguito.
   - Scegli Servizio AWSs per Categoria di servizio.
   - Per Service Name (Nome servizio), esegui la ricerca inserendo la parola chiave **`iotwireless`**. Nella lista di servizi `iotwireless`, scegli l'endpoint API del piano di controllo per la regione. L'endpoint sarà nel formato `com.amazonaws.`*`region`*`.iotwireless.api`.
   - Per VPC e Subnets (Sottoreti) scegli il VPC in cui desideri creare l'endpoint e le zone di disponibilità in cui desideri creare la rete endpoint.

     > **Note**
     >
     > Non tutte le zone di disponibilità possono essere supportate dal servizio `iotwireless`.

   - Per Enable DNS Name (Abilita nome DNS), scegli Enable for this endpoint (Abilita per questo endpoint).

     La scelta di questa opzione risolverà automaticamente il DNS e creerà un routing in Amazon Route 53 Public Data Plane, in modo che le API utilizzate in seguito per testare la connessione passino attraverso gli endpoint privatelink.

- In Security group (Gruppo di sicurezza), scegli i gruppi di sicurezza da associare alle interfacce di rete dell'endpoint.
- Facoltativamente, puoi aggiungere o rimuovere i tag. I tag sono coppie nome-valore utilizzate per l'associazione al tuo endpoint.

3. Per creare l'endpoint VPC, scegli Create endpoint (Crea endpoint).

Verifica la connessione all’endpoint dell’interfaccia

Puoi utilizzare un SSH per accedere all'istanza di Amazon EC2 e quindi utilizzare AWS CLI per connetterti agli endpoint dell'interfaccia privatelink.

Prima di connetterti all'endpoint dell'interfaccia, scarica la versione più recente di AWS CLI seguendo le istruzioni descritte in Installazione, aggiornamento e disinstallazione di AWS CLI versione 2 su Linux.

Di seguito sono riportati esempi che mostrano come testare la connessione all'endpoint di interfaccia utilizzando la CLI.

```
aws iotwireless create-service-profile \
    --endpoint-url https://api.iotwireless.region.amazonaws.com  \
    --name='test-privatelink'
```

L'esempio seguente mostra un esempio dell’esecuzione del comando.

```
Response:
{
 "Arn": "arn:aws:iotwireless:region:acct_number:ServiceProfile/1a2345ba-4c5d-67b0-ab67-e0c8342f2857",
 "Id": "1a2345ba-4c5d-67b0-ab67-e0c8342f2857"
}
```

Analogamente, puoi eseguire i seguenti comandi per ottenere le informazioni sul profilo del servizio o elencare tutti i profili di servizio.

```
aws iotwireless get-service-profile \
    --endpoint-url https://api.iotwireless.region.amazonaws.com
    --id="1a2345ba-4c5d-67b0-ab67-e0c8342f2857"
```

Di seguito viene illustrato un esempio per il comando list-device-profiles.

```
aws iotwireless list-device-profiles \
    --endpoint-url https://api.iotwireless.region.amazonaws.com
```

Onboarding degli endpoint API piano dati AWS IoT Core per LoRaWAN

Gli endpoint del piano dati AWS IoT Core per LoRaWAN sono costituiti dai seguenti endpoint. Questi endpoint si ottengono quando si aggiunge il gateway ad AWS IoT Core per LoRaWAN. Per ulteriori informazioni, consultare Aggiungi un gateway a AWS IoT Core per LoRaWAN.

- Endpoint LoRaWAN Network Server (LNS)

  Gli endpoint LNS sono del formato *account-specific-prefix*`.lns.lorawan.`*region*`.amazonaws.com`. È possibile utilizzare questo endpoint per stabilire una connessione per lo scambio di messaggi uplink e downlink LoRa.

- Endpoint CUPS (Configuration and Update Server)

  Gli endpoint CUPS sono del formato *account-specific-prefix*`.cups.lorawan.`*region*`.amazonaws.com`. È possibile utilizzare questo endpoint per la gestione delle credenziali, la configurazione remota e l'aggiornamento del firmware dei gateway.

Per ulteriori informazioni, consultare Utilizzo di protocolli CUPS e LNS.

Per trovare gli endpoint dell'API del piano dati per il tuo Account AWS e la tua Regione, utilizza il comando CLI get-service-endpoint mostrato qui, o il comando REST API `GetServiceEndpoint`. Per ulteriori informazioni, consulta AWS IoT Core per LoRaWAN Endpoint API Piano Dati.

È possibile collegare il tuo gateway LoRaWAN on-premise per comunicare con gli endpoint AWS IoT Core per LoRaWAN. Per stabilire questa connessione, connetti innanzitutto il gateway locale all'account Account AWS nel VPC utilizzando una connessione VPN. È quindi possibile comunicare con gli endpoint dell'interfaccia del piano dati nel VPC AWS IoT Core per LoRaWAN che sono alimentati da privatelink.

Di seguito viene spiegato come integrare questi endpoint.

- Crea endpoint di interfaccia VPC e zona ospitata privata
- Utilizza VPN per connettere i gateway LoRa al tuo Account AWS

Crea endpoint di interfaccia VPC e zona ospitata privata

AWS IoT Core per LoRaWAN dispone di due endpoint del piano dati, l'endpoint Configuration and Update Server (CUPS) e l'endpoint LoRaWAN Network Server (LNS). Il processo di configurazione per stabilire una connessione privatelink a entrambi gli endpoint è lo stesso, quindi possiamo utilizzare l'endpoint LNS a scopo illustrativo.

Per gli endpoint del piano dati, i gateway LoRa si connettono innanzitutto al tuo Account AWS nel tuo Amazon VPC, che poi si connette all'endpoint VPC nel VPC AWS IoT Core per LoRaWAN.

Quando ci si connette agli endpoint, i nomi DNS possono essere risolti all'interno di un VPC ma non possono essere risolti su più VPC. Per disabilitare il DNS privato durante la creazione dell'endpoint, disabilita l'impostazione Enable DNS name (Abilitare nome DNS). È possibile utilizzare una zona ospitata privata per fornire informazioni su come si desidera che Route 53 risponda alle query DNS per i VPC. Per condividere il VPC con un ambiente on-premise, è possibile utilizzare un Route 53 Resolver per facilitare il DNS ibrido.

Per completare questa procedura, esegui le fasi seguenti.

- Crea un Amazon VPC e una sottorete
- Crea un endpoint Amazon VPC dell'interfaccia
- Configura una zona ospitata privata
- Configura il resolver in ingresso Route 53
- Passaggi successivi

Crea un Amazon VPC e una sottorete

Puoi riutilizzare l'Amazon VPC e la sottorete che hai creato durante l'onboarding dell'endpoint del piano di controllo. Per informazioni, consulta Crea il tuo Amazon VPC e la sottorete.

Crea un endpoint Amazon VPC dell'interfaccia

È possibile creare un endpoint VPC per il VPC, allo stesso modo in cui se ne creerebbe uno per l'endpoint del piano di controllo.

1. Passa alla console VPC Endpoint e scegli Create Endpoint (Creazione endpoint).
2. Nella pagina Create Endpoint (Crea endpoint), specifica le informazioni riportate di seguito.
   - Scegli Servizio AWSs per Categoria di servizio.

- Per Service Name (Nome servizio), esegui la ricerca inserendo la parola chiave **`lns`**. Nella lista dei servizi `lns`, scegli l'endpoint API del piano dati LNS per la propria regione. L'endpoint sarà del formato `com.amazonaws.`*`region`*`.lorawan.lns`.

  > **Note**
  >
  > Se stai seguendo questa procedura per il tuo endpoint CUPS, cerca `cups`. L'endpoint sarà del formato `com.amazonaws.`*`region`*`.lorawan.cups`.

- Per VPC e Subnets (Sottoreti) scegli il VPC in cui desideri creare l'endpoint e le zone di disponibilità in cui desideri creare la rete endpoint.

  > **Note**
  >
  > Non tutte le zone di disponibilità possono essere supportate per il servizio `iotwireless`.

- Per Enable DNS name (Abilitare nome DNS), assicurati che Enable for this endpoint (Abilita per questo endpoint) non sia selezionata.

  Non selezionando questa opzione, è possibile disabilitare il DNS privato per l'endpoint VPC e utilizzare invece la zona ospitata privata.

- In Security group (Gruppo di sicurezza), scegli i gruppi di sicurezza da associare alle interfacce di rete dell'endpoint.
- Facoltativamente, puoi aggiungere o rimuovere i tag. I tag sono coppie nome-valore utilizzate per l'associazione al tuo endpoint.

3. Per creare l'endpoint VPC, scegli Create endpoint (Crea endpoint).

Configura una zona ospitata privata

Dopo aver creato l'endpoint privatelink, nella scheda Details (Dettagli) del tuo endpoint viene visualizzato un elenco di nomi DNS. È possibile utilizzare uno di questi nomi DNS per configurare la zona ospitata privata. Il nome DNS sarà nel formato `vpce-`*`xxxx`*`.lns.lorawan.`*`region`*`.vpce.amazonaws.com`.

Creare la zona ospitata privata

Per creare una zona ospitata privata:

1. Passa alla console Route 53 Hosted zone (Zone ospitate) e scegli Create hosted zone (Crea una zona ospitata).
2. Nella pagina Create hosted zone (Crea una zona ospitata), specifica le informazioni riportate di seguito.
   - Per Domain name (Nome dominio), inserisci il nome completo del servizio per l'endpoint LNS, **`lns.lorawan.region.amazonaws.com`**.

     > **Note**
     >
     > Se stai seguendo questa procedura per il tuo endpoint CUPS, inserisci **`cups.lorawan.region.amazonaws.com`**.

   - Nell'elenco Type (Tipo), scegli Private Hosted Zone (Zona ospitata privata).
   - Facoltativamente, puoi aggiungere o rimuovere tag da associare alla tua zona ospitata.
3. Per creare la tua zona privata ospitata, scegli Create hosted zone (Crea una zona ospitata).

Per ulteriori informazioni consulta Creating a private hosted zone (Creazione di una zona ospitata privata).

Dopo aver creato una zona ospitata privata, è possibile creare un registro che indica al DNS come si desidera che il traffico venga instradato a quel dominio.

Creazione di un record

Dopo aver creato una zona ospitata privata, è possibile creare un registro che indica al DNS come si desidera che il traffico venga instradato a quel dominio. Per creare un record:

1. Nell'elenco delle zone ospitate visualizzate, scegli la zona ospitata privata creata in precedenza e scegli Create record (Crea un record).
2. Utilizza il metodo della procedura guidata per creare il record. Se la console presenta il metodo Quick create (Creazione rapida), scegli Switch to wizard (Passa alla procedura guidata).
3. Scegli Simple Routing (Instradamento semplice) per Routing policy (Policy di instradamento) e poi Next (Successivo).
4. Nella pagina Configure records (Configura record), scegli Define simple record (Definisci record semplice).
5. Nella pagina Define simple record (Definisci record semplice):

- Per Record name (Nome record) inserisci l'alias del numero del tuo account Account AWS. È possibile ottenere questo valore quando si esegue l'onboarding del gateway o si utilizza il `GetServiceEndpoint` REST API.
- Per Record type (Tipo di record), mantieni il valore come `A - Routes traffic to an IPv4 address and some AWS resources`.
- In Value/Route traffic to (Valore/Instradamento del traffico a), seleziona Alias to VPC endpoint (Alias all'endpoint VPC). Scegli la tua Regione quindi scegli l'endpoint creato in precedenza, come descritto in Crea un endpoint Amazon VPC dell'interfaccia dall'elenco degli endpoint visualizzati.

6. Scegli Define simple record (Definizione del record semplice) per creare il record.

Configura il resolver in ingresso Route 53

Per condividere un endpoint VPC in un ambiente on-premise, è possibile utilizzare un Resolver Route 53 per facilitare il DNS ibrido. Il resolver in ingresso consente di instradare il traffico dalla rete on-premise agli endpoint del piano dati senza passare attraverso Internet pubblico. Per restituire i valori dell'indirizzo IP privato per il servizio, crea il Resolver Route 53 nello stesso VPC dell'endpoint VPC.

Quando si crea il resolver in entrata, è sufficiente specificare il VPC e le sottoreti create in precedenza nelle zone di disponibilità. Il Resolver Route 53 utilizza queste informazioni per assegnare automaticamente un indirizzo IP per instradare il traffico a ciascuna sottorete.

Per creare il resolver in entrata:

1. Passa alla console Route 53 Inbound endpoints (Endpoint in entrata) e scegli Create inbound endpoint (Crea endpoint in entrata).

   > **Note**
   >
   > Assicurati di utilizzare lo stesso Regione AWS utilizzato durante la creazione dell'endpoint e della zona ospitata privata.

2. Nella pagina Create inbound endpoint (Crea endpoint in entrata), specifica le informazioni riportate di seguito.
   - Inserisci un nome per Endpoint name (Nome endpoint) (ad esempio, **`VPC_A_Test`**).
   - Per VPC in the region (VPC nella regione), scegli lo stesso VPC utilizzato durante la creazione dell'endpoint VPC.

- Configura il Gruppo di sicurezza per questo endpoint per permettere il traffico in ingresso dalla rete locale.
- Per l'indirizzo IP, scegli Use an IP address that is selected automatically, (Utilizza un indirizzo IP selezionato automaticamente).

3. Scegli Submit (Invia) per creare il resolver in entrata.

Per questo, supponiamo che gli indirizzi IP `10.100.0.145` e `10.100.192.10` siano stati assegnati per il Resolver Route 53 in ingresso per il traffico di routing.

Passaggi successivi

Hai creato la zona ospitata privata e un risolutore in entrata per instradare il traffico per le voci DNS. Ora puoi utilizzare una Site-to-Site VPN o un endpoint Client VPN. Per ulteriori informazioni, consultare Utilizza VPN per connettere i gateway LoRa al tuo Account AWS.

Utilizza VPN per connettere i gateway LoRa al tuo Account AWS

Per connettere i gateway on-premise al tuo Account AWS puoi utilizzare una connessione Site-to-Site VPN o un endpoint Client VPN.

Prima di poter connettere i gateway on-premise, è necessario aver creato l'endpoint VPC e configurato una zona ospitata privata e un resolver in ingresso in modo che il traffico proveniente dai gateway non passi attraverso Internet pubblico. Per ulteriori informazioni, consultare Crea endpoint di interfaccia VPC e zona ospitata privata.

endpoint Site-to-Site VPN

Se non disponi dell'hardware del gateway o desideri testare la connessione VPN utilizzando un Account AWS, puoi usare una connessione Site-to-Site VPN. Puoi utilizzare Site-to-Site VPN per connetterti agli endpoint VPC dallo stesso Account AWS o da un altro Account AWS che potresti usare in un altro Regione AWS.

> **Note**
>
> Se disponi dell'hardware del gateway e desideri configurare una connessione VPN, ti consigliamo di utilizzare invece il Client VPN. Per istruzioni, consulta Endpoint Client VPN.

Per configurare un Site-to-Site VPN:

1. Crea un altro VPC nel sito da cui desideri impostare la connessione. Per `VPC-A` puoi riutilizzare il VPC creato in precedenza. Per creare un altro VPC (ad esempio, `VPC-B`), utilizza un blocco CIDR che non si sovrappone al blocco CIDR del VPC creato in precedenza.

   Per informazioni sulla configurazione dei VPC, segui le istruzioni descritte in AWS configurazione della connessione Site-to-Site VPN.

   > **Note**
   >
   > Il metodo Site-to-Site VPN descritto nel documento utilizza OpenSWAN per la connessione VPN, che supporta un solo tunnel VPN. Se utilizzi un altro software commerciale per la VPN, potresti essere in grado di impostare due tunnel tra i siti.

2. Dopo aver configurato la connessione VPN, aggiorna il file `/etc/resolv.conf` aggiungendo l'indirizzo IP del resolver in entrata dal tuo account Account AWS. Utilizza questo indirizzo IP per il nameserver. Per informazioni su come ottenere questo indirizzo IP, consulta Configura il resolver in ingresso Route 53. Per questo esempio, possiamo usare l'indirizzo IP `10.100.0.145` assegnato al momento della creazione del Resolver Route 53.

   ```
   options timeout:2 attempts:5
   ; generated by /usr/sbin/dhclient-script
   search region.compute.internal
   nameserver 10.100.0.145
   ```

3. Ora possiamo verificare se la connessione VPN utilizza l'endpoint AWS PrivateLink invece di passare attraverso Internet pubblico utilizzando un comando `nslookup`. Di seguito viene illustrato un esempio dell'esecuzione del comando.

   ```
   nslookup account-specific-prefix.lns.lorawan.region.amazonaws.com
   ```

   Di seguito viene illustrato un esempio di output dell'esecuzione del comando, che mostra un indirizzo IP privato che indica che la connessione è stata stabilita all'endpoint LNS AWS PrivateLink.

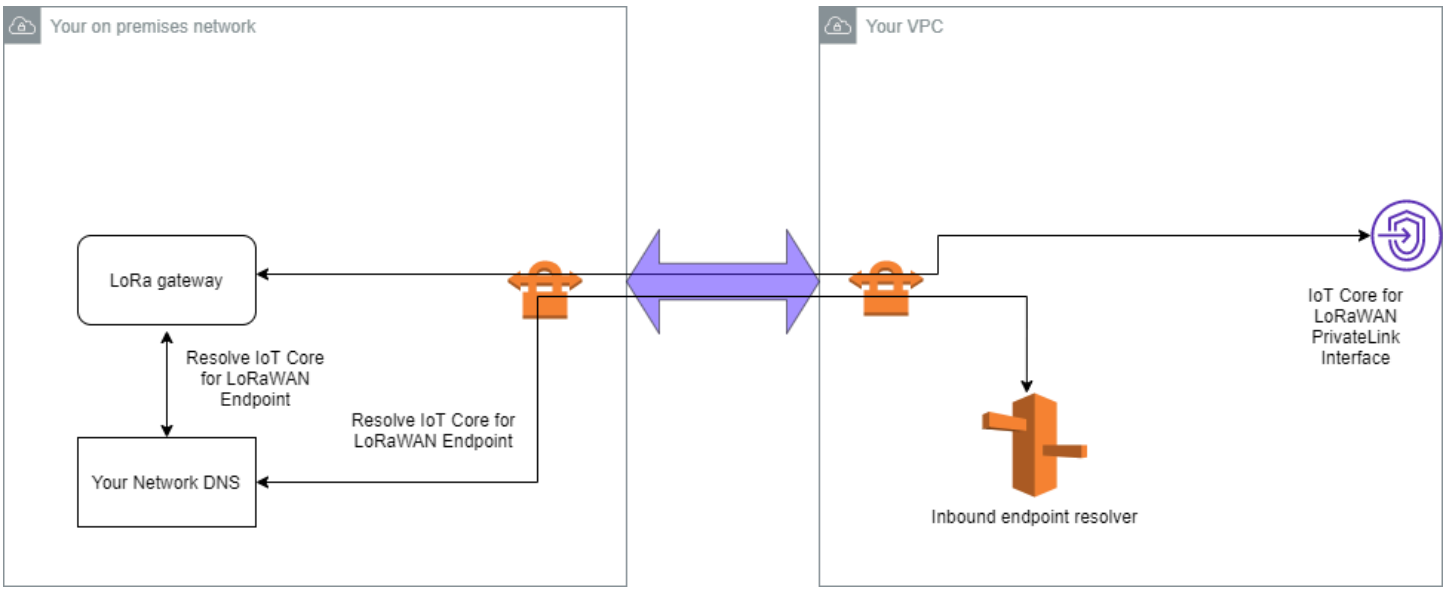
   ```
   Server: 10.100.0.145
   Address: 10.100.0.145

   Non-authoritative answer:
   Name: https://xxxxx.lns.lorawan.region.amazonaws.com
   ```

```
Address: 10.100.0.204
```

Per informazioni sull'utilizzo di una connessione Site-to-Site VPN, consulta Funzionamento di Site-to-Site VPN.

Endpoint Client VPN

AWS Client VPN è un servizio VPN gestito, basato su cloud, che consente di controllare in modo sicuro l'accesso alle risorse AWS nella tua rete locale. Di seguito viene illustrata l'architettura per il servizio Client VPN.



Per stabilire una connessione VPN a un endpoint Client VPN:

1. Crea un endpoint Client VPN seguendo le istruzioni descritte in Nozioni di base su AWS Client VPN.
2. Accedi alla rete on-premise (ad esempio, un router Wi-Fi) utilizzando l'URL di accesso per tale router (ad esempio, `192.168.1.1`), e individua nome e password di root.
3. Configura il gateway LoRaWAN seguendo le istruzioni contenute nella documentazione del gateway e quindi aggiungi il gateway ad AWS IoT Core per LoRaWAN. Per informazioni su come aggiungere un gateway, consulta Integrare i gateway per AWS IoT Core per LoRaWAN.
4. Controlla che il firmware del gateway sia aggiornato. Se il firmware non è aggiornato, è possibile seguire le istruzioni fornite nella rete On-premise per aggiornare il firmware del gateway. Per ulteriori informazioni, consultare Aggiornare il firmware del gateway utilizzando il servizio CUPS con AWS IoT Core per LoRaWAN.

5. Verifica se OpenVPN è stato abilitato. Se è stato abilitato, passa al passaggio successivo per configurare il client OpenVPN all'interno della rete on-premise. Se non è stato abilitato, segui le istruzioni in Guida all'installazione di OpenVPN per OpenWrt.

   > **Note**
   >
   > In questo esempio viene utilizzato OpenVPN. È possibile utilizzare altri client VPN come AWS VPN o AWS Direct Connect per configurare la connessione Client VPN.

6. Configura il client OpenVPN in base alle informazioni dalla configurazione del client e alle modalità di utilizzo Client OpenVPN che utilizza LuCi.
7. SSH alla rete on-premise e aggiorna il file `/etc/resolv.conf` aggiungendo l'indirizzo IP del resolver in entrata nel tuo account Account AWS (`10.100.0.145`).
8. Per il traffico del gateway utilizza AWS PrivateLink per connetterti all'endpoint, sostituisci la prima voce DNS del gateway all'indirizzo IP del resolver in ingresso.

Per informazioni sull'utilizzo di una connessione Site-to-Site VPN, consulta Nozioni di base su Client VPN.

Connessione agli endpoint LNS e CUPS VPC

Di seguito viene illustrato come testare la connessione agli endpoint LNS e CUPS VPC.

Test dell'endpoint CUPS

Per testare la connessione AWS PrivateLink all'endpoint CUPS dal gateway LoRa, esegui il comando seguente:

```
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": "xxxxxxxxxxxx",
              "cupsUri": "https://xxxx.cups.lorawan.region.amazonaws.com:443",
              "cupsCredCrc":1234, "tcCredCrc":552384314
             }'
      –output cups.out
```

Test dell'endpoint LNS

Per testare l'endpoint LNS, effettua prima il provisioning di un dispositivo LoRaWAN che funzionerà con il gateway wireless. Puoi quindi aggiungere il dispositivo ed eseguire la procedura join dopo la quale è possibile iniziare a inviare messaggi di uplink.

AWS IoT Core per Amazon Sidewalk

AWS IoT Core per Amazon Sidewalk fornisce i servizi cloud che è possibile utilizzare per connettere i dispositivi finali Sidewalk ad Cloud AWS e utilizzare altri Servizio AWS.

Amazon Sidewalk è una rete sicura e condivisa che consente ai dispositivi della community di connettersi e rimanere connessi. Amazon Sidewalk trasferisce i dati tra i dispositivi finali Sidewalk e i gateway Sidewalk e tra i gateway Sidewalk e il cloud Sidewalk.

Accesso ad AWS IoT Core per Amazon Sidewalk

È possibile eseguire l'onboarding dei dispositivi Sidewalk in AWS IoT utilizzando la console o le operazioni API AWS IoT Wireless. Dopo che è stato eseguito l'onboarding dei dispositivi, i relativi messaggi vengono inviati ad AWS IoT Core. Quindi, è possibile iniziare a sviluppare le applicazioni aziendali su AWS Cloud, che utilizza i dati dei dispositivi Amazon Sidewalk.

Utilizzo della console

Per eseguire l'onboarding dei dispositivi finali Sidewalk, accedi alla AWS Management Console e seleziona la pagina Dispositivi sulla console AWS IoT. Dopo aver eseguito l'onboarding dei dispositivi, puoi visualizzarli e gestirli in questa pagina della console IoT.

Utilizzo dell'API o dell'interfaccia a riga di comando

Puoi eseguire l'onboarding dei dispositivi Sidewalk e LoRaWAN utilizzando le operazioni API AWS IoT Wireless. L'API AWS IoT Wireless su cui si basa AWS IoT Core è supportata dall'SDK AWS. Per ulteriori informazioni, consulta AWS SDKs and Toolkits (SDK e kit di strumenti).

È possibile utilizzare la AWS CLI per eseguire comandi per l'onboarding e la gestione dei dispositivi finali Sidewalk. Per ulteriori informazioni, consulta la documentazione di riferimento dell'interfaccia della riga di comando AWS IoT Wireless.

Regioni ed endpoint per AWS IoT Core per Amazon Sidewalk

Amazon Sidewalk è disponibile solo nella Regione AWS `us-east-1`. AWS IoT Core per Amazon Sidewalk fornisce supporto per gli endpoint API del piano di controllo (control-plane) e del piano dati in questa Regione. Gli endpoint API del piano dati sono specifici per Account AWS. Per ulteriori informazioni, consultare Endpoint del servizio AWS IoT Wireless in Riferimenti generali di AWS.

AWS IoT Core per Amazon Sidewalk dispone di quote applicabili ai dati del dispositivo che vengono trasmessi tra il dispositivo e Cloud AWS e il TPS massimo per le operazioni API AWS IoT Wireless. Per ulteriori informazioni, consultare AWS IoT Wireless quotas in Riferimenti generali di AWS.

Prezzi di AWS IoT Core per Amazon Sidewalk

Quando effettui la registrazione ad AWS, puoi iniziare a utilizzare AWS IoT Core per Amazon Sidewalk gratuitamente mediante il Piano gratuito AWS.

Per ulteriori informazioni sulla panoramica generale del prodotto e sui prezzi, consulta prezzi di AWS IoT Core.

Cos'è AWS IoT Core per Amazon Sidewalk?

Con AWS IoT Core per Amazon Sidewalk, è possibile eseguire l'onboarding dei dispositivi finali Amazon Sidewalk in AWS IoT, nonché gestirli e monitorarli. Inoltre, consente di gestire le destinazioni che inviano i dati del dispositivo ad altri Servizi AWS.

Caratteristiche di AWS IoT Core per Amazon Sidewalk

Utilizzando AWS IoT Core per Amazon Sidewalk, puoi:

- Eseguire l'onboarding dei dispositivi finali Sidewalk in AWS IoT utilizzando la console AWS IoT, le operazioni API AWS IoT Core per Amazon Sidewalk o i comandi AWS CLI.
- Sfruttare le funzionalità offerte da Cloud AWS.
- Creare una destinazione che utilizza le regole AWS IoT per elaborare i messaggi di payload in entrata e interagire con altri Servizi AWS.
- Abilitare le notifiche degli eventi per ricevere messaggi sugli eventi, ad esempio quando è stato effettuato il provisioning o la registrazione del dispositivo finale Sidewalk, o se un messaggio in downlink è stato recapitato al dispositivo.
- Registrare e monitorare i dispositivi finali Sidewalk in tempo reale, ottenere informazioni utili, nonché identificare e risolvere gli errori.
- Associare i dispositivi finali Sidewalk a un oggetto AWS IoT, che consente di archiviare una rappresentazione del dispositivo sul cloud. Gli oggetti in AWS IoT semplificano la ricerca e la gestione delle funzionalità e l'accesso ad altre funzionalità AWS IoT Core.

I seguenti argomenti ti aiuteranno a conoscere Amazon Sidewalk e AWS IoT Core per Amazon Sidewalk.

Argomenti

Cos'è Amazon Sidewalk?

Amazon Sidewalk è una rete di community sicura che utilizza Amazon Sidewalk Bridges, come dispositivi Amazon Echo e Ring compatibili, per fornire connettività cloud per dispositivi IoT. Amazon Sidewalk consente una connettività a bassa larghezza di banda e a lungo raggio in casa e oltre utilizzando Bluetooth LE per comunicazioni a breve distanza e protocolli radio LoRa e FSK a frequenze di 900 MHz per coprire distanze più lunghe.

Quando Amazon Sidewalk è abilitata, questa rete può supportare altri dispositivi finali Sidewalk nella community e può essere utilizzata per applicazioni come il rilevamento dell'ambiente. Amazon Sidewalk consente ai dispositivi di connettersi e rimanere connessi.

Caratteristiche di Amazon Sidewalk

Di seguito sono riportate le caratteristiche di Amazon Sidewalk.

- Amazon Sidewalk crea una rete a bassa larghezza di banda utilizzando gateway Sidewalk che includono dispositivi Ring ed Echo. Utilizzando i gateway, è possibile condividere una parte della larghezza di banda di Internet, che viene quindi utilizzata per connettere i dispositivi finali alla rete.
- Amazon Sidewalk offre un meccanismo di rete sicuro con più livelli di crittografia e sicurezza.
- Amazon Sidewalk offre un meccanismo semplice per abilitare o disabilitare la partecipazione a Sidewalk.

Concetti di Amazon Sidewalk

Di seguito sono elencati alcuni concetti chiave di Amazon Sidewalk.

Gateway Sidewalk

I gateway Sidewalk, o bridge Amazon Sidewalk, instradano i dati tra i dispositivi finali Sidewalk e il cloud. I gateway sono dispositivi Amazon, come il dispositivo Echo o Ring Floodlight Cam,

che supportano SubG-CSS (asincrono, LDR), SubG-FSK (sincrono, HDR) o Bluetooth LE per la comunicazione Sidewalk. I gateway Sidewalk condividono una parte della larghezza di banda di Internet con la community Sidewalk per fornire connettività a un gruppo di dispositivi abilitati per Sidewalk.

Dispositivi finali Sidewalk

I dispositivi finali Sidewalk eseguono il roaming su Amazon Sidewalk collegandosi ai gateway Sidewalk. I dispositivi finali sono prodotti intelligenti a bassa larghezza di banda e basso consumo, come luci o serrature abilitati per Sidewalk.

> **Note**
>
> Alcuni gateway Sidewalk possono anche fungere da dispositivi finali.

Sidewalk Network Server

Il Sidewalk Network Server, gestito da Amazon, verifica i pacchetti in entrata e instrada i messaggi in uplink e in downlink alla destinazione desiderata, mantenendo la rete Sidewalk sincronizzata nel tempo.

Ulteriori informazioni su Amazon Sidewalk

Per ulteriori informazioni su Amazon Sidewalk, consulta le pagine Web seguenti:

- Amazon Sidewalk
- Documentazione Amazon Sidewalk
- AWS IoT Core per Amazon Sidewalk

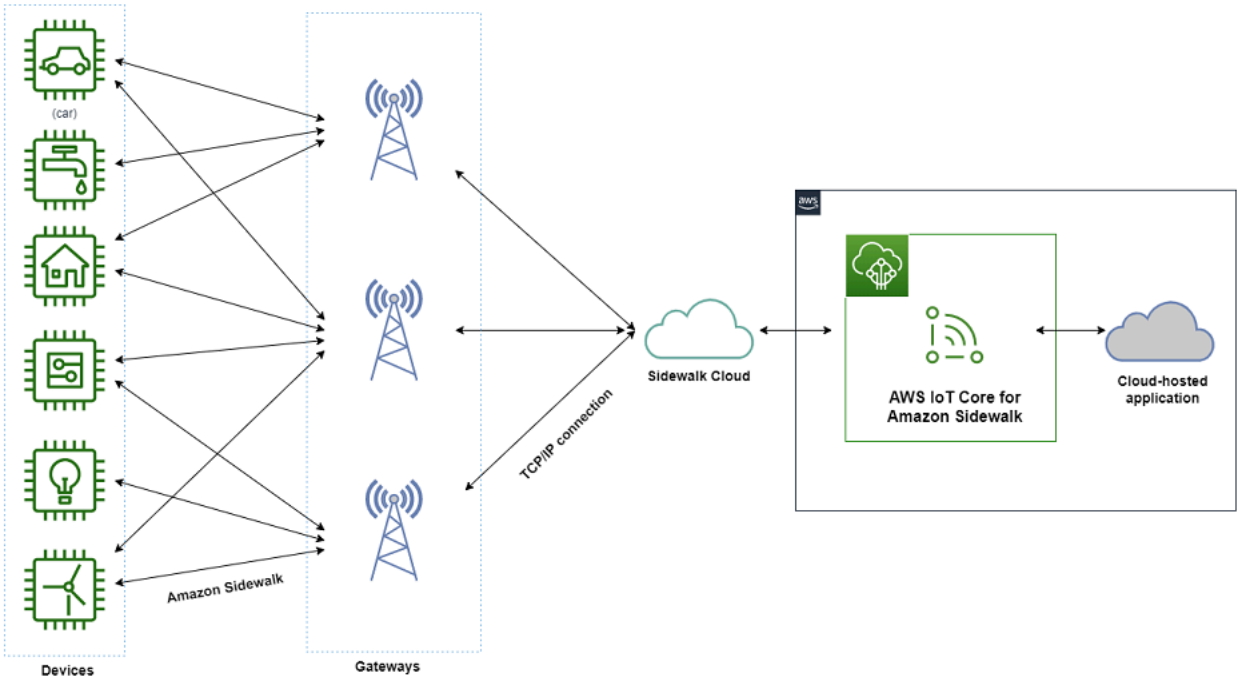
Come funziona AWS IoT Core per Amazon Sidewalk

Con AWS IoT Core per Amazon Sidewalk, è possibile eseguire l'onboarding dei dispositivi finali Amazon Sidewalk in AWS IoT, nonché gestirli e monitorarli. Inoltre, consente di gestire le destinazioni che inviano i dati del dispositivo ad altri Servizio AWS.

AWS IoT Core per Amazon Sidewalk fornisce i servizi cloud che è possibile utilizzare per connettere i dispositivi finali Sidewalk ad Cloud AWS e utilizzare altri Servizio AWS. È anche possibile utilizzare

AWS IoT Core per Amazon Sidewalk per gestire i dispositivi Sidewalk e monitorare e creare applicazioni su di essi.

I dispositivi finali Sidewalk comunicano con AWS IoT Core tramite i gateway Sidewalk. AWS IoT Core per Amazon Sidewalk gestisce le policy dei servizi e dei dispositivi richiesti da AWS IoT Core per gestire e comunicare con i dispositivi finali e i gateway Sidewalk. Inoltre, consente di gestire le destinazioni che inviano i dati del dispositivo ad altri Servizio AWS.



Nozioni di base sull'utilizzo di AWS IoT Core per Amazon Sidewalk

È possibile utilizzare la console AWS IoT, l'API AWS IoT Core per Amazon Sidewalk o AWS CLI per creare ed eseguire l'onboarding dei dispositivi finali Sidewalk e collegarli alla rete Sidewalk. Per informazioni sulle nozioni di base sull'utilizzo di Amazon Sidewalk e sull'onboarding di dispositivi finali in AWS IoT, consulta gli argomenti seguenti.

- Nozioni di base sull'utilizzo di AWS IoT Core per Amazon Sidewalk

  In questo argomento vengono descritti i prerequisiti per l'onboarding dei dispositivi finali Sidewalk, viene illustrato il flusso di lavoro utilizzando un'applicazione di monitoraggio dei sensori e viene fornita una panoramica su come eseguire l'onboarding del dispositivo mediante i comandi AWS CLI.
- Connessione a AWS IoT Core per Amazon Sidewalk

In questa sezione vengono descritti i diversi passaggi nell'introduzione al flusso di lavoro di onboarding e illustrato l'onboarding dei dispositivi finali mediante la console e le operazioni API. Verrà anche collegato il dispositivo e visualizzati i messaggi scambiati tra il dispositivo e AWS IoT Core per Amazon Sidewalk.

- Dispositivi di provisioning in blocco con AWS IoT Core per Amazon Sidewalk

  In questa sezione viene fornito un tutorial dettagliato per il provisioning in blocco dei dispositivi finali Sidewalk utilizzando AWS IoT Core per Amazon Sidewalk. Verranno fornite informazioni sul flusso di lavoro di provisioning in blocco e su come eseguire l'onboarding di un numero elevato di dispositivi Sidewalk.

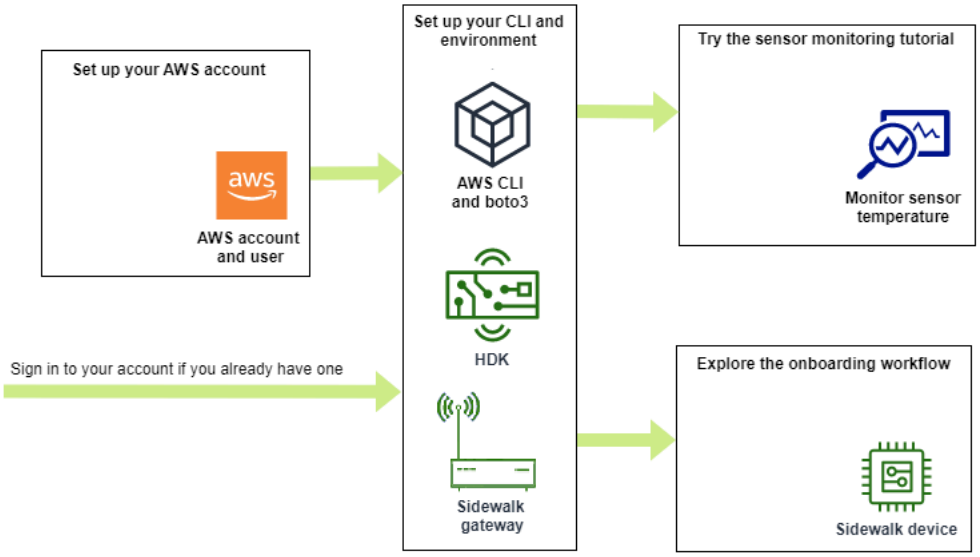
Ulteriori informazioni su AWS IoT Core per Amazon Sidewalk

Per ulteriori informazioni su AWS IoT Core per Amazon Sidewalk, consulta le pagine Web seguenti:

- Amazon Sidewalk
- Documentazione Amazon Sidewalk
- AWS IoT Core per Amazon Sidewalk

Nozioni di base sull'utilizzo di AWS IoT Core per Amazon Sidewalk

In questa sezione viene illustrato come iniziare a connettere i dispositivi finali Sidewalk ad AWS IoT Core per Amazon Sidewalk. Viene descritto come connettere un dispositivo finale ad Amazon Sidewalk e scambiare messaggi tra di essi. Verranno fornite informazioni sull'applicazione di esempio Sidewalk e una panoramica su come eseguire il monitoraggio dei sensori utilizzando AWS IoT Core per Amazon Sidewalk. L'applicazione di esempio fornisce un pannello di controllo per visualizzare e monitorare le modifiche alla temperatura del sensore.



I seguenti argomenti ti forniscono le nozioni di base per iniziare a utilizzare AWS IoT Core per Amazon Sidewalk.

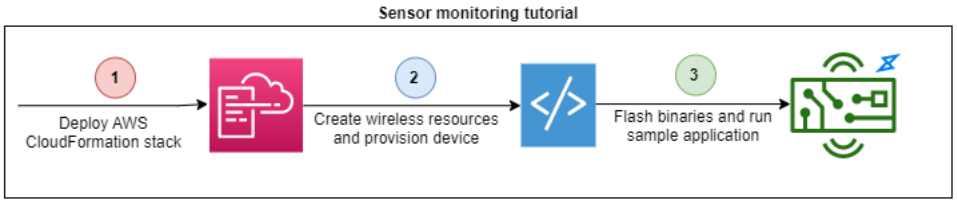
Argomenti

- Prova del tutorial sul monitoraggio dei sensori
- Introduzione all'onboarding dei dispositivi Sidewalk

Prova del tutorial sul monitoraggio dei sensori

In questa sezione viene fornita una panoramica dell'applicazione di esempio Amazon Sidewalk su GitHub che mostra come monitorare la temperatura di un sensore. In questo tutorial vengono utilizzati script che creano in modo programmatico le risorse wireless richieste, effettuano il provisioning del dispositivo finale e memorizzano nella flash i file binari, quindi collegano il dispositivo finale all'applicazione. Gli script che utilizzano AWS CLI e i comandi Python creano uno stack AWS CloudFormation e risorse wireless, quindi memorizzano nella flash i file binari e distribuiscono l'applicazione sul kit di sviluppo dell'hardware (HDK).

Nel diagramma seguente vengono illustrati i passaggi coinvolti quando si esegue l'applicazione di esempio e si collega il dispositivo finale Sidewalk all'applicazione. Per istruzioni dettagliate, inclusi i prerequisiti e la configurazione per questo tutorial, consultare il documento README in GitHub.



Introduzione all'onboarding dei dispositivi Sidewalk

In questa sezione viene illustrato come eseguire l'onboarding dei dispositivi finali Sidewalk in AWS IoT Core per Amazon Sidewalk. Per eseguire l'onboarding dei dispositivi, aggiungi innanzitutto il dispositivo Sidewalk, effettua il provisioning del dispositivo e la registrazione, quindi connetti l'hardware all'applicazione cloud. Prima di eseguire questo tutorial, rivedi e completa Installazione di Python e della AWS CLI.

Nella procedura seguente viene illustrato come eseguire l'onboarding e collegare i dispositivi finali Sidewalk in AWS IoT Core per Amazon Sidewalk. Se desideri eseguire l'onboarding dei dispositivi utilizzando AWS CLI, puoi fare riferimento ai comandi di esempio forniti in questa sezione. Per informazioni sull'onboarding dei dispositivi mediante la console AWS IoT, consultare Connessione a AWS IoT Core per Amazon Sidewalk.

> **Important**
>
> Per eseguire l'intero flusso di lavoro di onboarding, viene anche effettuato il provisioning e la registrazione del dispositivo finale e il collegamento del kit di sviluppo dell'hardware (HDK). Per ulteriori informazioni, consultare la pagina relativa al provisioning e alla registrazione del dispositivo finale nella documentazione di Amazon Sidewalk.

Argomenti

Fase 1: Aggiunta del dispositivo Sidewalk ad AWS IoT Core per Amazon Sidewalk

Di seguito viene fornita una panoramica della procedura eseguita per aggiungere il dispositivo finale Sidewalk ad AWS IoT Core per Amazon Sidewalk. Archivia le informazioni ottenute sul profilo del

dispositivo e sul dispositivo wireless che viene creato. Utilizzerai queste informazioni per effettuare il provisioning e la registrazione del dispositivo finale. Per ulteriori informazioni su questa procedura, consultare Aggiunta del dispositivo ad AWS IoT Core per Amazon Sidewalk.

1. Creazione di un profilo del dispositivo

   Crea un profilo del dispositivo contenente le configurazioni condivise per i dispositivi Sidewalk. Durante la creazione del profilo, specifica un *name* per il profilo come una stringa alfanumerica. Per creare un profilo, vai alla scheda Sidewalk dell'hub Profili nella console AWS IoT e scegli Crea profilo oppure utilizza l'operazione API `CreateDeviceProfile` o il comando dell'interfaccia a riga di comando `create-device-profile` come mostrato in questo esempio.

   ```
   // Add your device profile using a name and the sidewalk object.
   aws iotwireless create-device-profile --name sidewalk_profile --sidewalk {}
   ```

2. Creazione del dispositivo finale Sidewalk

   Crea il tuo dispositivo finale Sidewalk con AWS IoT Core per Amazon Sidewalk. Specifica un nome destinazione e l'ID del profilo del dispositivo ottenuto nella fase precedente. Per aggiungere un dispositivo, vai alla scheda Sidewalk dell'hub Dispositivi nella console AWS IoT e scegli Provisioning del dispositivo oppure utilizza l'operazione API `CreateWirelessDevice` o il comando dell'interfaccia a riga di comando `create-wireless-device` come mostrato in questo esempio.

   > **Note**
   >
   > Specifica un nome per la destinazione che sia univoco per Account AWS e Regione AWS. Lo stesso nome destinazione verrà utilizzato quando si aggiunge la destinazione ad AWS IoT Core per 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. Ottenere informazioni sul profilo del dispositivo e sul dispositivo wireless

   Ottieni le informazioni sul profilo del dispositivo e sul dispositivo wireless come un file JSON. Il file JSON contiene informazioni sui dettagli del dispositivo, i certificati dei dispositivi, le chiavi private, `DeviceTypeId` e il numero di serie di produzione Sidewalk (SMSN).

   - Se stai usando la console AWS IoT, puoi utilizzare la scheda Sidewalk dell'hub Dispositivi per scaricare un file JSON combinato per il dispositivo finale Sidewalk.
   - Se stai usando le operazioni API, archivia le risposte ottenute dalle operazioni API `GetDeviceProfile` e `GetWirelessDevice` come file JSON separati, ad esempio *`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
   ```

Fase 2: Creazione di una destinazione per il dispositivo finale Sidewalk

Di seguito viene fornita una panoramica della procedura che verrà eseguita per aggiungere la destinazione ad AWS IoT Core per Amazon Sidewalk. Utilizzando la AWS Management Console, le operazioni API AWS IoT Wireless o AWS CLI, esegui i seguenti passaggi per creare una regola AWS IoT e una destinazione. Puoi quindi eseguire la connessone alla piattaforma hardware e visualizzare e scambiare messaggi. Per un esempio di ruolo IAM e regola AWS IoT utilizzati per gli esempi AWS CLI di questa sezione, consultare Creazione di un ruolo IAM e della regola IoT per la destinazione.

1. Creazione di un ruolo IAM

   Crea un ruolo IAM che concede l'autorizzazione AWS IoT Core per Amazon Sidewalk per inviare dati alla regola AWS IoT. Per creare il ruolo, utilizza l'operazione API `CreateRole` o il comando dell'interfaccia a riga di comando `create-role`. Puoi assegnate al ruolo il nome *`SidewalkRole`*.

   ```
   aws iam create-role --role-name lambda-ex \
       --assume-role-policy-document file://lambda-trust-policy.json
   ```

2. Creazione di una regola per la destinazione

   Crea una regola AWS IoT che elabora i dati del dispositivo e specifica l'argomento in cui vengono pubblicati i messaggi. I messaggi su questo argomento verranno visualizzati dopo la connessione alla piattaforma hardware. Utilizza l'operazione API AWS IoT Core, `CreateTopicRule` o il comando AWS CLI, `create-topic-rule`, per creare una regola per la destinazione.

   ```
   aws iot create-topic-rule --rule-name Sidewalkrule \
       --topic-rule-payload file://myrule.json
   ```

3. Creazione di una destinazione

   Crea una destinazione che associa il dispositivo Sidewalk alla regola IoT utilizzata per elaborarlo per l'uso con altri Servizi AWS. Puoi aggiungere una destinazione utilizzando l'hub Destinazioni della console AWS IoT, l'operazione API `CreateDestination` o il comando dell'interfaccia a riga di comando `create-destination`.

   ```
   aws iotwireless create-destination --name SidewalkDestination \
       --expression-type RuleName --expression SidewalkRule \
       --role-arn arn:aws:iam::123456789012:role/SidewalkRole
   ```

Fase 3: Effettuare il provisioning e registrare il dispositivo finale

Utilizzando i comandi Python, è possibile effettuare il provisioning e la registrazione del dispositivo finale. Lo script di provisioning utilizza i dati JSON del dispositivo ottenuti per generare un'immagine binaria di produzione, che viene memorizzata nella flash sulla scheda hardware. Il dispositivo finale viene quindi registrato per la connessione alla piattaforma hardware. Per ulteriori informazioni, consultare la pagina relativa al provisioning e alla registrazione del dispositivo finale nella documentazione di Amazon Sidewalk.

> **Note**
>
> Durante la registrazione del dispositivo finale Sidewalk, il gateway deve fornire il consenso esplicito ad Amazon Sidewalk e il gateway e il dispositivo devono trovarsi entro una determinata distanza tra loro.

Fase 4: Connessione a un dispositivo finale Sidewalk e scambio di messaggi

Dopo aver registrato il dispositivo finale, è possibile connetterlo e iniziare a scambiare messaggi e dati del dispositivo.

1. Connessione del dispositivo finale Sidewalk

   Collega l'HDK al computer e segui le istruzioni fornite dalla documentazione del fornitore per connetterti all'HDK. Per ulteriori informazioni, consultare la pagina relativa al provisioning e alla registrazione del dispositivo finale nella documentazione di Amazon Sidewalk.

2. Visualizzazione e scambio di messaggi

   Utilizza il client MQTT per effettuare la sottoscrizione all'argomento specificato nella regola e visualizzare il messaggio ricevuto. Puoi anche utilizzare l'operazione API `SendDataToWirelessDevice` o il comando della riga di comando `send-data-to-wireless-device` per inviare un messaggio in downlink al dispositivo e verificare lo stato della connettività.

   (Facoltativo) Puoi abilitare gli eventi sullo stato di consegna dei messaggi per verificare se il messaggio in downlink è stato ricevuto correttamente.

```
aws iotwireless send-data-to-wireless-device \
    --id "<Wireless_Device_ID>" \
    --payload-data "SGVsbG8gVG8gRGV2c2lt" \
    --wireless-metadata Sidewalk={Seq=1,AckModeRetryDurationSecs=10}
```

Connessione a AWS IoT Core per Amazon Sidewalk

In questa sezione viene illustrato come eseguire l'onboarding del dispositivo finale Sidewalk e quindi connetterlo alla rete Sidewalk. Vengono descritti i passaggi eseguiti nel tutorial di onboarding, come indicato in Introduzione all'onboarding dei dispositivi Sidewalk. Verranno fornite informazioni su come eseguire l'onboarding dei dispositivi mediante la console AWS IoT per Amazon Sidewalk e le operazioni API AWS IoT Core. Inoltre, verranno fornite informazioni sui comandi AWS CLI che eseguono queste operazioni.

Prerequisiti

Per aggiungere il dispositivo finale e la destinazione ad AWS IoT Core per Amazon Sidewalk, devi configurare Account AWS. Per eseguire queste operazioni mediante l'API AWS IoT Wireless o i comandi AWS CLI, devi anche configurare AWS CLI. Per ulteriori informazioni sui prerequisiti e la configurazione, consultare Installazione di Python e della AWS CLI.

> **Note**
>
> Per eseguire l'intero flusso di lavoro di onboarding per il provisioning e la registrazione del dispositivo finale e la connessione al kit di sviluppo dell'hardware (HDK), devi anche configurare il gateway Sidewalk e HDK. Per ulteriori informazioni, consultare le pagine relative alla configurazione del kit di sviluppo dell'hardware (HDK) e alla configurazione di un gateway Sidewalk nella documentazione di Amazon Sidewalk.

Descrizione delle risorse Sidewalk

Prima di iniziare a creare le risorse, è consigliabile considerare la convenzione di denominazione dei dispositivi finali Sidewalk, dei profili dei dispositivi e delle destinazioni. AWS IoT Core per Amazon Sidewalk assegna un identificatore univoco alle risorse create. Tuttavia, puoi assegnare nomi più descrittivi, aggiungere una descrizione o aggiungere tag opzionali per facilitare l'identificazione e la gestione.

> **Note**
>
> Il nome della destinazione non può essere modificato dopo che è stato creato. Utilizza un nome univoco per Account AWS e Regione AWS.

Per ulteriori informazioni, consultare Descrizione delle risorse AWS IoT Wireless.

Argomenti

- Aggiunta del dispositivo ad AWS IoT Core per Amazon Sidewalk
- Aggiunta di una destinazione per il dispositivo finale Sidewalk
- Connetti il tuo dispositivo Sidewalk e visualizza il formato dei metadati uplink

Aggiunta del dispositivo ad AWS IoT Core per Amazon Sidewalk

Prima di creare un dispositivo wireless, crea innanzitutto un profilo del dispositivo. I profili dei dispositivi definiscono le funzionalità del dispositivo e altri parametri per i dispositivi Sidewalk. Un singolo profilo del dispositivo può essere associato a più dispositivi.

Dopo che hai creato un profilo del dispositivo, quando recuperi informazioni sul profilo, viene restituito un `DeviceTypeId`. Quando effettui il provisioning del dispositivo finale, utilizzerai questo ID, i certificati dei dispositivi, la chiave pubblica del server di applicazioni e l'SMSN.

Come creare e aggiungere il dispositivo

1. Crea un profilo del dispositivo per i dispositivi finali Sidewalk. Specifica un nome del profilo da utilizzare per i dispositivi Sidewalk come una stringa alfanumerica. Il profilo consentirà di identificare i dispositivi a cui associarlo.
   - (Console) Durante l'aggiunta del dispositivo Sidewalk, puoi anche creare un nuovo profilo. Questo consente di aggiungere rapidamente il dispositivo ad AWS IoT Core per Amazon Sidewalk e associarlo a un profilo.
   - (API) Utilizza l'operazione API `CreateDeviceProfile` specificando un nome del profilo e l'oggetto Sidewalk, `sidewalk {}`. La risposta API conterrà un ID profilo e un ARN (Amazon Resource Name).
2. Aggiunta del dispositivo wireless ad AWS IoT Core per Amazon Sidewalk. Specifica un nome di destinazione e scegli il profilo del dispositivo creato nella fase precedente.
   - (Console) Durante l'aggiunta del dispositivo Sidewalk, inserisci un nome di destinazione e scegli il profilo creato.
   - (API) Utilizza l'operazione API `CreateWirelessDevice`. Specifica un nome di destinazione e l'ID del profilo del dispositivo ottenuto in precedenza.

   Parametri dei dispositivi wireless

Parametro	Descrizione	Note
Nome della destinazione	Il nome della destinazione che descrive le regole AWS IoT per l'elaborazione dei dati del dispositivo che verranno utilizzati da altri Servizio AWS.	Se non hai ancora creato una destinazione, puoi fornire qualsiasi valore di stringa. AWS IoT Core per Amazon Sidewalk creerà una destinazione vuota durante la creazione del dispositivo, che

Parametro	Descrizione	Note
		potrai quindi aggiornare durante l'aggiunta della destinazione.
Profilo del dispositivo	Il profilo del dispositivo creato in precedenza.	–

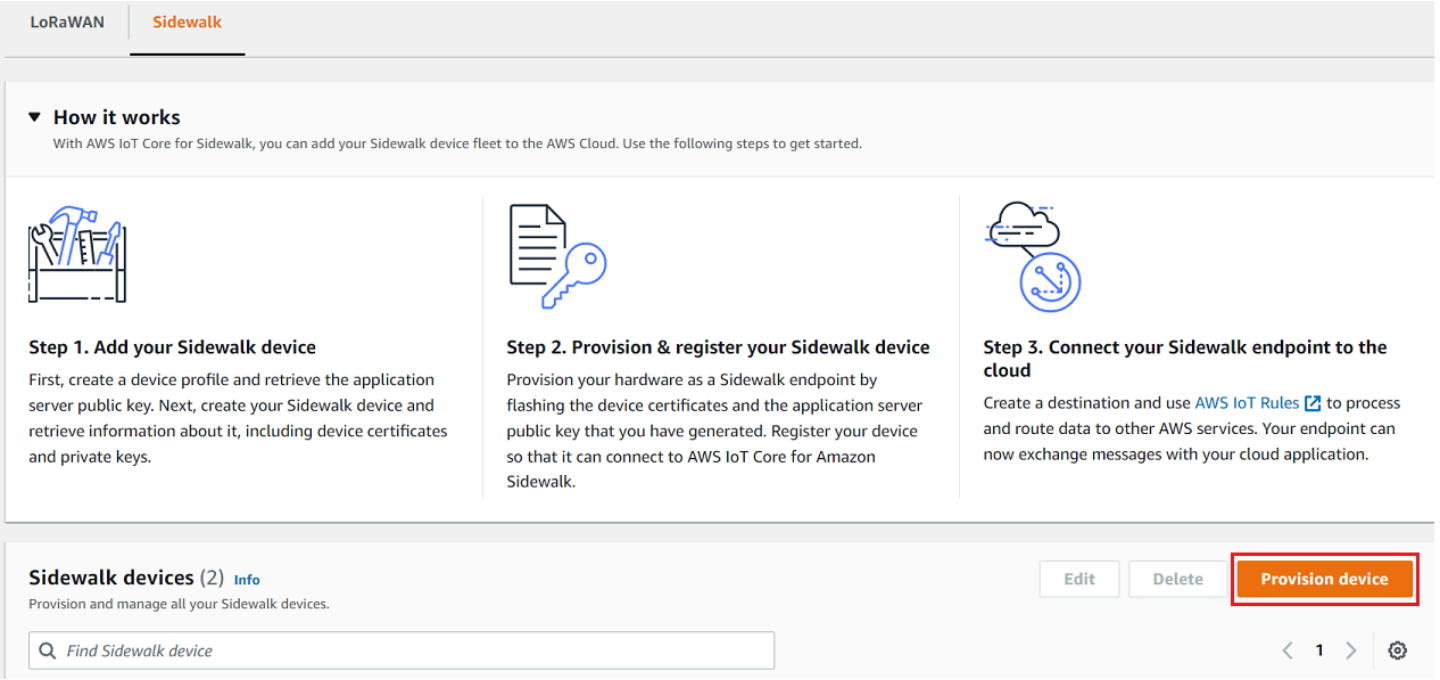
3. Ottieni il file JSON contenente le informazioni richieste per il provisioning del dispositivo finale.
   - (Console) Scarica questo file dalla pagina dei dettagli del dispositivo Sidewalk creato.
   - (API) Utilizza le operazioni API `GetDeviceProfile` e `GetWirelessDevice` per recuperare informazioni sul profilo del dispositivo e sul dispositivo wireless. Archivia le informazioni della risposta API come file JSON, ad esempio *`device_profile.json`* e *`wireless_device.json`*.

Aggiunta del profilo del dispositivo e del dispositivo finale Sidewalk

In questa sezione viene illustrato come creare un profilo del dispositivo. Inoltre, viene illustrato come utilizzare la console AWS IoT e la AWS CLI per aggiungere il dispositivo finale Sidewalk ad AWS IoT Core per Amazon Sidewalk.

Aggiunta del dispositivo Sidewalk (console)

Per aggiungere il dispositivo Sidewalk mediante la console AWS IoT, passa alla scheda Sidewalk dell'hub Dispositivi, scegli Provisioning del dispositivo, quindi esegui la procedura seguente.



1. Specifica dei dettagli dispositivo

   Specifica le informazioni di configurazione per il dispositivo Sidewalk. Puoi anche creare un nuovo profilo del dispositivo o scegliere un profilo esistente per il dispositivo Sidewalk.

   a. Specifica un nome del dispositivo e una descrizione facoltativa. La descrizione può contenere un massimo di 2048 caratteri. Questi campi possono essere modificati dopo che il dispositivo è stato creato.

   b. Scegli un profilo del dispositivo da associare al dispositivo Sidewalk. Se disponi già di profili dei dispositivi esistenti, puoi scegliere il tuo profilo. Per creare un nuovo profilo, scegli Crea nuovo profilo, quindi inserisci un nome per il profilo.

      > **Note**
      >
      > Per collegare tag al profilo del dispositivo, dopo che crei il profilo, passa all'hub Profili, quindi modifica il profilo per aggiungere queste informazioni.

   c. Specifica il nome della destinazione che instraderà i messaggi dal dispositivo ad altri Servizi AWS. Se non hai già creato una destinazione, passa all'hub Destinazioni per crearla. Puoi quindi scegliere tale destinazione per il dispositivo Sidewalk. Per ulteriori informazioni, consultare Aggiunta di una destinazione per il dispositivo finale Sidewalk.

   d. Scegli Avanti per continuare ad aggiungere il dispositivo Sidewalk.

2. Associazione del dispositivo Sidewalk all'oggetto AWS IoT (opzionale)

   Facoltativamente, puoi associare il dispositivo Sidewalk a un oggetto AWS IoT. Gli oggetti IoT sono voci nel registro dei dispositivi AWS IoT. Gli oggetti semplificano la ricerca e la gestione dei dispositivi. L'associazione di un oggetto al dispositivo consente al dispositivo di accedere ad altre funzionalità di AWS IoT Core.

   Per associare il dispositivo ad un oggetto, scegli Registrazione automatica degli oggetti.

   a. Inserisci un nome univoco per l'oggetto IoT che desideri associare al dispositivo Sidewalk. I nomi degli oggetti fanno distinzione tra maiuscole e minuscole e devono essere univoci in Account AWS e nella Regione AWS.
   b. Fornisci eventuali configurazioni aggiuntive per l'oggetto IoT, ad esempio utilizzando un tipo di oggetto o attributi ricercabili, che possono essere utilizzati per filtrare da un elenco di oggetti.
   c. Scegli Avanti e verifica le informazioni sul dispositivo Sidewalk, quindi seleziona Crea.

Aggiunta del dispositivo Sidewalk (interfaccia a riga di comando)

Per aggiungere il dispositivo Sidewalk e scaricare i file JSON che verranno utilizzati per effettuare il provisioning del dispositivo Sidewalk, esegui le seguenti operazioni API.

Argomenti

- Fase 1: Creazione di un profilo del dispositivo
- Fase 2: Aggiunta del dispositivo Sidewalk

Fase 1: Creazione di un profilo del dispositivo

Per creare un profilo del dispositivo in Account AWS, utilizza l'operazione API `CreateDeviceProfile` o il comando dell'interfaccia a riga di comando `create-device-profile`. Durante la creazione del profilo del dispositivo, specifica il nome e fornisci eventuali tag opzionali come coppie nome-valore.

Ad esempio, il comando seguente crea un profilo del dispositivo per i dispositivi Sidewalk:

```
aws iotwireless create-device-profile \
    --name sidewalk_profile --sidewalk {}
```

L'esecuzione di questo comando restituisce il nome della risorsa Amazon (ARN) e l'ID del profilo del dispositivo come output.

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

Fase 2: Aggiunta del dispositivo Sidewalk

Per aggiungere il dispositivo Sidewalk all'account per AWS IoT Core per Amazon Sidewalk, utilizza l'operazione API `CreateWirelessDevice` o il comando dell'interfaccia a riga di comando `create-wireless-device`. Durante la creazione del dispositivo, specifica i seguenti parametri, in aggiunta a un nome e una descrizione facoltativi per il dispositivo Sidewalk.

> **Note**
>
> Se desideri associare il dispositivo Sidewalk a un oggetto AWS IoT, utilizza l'operazione API `AssociateWirelessDeviceWithThing` o il comando dell'interfaccia a riga di comando `associate-wireless-device-with-thing`.

Il comando seguente mostra un esempio di creazione di un dispositivo Sidewalk:

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

Nell'esempio seguente viene mostrato il contenuto del file `device.json`.

Contenuto di device.json

```
{
  "Type": "Sidewalk",
  "Name": "SidewalkDevice",
  "DestinationName": "SidewalkDestination",
  "Sidewalk": {
    "DeviceProfileId": "12345678-a1b2-3c45-67d8-e90fa1b2c34d"
    }
}
```

L'esecuzione di questo comando restituisce l'ID dispositivo e il nome della risorsa Amazon (ARN) come output.

```
{
    "Arn": "arn:aws:iotwireless:us-east-1:123456789012:WirelessDevice/23456789-abcd-0123-bcde-fabc012345678",
    "Id": "23456789-abcd-0123-bcde-fabc012345678"
}
```

Ottenere i file JSON del dispositivo per il provisioning

Dopo aver aggiunto il dispositivo Sidewalk ad AWS IoT Core per Amazon Sidewalk, scarica il file JSON contenente le informazioni necessarie per effettuare il provisioning del dispositivo finale. Puoi recuperare queste informazioni utilizzando la console AWS IoT o AWS CLI. Per ulteriori informazioni su come effettuare il provisioning del dispositivo, consultare la pagina relativa al provisioning e alla registrazione del dispositivo finale nella documentazione di Amazon Sidewalk.

Ottenere il file JSON (console)

Per ottenere il file JSON per il provisioning del dispositivo Sidewalk:

1. Passa all'hub Dispositivi Sidewalk.
2. Scegli il dispositivo aggiunto ad AWS IoT Core per Amazon Sidewalk per visualizzarne i relativi dettagli.
3. Ottieni il file JSON scegliendo Scarica il file JSON del dispositivo nella pagina dei dettagli del dispositivo aggiunto.

   Verrà scaricato un file `certificate.json` contenente le informazioni richieste per il provisioning del dispositivo finale. Di seguito è riportato un file JSON di esempio. Contiene i certificati dei dispositivi, le chiavi private, il numero di serie di produzione Sidewalk (SMSN) e il `DeviceTypeID`.

   ```
   {
     "p256R1": "grg8izXoVvQ86cPVm0GMyWuZYHEBbbH ... DANKkOKoNT3bUGz+/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"
}
```

Nella pagina dei dettagli del dispositivo Sidewalk, verranno anche visualizzate le informazioni relative a:

- L'ID dispositivo, il nome della risorsa Amazon (ARN) e i dettagli relativi a qualsiasi oggetto AWS IoT a cui il dispositivo è associato.
- Il profilo del dispositivo e i dettagli della destinazione.
- L'ora di ricezione dell'ultimo messaggio in uplink dal dispositivo.
- Lo stato che indica se è stato effettuato il provisioning del dispositivo o se è stato registrato.

Ottenere il file JSON (CLI)

Per ottenere i file JSON per il provisioning del dispositivo finale Sidewalk utilizzando l'API AWS IoT Core per Amazon Sidewalk o AWS CLI, salva la risposta API recuperando le informazioni sul profilo del dispositivo e sul dispositivo wireless come file JSON, ad esempio *`wireless_device.json`* e *`device_profile.json`* temporaneamente. Potrai utilizzarli in seguito per effettuare il provisioning del dispositivo Sidewalk.

Di seguito viene illustrato come recuperare i file JSON.

Argomenti

- Fase 1: Ottenere le informazioni sul profilo del dispositivo come file JSON
- Fase 2: Ottenere informazioni sul dispositivo Sidewalk come un file JSON

Fase 1: Ottenere le informazioni sul profilo del dispositivo come file JSON

Utilizza l'operazione API `GetDeviceProfile` o il comando dell'interfaccia a riga di comando `get-device-profile` per ottenere informazioni sul profilo del dispositivo aggiunto all'account per AWS

IoT Core per Amazon Sidewalk. Per recuperare informazioni sul profilo del dispositivo, specifica l'ID del profilo.

L'API restituirà quindi le informazioni sul profilo del dispositivo corrispondenti all'identificatore specificato e all'ID dispositivo. Salva queste informazioni di risposta come un file e assegna un nome come *device_profile.json*.

Di seguito viene illustrato un esempio del comando dell'interfaccia a riga di comando:

```
aws iotwireless get-device-profile \
    --id "12345678-a1b2-3c45-67d8-e90fa1b2c34d" > device_profile.json
```

L'esecuzione di questo comando restituisce i parametri del profilo del dispositivo, la chiave pubblica del server di applicazioni e il `DeviceTypeID`. Di seguito viene mostrato un file JSON contenente informazioni di risposta di esempio dall'API. Per ulteriori informazioni sui parametri nella risposta API, consultare GetDeviceProfile.

Risposta API **`GetDeviceProfile`** (contenuto di ***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
    }
}
```

Fase 2: Ottenere informazioni sul dispositivo Sidewalk come un file JSON

Utilizza l'operazione API GetWirelessDevice o il comando dell'interfaccia a riga di comando get-wireless-device per ottenere informazioni sul dispositivo Sidewalk aggiunto all'account per AWS IoT Core per Amazon Sidewalk. Per ottenere informazioni sul dispositivo finale, fornisci l'identificatore del dispositivo wireless ottenuto durante l'aggiunta del dispositivo.

L'API restituirà quindi le informazioni sul dispositivo corrispondenti all'identificatore specificato e all'ID dispositivo. Salva queste informazioni di risposta come un file JSON. Assegna al file un nome significativo, ad esempio *wireless_device.json*.

Di seguito viene illustrato un esempio dell'esecuzione del comando mediante l'interfaccia a riga di comando:

```
aws iotwireless get-wireless-device --identifier-type WirelessDeviceId \
    --identifier "23456789-abcd-0123-bcde-fabc012345678" > wireless_device.json
```

L'esecuzione di questo comando restituisce i dettagli del dispositivo, i certificati dei dispositivi, le chiavi private e il numero di serie di produzione Sidewalk (SMSN). Nell'esempio seguente viene illustrato un output di esempio di esecuzione di questo comando. Per ulteriori informazioni sui parametri nella risposta API, consultare GetWirelessDevice.

Risposta API **GetWirelessDevice** (contenuto di ***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": "hDdkJw9L2uMCORjImjMHqzNR6nYYh6QKncSl5GthQNl7NKe4ounb5UMQtLjnm7zOUPYOqghCeVOLCBUiQe2Z
F+GeltcafZcFKhS+O5NPcVNR/fHYaf/cn5iUbRwlz/T
+ODXvGdwkBkgDyFgoUJgn7JdzFjaneE5qzTWXUbL79i1sXToGGjP8hiD9jJhidPWhIswleydAWgO1OZGA4CjzIaSGVM1Vta
uMMBfgAeL8Tdv5LkFIPIB3ZX9zt8zzmAuFRzI4MuNjWfIDnOF6AKu37WWU6/
QYhZoQrW9D/wndiCcsRGl+ANn367r/HE02Re4DOiCfs9f2rjc4LT1LKt7g/KW2ii+W
+9HYvvY0bBAI+AHx6Cx4j+djabTsvrgW2k6NU2zUSM7bdDP3z2a2+Z4WzBji/jYwt/
```

```
OP8rpsy5Ee4ywXUfCsfQ0rKOr0zay6yh27p3I3MZle2oCO4JIlqK0VbIQqsXzSSyp6XXS0lhmuGugZ1AAADGz
+gFBeX/ZNN8VJwnsNfgzj4me1HgVJdUo4W9kvx9cr2jHWkC3Oj/bdBTh1+yBjOC53yHlQK/
l1GHrEWiWPPnE434LRxnWkwr8EHD4oieJxC8fkIxkQfj+gHhU79Z
+oAAYAAAzsnf9SDIZPoDXF0TdC9POqTgld0oXDl2XPaVD4CvvLearrOSlFv+lsNbC4rgZn23MtIBM/7YQmJwmQ
+FXRup6Tkubg1hpz04J/09dxg8UiZmntHiUr1GfkTOFMYqRB+Aw==
"
            },
            {
                "SigningAlg": "P256r1",
                "Value": "hDdkJw9L2uMCORjImjMHqzNR6nYYh6QKncSl5GthQNmHmGU8a
+SOqDXWwDNt3VSntpbTTQl7cMIusqweQo+JPXXWElbGh7eaxPGz4ZeF5yM2cqVNUrQr1lX/6lZ
+OLuycrFrLzzB9APi0NIMLqV/Rt7XJssHQs2RPcT1ul/2XVpa6ztULJeQi2JwhTb/k48wbh/EvafG/
ibrIBIx9v7/
dwGRAPKHq7Uwb9hHnhpa8qNOUtjeUdIwJNh9vCBFX9s22t4PdortoFxbXo9C149PDDD4wqUHJGYlCsVX/
Sqqjf7Aug3h5dwdYN6cDgsuuiOm0+aBcXBGpkh7OxVxlwXkIP
+11dt23TkrSUKd0B01sc9Mc/0yEBCzx5RutKBwsefzyOl4vQX3AHgV7oD/XV73THMgGiDxQ55CPaaxN/
pm791VkQ76BSZaBeF+Su6tg0k/
eQneklt8Du5uqkyBHVxy8MvxsBIMZ73vIFwUrLHjDeq3+nOOyQqSBMnrHKU2mAwN3zb2LolwjPkKNOh1+NNnv99L2pBcNCn
+BgewzYNdWrXyKkp4O3ZDa4f+5SVWvbY5eyDDXcohvz/
OcCtuRjAkzKBCvIjBDnCv1McjVdCO3+utizGntfhAo1RZstnOoRkgVF2WuMT9IrUmzYximuTXUmWtjyFSTqgNBZwHWUTlMm
csC4HPTKr3dazdvEkhwGAAAIFByCjSp/5WHc4AhsyjMvKCsZQiKgiI8ECwjfXBaSZdY4zYsRlO3FC428H1atrFChFCZT0Bq
+vAUJiP8XqiEdXeqf2mYMJ5ykoDpwkve/cUQfPpjzFQlQfvwjBwiJDANKkOKoNT3bUGz+/f/pyTE
+xMRdIUBZ1Bw==
"
            }
        ],
        "DeviceProfileId": "0ff5b0c6-f149-4498-af34-21993acd52a7",
        "PrivateKeys": [
            {
                "SigningAlg": "Ed25519",

 "Value": "2c24d4572327f23b9bef38097137c29224a9e979081b3d90124ac9dfa477934e"
            },
            {
                "SigningAlg": "P256r1",

 "Value": "38d526f29cfaf142f596deca187bd809ef71bc13435eedc885b63bb825d63def"
            }
        ],

 "SidewalkManufacturingSn": "843764270F4BDAE3023918C89A3307AB3351EA761887A40A9DC4A5E46B6140D9",
        "Status": "PROVISIONED"
    },

    ...
```

```
}
```

Passaggi successivi

Archivia i file JSON *wireless_device.json* e *device_profile.json*temporaneamente, poiché verranno utilizzati nel passaggio successivo per effettuare il provisioning e registrare il dispositivo finale per la connessione alla piattaforma hardware. Per ulteriori informazioni, consultare la pagina relativa al provisioning e alla registrazione del dispositivo finale nella documentazione di Amazon Sidewalk.

Aggiunta di una destinazione per il dispositivo finale Sidewalk

Utilizza regole AWS IoT per elaborare i dati e i messaggi dei dispositivi e instradarli ad altri servizi. Puoi anche definire regole per elaborare i messaggi binari ricevuti da un dispositivo e convertire i messaggi in altri formati per essere utilizzati da altri servizi. Destinazioni associano il dispositivo finale Sidewalk alla regola che elabora i dati del dispositivo da inviare ad altri Servizio AWS.

Come creare e utilizzare una destinazione

1. Crea una regola AWS IoT e un ruolo IAM per la destinazione. La regola AWS IoT specifica le regole che elaborano i dati del dispositivo e li instrada per essere utilizzati da altri Servizio AWS e dalle applicazioni. Il ruolo IAM concede l'autorizzazione per accedere alla regola.
2. Crea una destinazione per i dispositivi Sidewalk utilizzando l'operazione API `CreateDestination`. Specifica il nome della destinazione, il nome della regola, il nome del ruolo ed eventuali parametri facoltativi. L'API restituirà un identificatore univoco per la destinazione, che puoi specificare durante l'aggiunta del dispositivo finale ad AWS IoT Core per Amazon Sidewalk.

Di seguito viene illustrato come creare una destinazione, una regola AWS IoT e un ruolo IAM per la destinazione.

Argomenti

- Creazione di una destinazione per il dispositivo Sidewalk
- Creazione di un ruolo IAM e della regola IoT per la destinazione

Creazione di una destinazione per il dispositivo Sidewalk

Puoi aggiungere una destinazione all'account per AWS IoT Core per Amazon Sidewalk mediante l'hub Destinazioni o `CreateDestination`. Durante la creazione della destinazione, specifica:

- Un nome univoco per la destinazione da utilizzare per il dispositivo finale Sidewalk.

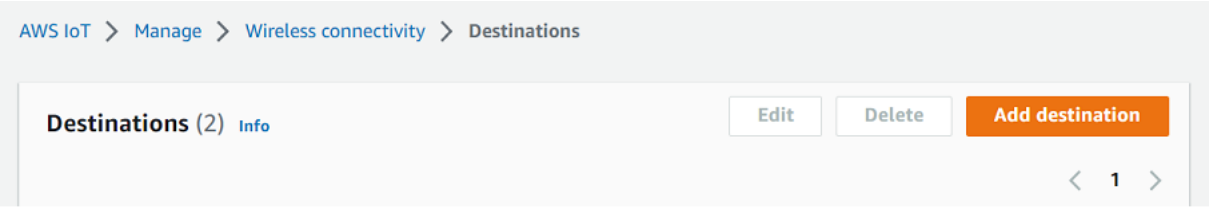
> **Note**
>
> Se aggiungi già il dispositivo utilizzando un nome della destinazione, devi usare tale nome quando crei la destinazione. Per ulteriori informazioni, consultare Fase 2: Aggiunta del dispositivo Sidewalk.

- Il nome della regola AWS IoT che elabora i dati del dispositivo e l'argomento in cui vengono pubblicati i messaggi.
- Il ruolo IAM che concede l'autorizzazione ai dati del dispositivo per accedere alla regola.

Nelle sezioni seguenti viene descritto come creare la regola AWS IoT e il ruolo IAM per la destinazione.

Creazione di una destinazione (console)

Per creare una destinazione utilizzando la console AWS IoT, passa all'hub Destinazioni e scegli Aggiungi destinazione.



Per elaborare i dati di un dispositivo, specifica i seguenti campi durante la creazione di una destinazione, quindi scegli Aggiungi destinazione.

- Dettagli della destinazione

  Inserisci un Nome della destinazione e una descrizione facoltativa per la destinazione.
- Nome regola

  La regola AWS IoT configurata per valutare i messaggi inviati dal tuo dispositivo ed elaborare i dati del dispositivo. Il nome della regola verrà mappato alla tua destinazione. La destinazione richiede la regola per elaborare i messaggi ricevuti. È possibile scegliere se elaborare i messaggi richiamando una regola AWS IoT o pubblicando sul broker di messaggi AWS IoT.
  - Se scegli Ente a rule name (Inserisci il nome di una regola), inserisci un nome, e quindi scegli Copy (Copia) per copiare il nome di una regola che inserirai quando crei la regola AWS IoT.

Puoi scegliere Create a rule (Crea una regola) per creare la regola ora o passare all'hub Rules (Regole) della console AWS IoT e creare una regola con quel nome.

Puoi anche inserire una regola e utilizzare impostazione Advanced (Avanzata) per specificare un nome dell'argomento. Il nome dell'argomento viene fornito durante l'invocazione della regola e si accede utilizzando l'espressione `topic` all'interno della regola. Per ulteriori informazioni sulle regole AWS IoT, consultare Regole AWS IoT.

- Se scegli Publish to AWS IoT message broker (Pubblica sul broker di messaggi IoT), inserisci un nome di argomento. È quindi possibile copiare il nome dell'argomento MQTT e più sottoscriventi possono iscriversi a questo argomento per ricevere messaggi pubblicati su tale argomento. Per ulteriori informazioni, consultare Argomenti MQTT.

Per ulteriori informazioni sulle regole AWS IoT per le destinazioni, consultare Creare regole per elaborare i messaggi del dispositivo LoRaWAN.

- Nome ruolo

Il ruolo IAM che fornisce al dispositivo l'autorizzazione ai dati per accedere alla regola denominata in Rule name (Nome regola). Nella console puoi creare un nuovo ruolo di servizio o selezionare un ruolo di servizio già esistente. Se stai creando un nuovo ruolo di servizio, puoi inserire un nome di ruolo (ad esempio, **`SidewalkDestinationRole`**), o lasciare vuoto per consentire a AWS IoT Core per LoRaWAN di generare un nuovo nome ruolo. AWS IoT Core per LoRaWAN creerà automaticamente il ruolo IAM con le autorizzazioni appropriate per tuo conto.

Creazione di una destinazione (interfaccia a riga di comando)

Per creare una destinazione, utilizza l'operazione API `CreateDestination` o il comando dell'interfaccia a riga di comando `create-destination`. Ad esempio, il comando seguente crea una destinazione per il dispositivo finale Sidewalk:

```
aws iotwireless create-destination --name SidewalkDestination \
    --expression-type RuleName --expression SidewalkRule \
    --role-arn arn:aws:iam::123456789012:role/SidewalkRole
```

L'esecuzione di questo comando restituisce i dettagli della destinazione, che includono il nome della risorsa Amazon (ARN) e il nome della destinazione.

```
{
```

```
    "Arn": "arn:aws:iotwireless:us-
east-1:123456789012:Destination/SidewalkDestination",
    "Name": "SidewalkDestination"
}
```

Per ulteriori informazioni sulla creazione di una destinazione, consultare Creare regole per elaborare i messaggi del dispositivo LoRaWAN.

Creazione di un ruolo IAM e della regola IoT per la destinazione

Le regole AWS IoT inviano messaggi del dispositivo ad altri servizi. Le regole AWS IoT possono anche elaborare i messaggi binari ricevuti da un dispositivo finale Sidewalk per l'utilizzo in altri servizi. Le destinazioni AWS IoT Core per Amazon Sidewalk associano un dispositivo wireless alla regola che elabora i dati dei messaggi del dispositivo da inviare ad altri servizi. La regola agisce sui dati del dispositivo non appena vengono ricevuti da AWS IoT Core per Amazon Sidewalk. Per tutti i dispositivi che inviano i propri dati allo stesso servizio, è possibile creare una destinazione che può essere condivisa da tutti i dispositivi. È inoltre necessario creare un ruolo IAM che conceda l'autorizzazione per inviare dati alla regola.

Creazione di un ruolo IAM per la destinazione

Crea un ruolo IAM che concede l'autorizzazione AWS IoT Core per Amazon Sidewalk per inviare dati alla regola AWS IoT. Per creare il ruolo, utilizza l'operazione API `CreateRole` o il comando dell'interfaccia a riga di comando `create-role`. Puoi denominare il ruolo come *`SidewalkRole`*.

```
aws iam create-role --role-name SidewalkRole \
    --assume-role-policy-document '{"Version": "2012-10-17","Statement":
 [{ "Effect": "Allow", "Principal": {"Service": "lambda.amazonaws.com"}, "Action":
 "sts:AssumeRole"}]}'
```

È inoltre possibile definire la policy di affidabilità per il ruolo utilizzando un file JSON.

```
aws iam create-role --role-name SidewalkRole \
    --assume-role-policy-document file://trust-policy.json
```

Nell'esempio seguente viene mostrato il contenuto del file JSON.

Contenuto di trust-policy.json

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Creazione di una regola per la destinazione

Utilizza l'operazione API AWS IoT Core, `CreateTopicRule` o il comando AWS CLI, `create-topic-rule`, per creare una regola. La regola dell'argomento verrà utilizzata dalla destinazione per instradare i dati ricevuti dal dispositivo finale Sidewalk ad altri Servizi AWS. Ad esempio, è possibile creare un'operazione della regola che invia un messaggio a una funzione Lambda. È possibile definire la funzione Lambda in modo che riceva i dati dell'applicazione dal dispositivo e utilizzi base64 per decodificare i dati del payload in modo da poter essere utilizzati da altre applicazioni.

Nelle fasi seguenti viene illustrato come creare la funzione Lambda e quindi una regola dell'argomento che invia un messaggio a questa funzione.

1. Creazione del ruolo di esecuzione e della policy

   Crea il ruolo IAM che concede alla funzione l'autorizzazione per accedere alle risorse AWS. È inoltre possibile definire la policy di affidabilità per il ruolo utilizzando un file JSON.

   ```
   aws iam create-role --role-name lambda-ex \
       --assume-role-policy-document file://lambda-trust-policy.json
   ```

   Nell'esempio seguente viene mostrato il contenuto del file JSON.

   Contenuto di lambda-trust-policy.json

   ```
   {
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Principal": {
   ```

```
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. Creazione e verifica della funzione Lambda

   Esegui la procedura seguente per creare una funzione AWS Lambda che esegue la decodifica base64 dei dati del payload.

   a. Scrivi il codice per decodificare i dati del payload. Ad esempio, puoi utilizzare il seguente codice Python di esempio. Specifica un nome per lo script, ad esempio *base64_decode.py*.

      Contenuto di 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. Crea un pacchetto di implementazione come un file zip contenente il file Python e assegna un nome come *base64_decode.zip*. Utilizza l'API `CreateFunction` o il comando dell'interfaccia a riga di comando `create-function` per creare una funzione Lambda per il codice di esempio, *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
      ```

Vedrai il seguente output. Durante la creazione della regola dell'argomento, utilizzerai il valore nome della risorsa Amazon (ARN) dell'output, `FunctionArn`.

```
{
    "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": "FpFMvUhayLkOoVBpNuNiIVML/tuGv2iJQ7t0yWVTU8c=",
    "Version": "$LATEST",
    "TracingConfig": {
        "Mode": "PassThrough"
    },
    "RevisionId": "88ebe1e1-bfdf-4dc3-84de-3017268fa1ff",
    ...
}
```

d. Per ottenere i log per una chiamata dalla riga di comando, utilizza l'opzione `--log-type` con il comando `invoke`. La risposta include un campo LogResult contenente fino a 4 KB di log con codifica base64 dalla chiamata.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

La risposta ricevuta deve contenere un `StatusCode` di 200. Per ulteriori informazioni sulla creazione e l'utilizzo di funzioni Lambda da AWS CLI, consultare Utilizzo di Lambda con AWS CLI.

3. Creazione di una regola dell'argomento

Utilizza l'API `CreateTopicRule` o il comando dell'interfaccia a riga di comando `create-topic-rule` per creare una regola dell'argomento che invia un messaggio a questa funzione Lambda. Puoi anche aggiungere una seconda operazione della regola che ripubblica su un argomento AWS IoT. Assegna a questa regola dell'argomento un nome come *`Sidewalkrule`*.

```
aws iot create-topic-rule --rule-name Sidewalkrule \
    --topic-rule-payload file://myrule.json
```

Puoi utilizzare il file `myrule.json` per specificare ulteriori dettagli relativi alla regola. Ad esempio, il seguente file JSON mostra come ripubblicare su un argomento AWS IoT e inviare un messaggio a una funzione 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/SidewalkRrepublishRole",
                 "topic": "project/sensor/observed"
             }
        }
    ],
}
```

Connetti il tuo dispositivo Sidewalk e visualizza il formato dei metadati uplink

In questo tutorial, verrà utilizzato il client di test MQTT per testare la connettività e visualizzare i messaggi scambiati tra il dispositivo finale e Cloud AWS. Per ricevere messaggi, nel client di test MQTT, effettua la sottoscrizione all'argomento specificato durante la creazione della regola IoT per la destinazione. Puoi anche inviare un messaggio in downlink da AWS IoT Core per Amazon Sidewalk al dispositivo utilizzando l'operazione API `SendDataToWirelessDevice`. Puoi verificare che il messaggio sia stato recapitato abilitando la notifica eventi per lo stato della consegna del messaggio.

> **Note**
>
> Per informazioni sulla connessione della piattaforma hardware e la relativa configurazione, consultare le pagine relative al provisioning e alle registrazione del dispositivo finale e alla configurazione del kit di sviluppo dell'hardware (HDK) nella documentazione di Amazon Sidewalk.

Invio di messaggi in downlink al dispositivo finale

Utilizza l'operazione API `SendDataToWirelessDevice` o il comando dell'interfaccia a riga di comando `send-data-to-wireless-device` per inviare messaggi in downlink da AWS IoT Core per Amazon Sidewalk al dispositivo finale Sidewalk. Di seguito viene illustrato un esempio di come eseguire questo comando. I dati del payload sono i dati binari da inviare, codificati in base64.

```
aws iotwireless send-data-to-wireless-device \
    --id "<Wireless_Device_ID>" \
    --payload-data "SGVsbG8gVG8gRGV2c2lt" \
    --wireless-metadata Sidewalk={Seq=1,AckModeRetryDurationSecs=10}
```

Di seguito viene mostrato un output di esempio di esecuzione di questo comando, che è un ID del messaggio in downlink inviato al dispositivo.

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

> **Note**
>
> L'API `SendDataToWirelessDevice` può restituire un ID messaggio, ma il messaggio potrebbe non essere recapitato correttamente. Per verificare lo stato del messaggio inviato al dispositivo, è possibile abilitare gli eventi sullo stato della consegna del messaggio per gli account e i dispositivi Sidewalk. Per ulteriori informazioni su come abilitare questo evento, consultare Notifiche di eventi per le risorse Sidewalk. Per ulteriori informazioni su questo tipo di evento, consultare Eventi di consegna dei messaggi.

Visualizzazione del formato dei messaggi in uplink dal dispositivo

Dopo aver collegato il dispositivo, è possibile effettuare la sottoscrizione all'argomento (ad esempio, *project/sensor/observed*) specificato durante la creazione della regola di destinazione e osservare i messaggi in uplink dal dispositivo.

Se durante la creazione della destinazione è stato specificato il nome di un argomento, è possibile eseguire la sottoscrizione all'argomento per monitorare i messaggi in uplink dal dispositivo finale. Passa a Client di test MQTT nella pagina Test della console AWS IoT, inserisci il nome dell'argomento (ad esempio, *project/sensor/observed*), quindi scegli Sottoscrizione.

Nell'esempio seguente viene illustrato il formato dei messaggi di uplink inviati da dispositivi Sidewalk ad AWS IoT. `WirelessMetadata` contiene metadati relativi alla richiesta di messaggio.

```
{
   "PayloadData":"ZjRlNjY1ZWNlNw==",
   "WirelessDeviceId":"wireless_device_id",
   "WirelessMetadata":{
      "Sidewalk":{
         "CmdExStatus":"Cmd",
         "SidewalkId":"device_id",
         "Seq":0,
         "MessageType":"messageType"
      }
    }
}
```

Nella tabella seguente viene illustrata una definizione dei diversi parametri nei metadati uplink. *device-id* è l'ID del dispositivo wireless, ad esempio *ABCDEF1234*, e *messageType* è il tipo di messaggio in uplink ricevuto dal dispositivo.

Parametri dei metadati uplink di Sidewalk

Parametro	Descrizione	Type	Richiesto
`PayloadData`	Il payload del messaggio inviato dal dispositivo wireless.	Stringa	Sì
`WirelessDeviceID`	L'identificatore del dispositivo wireless che invia i dati	Stringa	Sì

Parametro	Descrizione	Type	Richiesto
`Sidewalk.CmdExStatus`	Stato del comando runtime. I messaggi del tipo di risposta devono includere il codice di stato, `COMMAND_EXEC_STATUS_SUCCESS` . Tuttavia, le notifiche potrebbero non includere il codice di stato.	Enumerazione	No
`Sidewalk.NackExStatus`	Stato del nack di risposta, che può essere `RADIO_TX_ERROR` o `MEMORY_ERROR` .	Gamma di stringhe	No

Dispositivi di provisioning in blocco con AWS IoT Core per Amazon Sidewalk

È possibile utilizzare il provisioning in blocco per eseguire l'onboarding di un numero elevato di dispositivi finali in AWS IoT Core per Amazon Sidewalk in blocco. Il provisioning in blocco è utile soprattutto quando si produce un numero elevato di dispositivi in una fabbrica e si desidera eseguirne l'onboarding in AWS IoT. Per ulteriori informazioni sulla produzione di dispositivi, consultare la pagina relativa alla produzione di dispositivi Amazon Sidewalk nella documentazione di Amazon Sidewalk.

Negli argomenti riportati di seguito viene illustrato il funzionamento del provisioning in blocco.

- Flusso di lavoro del provisioning in blocco Amazon Sidewalk

  In questo argomento vengono illustrati alcuni concetti chiave del provisioning in blocco e del relativo funzionamento. Vengono anche illustrati i passaggi che devono essere eseguiti per poter importare i dispositivi in AWS IoT Core per Amazon Sidewalk.
- Creazione dei profili dei dispositivi con supporto di fabbrica

  In questo argomento viene descritto come creare un profilo del dispositivo e ottenere il supporto di fabbrica corrispondente. Verranno inoltre fornite informazioni su come recuperare la chiave YubiHSM e inviarla al produttore per ottenere il log di controllo dopo che i dispositivi sono stati prodotti.
- Provisioning dei dispositivi Sidewalk mediante attività di importazione

In questo argomento viene illustrato come eseguire il provisioning in blocco dei dispositivi Sidewalk creando e utilizzando attività di importazione. Verrà anche descritto come aggiornare o eliminare le attività di importazione e visualizzare lo stato dell'attività di importazione e dei dispositivi nell'attività.

Argomenti

Flusso di lavoro del provisioning in blocco Amazon Sidewalk

Nelle sezioni seguenti vengono illustrati i concetti chiave del provisioning in blocco e il relativo funzionamento. Le fasi coinvolte nel provisioning in blocco includono:

1. Creazione di un profilo del dispositivo mediante AWS IoT Core per Amazon Sidewalk.
2. Richiesta al team Amazon Sidewalk di una chiave YubiHSM e aggiornamento del profilo del dispositivo con supporto di fabbrica.
3. Invio della chiave YubiHSM al produttore affinché AWS IoT Core per Amazon Sidewalk possa ottenere il log di controllo una volta che i dispositivi sono stati prodotti.
4. Creazione di un'attività di importazione e fornitura dei numeri di serie (SMSN) dei dispositivi per cui eseguire l'onboarding in AWS IoT Core per Amazon Sidewalk.

Componenti del provisioning in blocco

I concetti seguenti illustrano alcuni componenti chiave del provisioning in blocco e come utilizzarli come parte del provisioning in blocco di dispositivi Sidewalk.

Chiave YubiHSM

Amazon crea uno o più HSM (moduli di sicurezza hardware) per ciascuno dei prodotti Sidewalk. Ogni HSM dispone di un numero di serie univoco, chiamato chiave YubiHSM, stampato sul modulo hardware. È possibile acquistare questa chiave dalla pagina web di Yubico.

La chiave è univoca per ciascun HSM e legata a ogni profilo del dispositivo creato con AWS IoT Core per Amazon Sidewalk. Per ottenere la chiave YubiHSM, contatta il team di Amazon Sidewalk. Se si invia la chiave YubiHSM al produttore, dopo che i dispositivi Sidewalk sono stati prodotti in

fabbrica, AWS IoT Core per Amazon Sidewalk riceverà un file di log di controllo contenente i numeri di serie dei dispositivi. Queste informazioni vengono confrontate con il file CSV di input per eseguire l'onboarding dei dispositivi in AWS IoT.

Chiave di attestazione del dispositivo (**DAK**)

Quando un dispositivo finale Sidewalk partecipa alla rete Sidewalk, occorre assegnare un certificato dispositivo Sidewalk. I certificati utilizzati per configurare il dispositivo includono un certificato privato specifico del dispositivo e i certificati dei dispositivi pubblici, che corrispondono alla catena di certificati Sidewalk. Quando i dispositivi Sidewalk vengono prodotti, YubiHSM firma i certificati dei dispositivi.

Di seguito viene illustrato un file JSON di esempio contenente i certificati dei dispositivi e le chiavi private. Per ulteriori informazioni, consultare Ottenere i file JSON del dispositivo per il provisioning.

```
{
  "p256R1": "grg8izXoVvQ86cPVm0GMyWuZYHEBbbH ... DANKkOKoNT3bUGz+/f/pyTE
+xMRdIUBZ1Bw==",
  "eD25519": "grg8izXoVvQ86cPVm0GMyWuZYHEBbbHD ... UiZmntHiUr1GfkTOFMYqRB+Aw==",
  "metadata": {
    "devicetypeid": "fe98",

    ...

    "devicePrivKeyP256R1":
 "3e704bf8d319b3a475179f1d68c60737b28c708f845d0198f2d00d00c88ee018",
    "devicePrivKeyEd25519":
 "17dacb3a46ad9a42d5c520ca5f47f0167f59ce54d740aa13918465faf533b8d0"
  },
  "applicationServerPublicKey":
 "5ce29b89c2e3ce6183b41e75fe54e45f61b8bb320efbdd2abd7aefa5957a316b"
}
```

La chiave di attestazione del dispositivo (DAK) è una chiave privata ottenuta durante la creazione del profilo del dispositivo. Corrisponde al certificato del prodotto, che è un certificato univoco rilasciato per ciascun prodotto Sidewalk. Quando contatti il team di Amazon Sidewalk, riceverai la catena di certificati Sidewalk, la chiave YubiHSM e un HSM con assegnata la chiave di attestazione del dispositivo (DAK) del prodotto.

Il profilo del dispositivo viene inoltre aggiornato con la nuova chiave di attestazione del dispositivo (DAK) e con il supporto di fabbrica abilitato. Le informazioni sui metadati DAK del profilo del

dispositivo forniscono dettagli come il nome DAK, l'ID certificato, l'APId (Advertised Product ID), se il supporto di fabbrica è abilitato e il numero massimo di firme che possono essere apportate dal DAK.

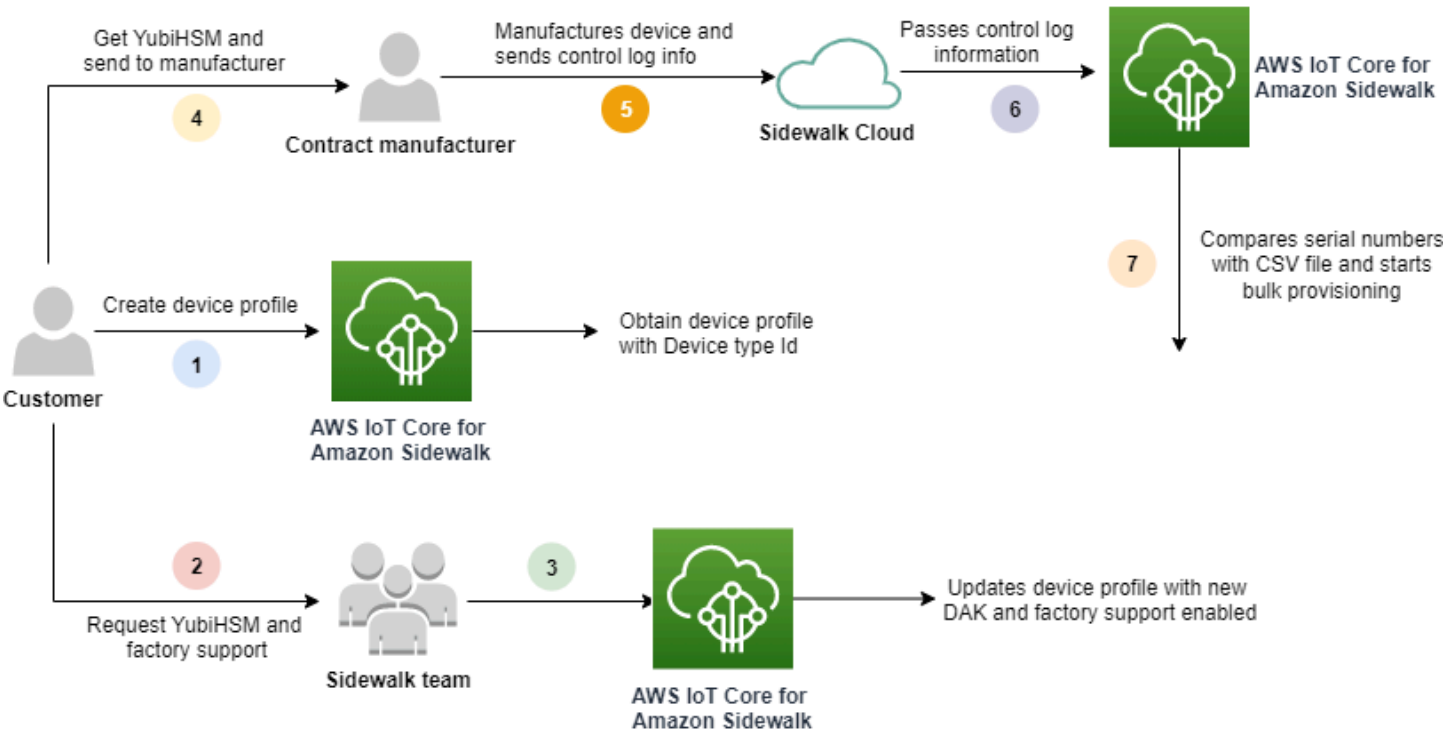
Advertised product ID (**`ApId`**)

Il parametro `ApId` è una stringa alfanumerica che identifica il prodotto pubblicizzato. Questo campo deve essere specificato quando si desidera utilizzare un determinato profilo del dispositivo per i dispositivi Sidewalk di cui si esegue il provisioning in blocco. AWS IoT Core per Amazon Sidewalk genera quindi la DAK e la fornisce all'utente tramite la chiave YubiHSM. Le informazioni DAK correlate verranno presentate nel profilo del dispositivo.

Per ottenere il `ApId`, dopo aver recuperato le informazioni relative al profilo del dispositivo creato, contatta il team di supporto di Amazon Sidewalk. Le informazioni sul profilo del dispositivo possono essere ottenute dalla console AWS IoT o mediante l'operazione API `GetDeviceProfile` o il comando dell'interfaccia a riga di comando `get-device-profile`.

Funzionamento del provisioning in blocco

Questo diagramma illustra il funzionamento del provisioning in blocco con AWS IoT Core per Amazon Sidewalk.



Nella procedura seguente vengono descritte le diverse fasi del processo di provisioning in blocco.

1. Creazione del profilo del dispositivo per il dispositivo Sidewalk

   Prima di portare il dispositivo finale in fabbrica, crea innanzitutto un profilo del dispositivo. Puoi utilizzare questo profilo per effettuare il provisioning di singoli dispositivi come descritto in Aggiunta del profilo del dispositivo e del dispositivo finale Sidewalk.

2. Richiesta del supporto di fabbrica per il profilo

   Quando sei pronto per portare il dispositivo finale in fabbrica, richiedi al team di Amazon Sidewalk la chiave YubiHSM e il supporto di fabbrica per il profilo del dispositivo.

3. Ottenere DAK e profilo supportato in fabbrica

   Il team di supporto di Amazon Sidewalk aggiornerà il profilo del dispositivo con la chiave di attestazione del dispositivo (DAK) del prodotto e il supporto di fabbrica. Il profilo del dispositivo verrà aggiornato automaticamente con un APId (advertised product ID) e una nuova DAK e informazioni sul certificato, come l'ID certificato. I dispositivi Sidewalk che utilizzano questo profilo dispongono dei requisiti per l'utilizzo con il provisioning di massa.

4. Invio della chiave YubiHSM al produttore (CM)

   Il dispositivo finale è ora qualificato, pertanto puoi inviare la chiave YubiHSM al produttore per conto terzi (CM) per avviare il processo di produzione. Per ulteriori informazioni, consultare la pagina relativa alla produzione di dispositivi Amazon Sidewalk nella documentazione di Amazon Sidewalk.

5. Produzione di dispositivi e invio di log di controllo e numeri di serie

   Il CM produce i dispositivi e genera log di controllo. Il CM fornisce inoltre un file CSV contenente un elenco di dispositivi da produrre e i relativi numeri di serie di produzione Sidewalk (SMSN). Nel codice seguente viene illustrato un log di controllo di esempio. Contiene i numeri di serie del dispositivo, l'APID e i certificati dei dispositivi pubblici.

```
{
    "controlLogs": [
    {
        "version": "4-0-1",
        "device":
        {
            "serialNumber": "device1",
            "productIdentifier": {
                "advertisedProductId": "abCD"
             },
```

```
            "sidewalkData": {
               "SidewalkED25519CertificateChain": "...",
               "SidewalkP256R1CertificateChain": "..."
            }
         }
      }
   ]
}
```

6. Passaggio delle informazioni del log di controllo ad AWS IoT Core per Amazon Sidewalk

   Il cloud Amazon Sidewalk recupera le informazioni del log di controllo dal produttore e le passa ad AWS IoT Core per Amazon Sidewalk. I dispositivi possono quindi essere creati insieme ai relativi numeri di serie.

7. Verifica della corrispondenza del numero di serie e avvio del provisioning in blocco

   Quando utilizzi la console AWS IoT o l'operazione API `StartWirelessDeviceImportTask` AWS IoT Core per Amazon Sidewalk, AWS IoT Core confronta il numero di serie di produzione Sidewalk (SMSN) di ogni dispositivo ottenuto da Amazon Sidewalk con i numeri di serie corrispondenti nel file CSV. Se queste informazioni corrispondono, il processo di provisioning in blocco viene avviato e vengono creati i dispositivi da importare in AWS IoT Core per Amazon Sidewalk.

Creazione dei profili dei dispositivi con supporto di fabbrica

Prima di poter eseguire il provisioning in blocco dei dispositivi Amazon Sidewalk, è necessario creare un profilo del dispositivo e quindi contattare il team di supporto di Amazon Sidewalk per richiedere il supporto di fabbrica. Il team di Amazon Sidewalk aggiornerà il profilo del dispositivo con una nuova chiave di attestazione del dispositivo (DAK), aggiungendo il relativo supporto di fabbrica. I dispositivi Sidewalk che utilizzano questo profilo sono quindi qualificati per l'utilizzo con AWS IoT Core per Amazon Sidewalk ed è possibile eseguire l'onboarding per il provisioning in blocco.

Nella procedura seguente viene illustrato come creare un profilo del dispositivo supportato in fabbrica.

1. Creazione di un profilo del dispositivo

   Crea innanzitutto un profilo del dispositivo. Quando crei un profilo, specifica un nome e dei tag opzionali come coppie nome-valore. Per ulteriori informazioni sui parametri richiesti, nonché la creazione e l'utilizzo dei profili, consultare Come creare e aggiungere il dispositivo.

2. Ottenere il supporto di fabbrica per il profilo

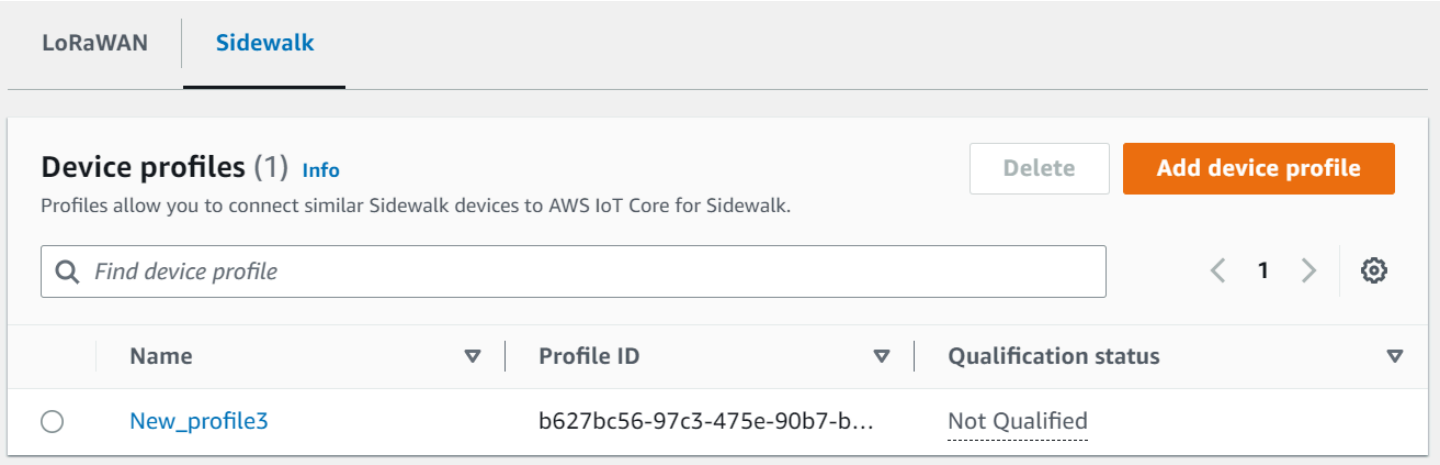
   Ottieni il supporto di fabbrica per il profilo del dispositivo affinché sia possibile qualificare i dispositivi che utilizzano questo profilo. Per la qualifica, crea un ticket con il team di Amazon Sidewalk. Dopo la conferma da parte del team, riceverai un ApId (advertised product ID) e il profilo verrà aggiornato con una DAK rilasciata in fabbrica. I dispositivi finali Sidewalk che utilizzano questo profilo saranno qualificati.

È possibile creare un profilo del dispositivo utilizzando la console AWS IoT, le operazioni API AWS IoT Core per Amazon Sidewalk o la AWS CLI.

Argomenti

Creazione di un profilo (console)

Per creare un profilo del dispositivo utilizzando la console AWS IoT, passa alla scheda Sidewalk dell'hub Profili e scegli Crea profilo.



Per creare un profilo, specifica i campi seguenti, quindi scegli Invia.

- Nome

  Inserisci un Nome per il profilo.

- Tag

Inserisci tag opzionali come coppie nome-valore per semplificare l'identificazione del profilo. I tag semplificano inoltre il monitoraggio dei costi di fatturazione.

Visualizzazione delle informazioni sul profilo e qualifica dei profili

Il profilo creato verrà visualizzato nell'hub Profili. Seleziona il profilo per visualizzare i relativi dettagli. Verranno visualizzate le informazioni seguenti:

- Il nome e l'identificatore univoco del profilo del dispositivo, nonché gli eventuali tag opzionali specificati come coppie nome-valore.
- La chiave pubblica del server di applicazioni e l'ID tipo dispositivo del profilo.
- Lo stato di qualifica, che indica che stai utilizzando un profilo del dispositivo non supportato in fabbrica. Per qualificare il profilo del dispositivo in modo che sia supportato in fabbrica, contatta il supporto Amazon Sidewalk.
- Le informazioni sulla chiave di attestazione del dispositivo (DAK). Dopo che il dispositivo è stato qualificato, verrà emessa una nuova DAK e il profilo verrà aggiornato automaticamente con le nuove informazioni DAK.

Creazione di un profilo (interfaccia a riga di comando)

Per creare un profilo del dispositivo, utilizza l'operazione API `CreateDeviceProfile` o il comando dell'interfaccia a riga di comando `create-device-profile`. Ad esempio, il comando seguente crea un profilo per il dispositivo finale Sidewalk.

```
aws iotwireless create-device-profile \
    --name sidewalk_device_profile --sidewalk {}
```

L'esecuzione di questo comando restituisce i dettagli del profilo, che includono il nome della risorsa Amazon (ARN) e l'ID del profilo.

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

Visualizzazione delle informazioni sul profilo e qualifica dei profili

Utilizza l'operazione API GetDeviceProfile o il comando dell'interfaccia a riga di comando get-device-profile per ottenere informazioni sul profilo del dispositivo aggiunto all'account per AWS IoT Core per Amazon Sidewalk. Per recuperare informazioni sul profilo del dispositivo, specifica l'ID del profilo. L'API restituirà quindi le informazioni sul profilo del dispositivo corrispondenti all'identificatore specificato.

Di seguito viene illustrato un esempio del comando dell'interfaccia a riga di comando:

```
aws iotwireless get-device-profile \
    --id "12345678-234a-45bc-67de-e8901234f0a1" > device_profile.json
```

L'esecuzione di questo comando restituisce i parametri del profilo del dispositivo, la chiave pubblica del server di applicazioni, il `DeviceTypeId`, `ApId`, lo stato di qualifica e le informazioni `DAKCertificate`.

In questo esempio, lo stato di qualifica e le informazioni DAK indicano che il profilo del dispositivo non è qualificato. Per qualificare il profilo, contattare il supporto Amazon Sidewalk. Verrà emesso una nuova DAK per il profilo senza limite dispositivo.

```
{
    "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
    }
}
```

Dopo che il team di supporto di Amazon Sidewalk conferma queste informazioni, riceverai l'APID e una DAK supportata in fabbrica, come mostrato nell'esempio seguente.

> **Note**
>
> Il `MaxAllowedSignature` di `-1` indica che la DAK non contiene un limite del dispositivo. Per informazioni sui parametri DAK, consultare 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
    }
}
```

Passaggi successivi

Dopo aver creato un profilo del dispositivo che dispone di una DAK supportata in fabbrica, fornisci al produttore la chiave YubiHSM ottenuta dal team. I dispositivi verranno quindi prodotti in fabbrica e le informazioni del log di controllo verranno passate ad Amazon Sidewalk, che contiene i numeri di serie (SMSN) dei dispositivi. Per ulteriori informazioni su questo flusso di lavoro, consultare la pagina relativa alla produzione di dispositivi Amazon Sidewalk nella documentazione di Amazon Sidewalk.

È quindi possibile effettuare il provisioning in blocco dei dispositivi Sidewalk fornendo ad AWS IoT Core per Amazon Sidewalk i numeri di serie dei dispositivi di cui eseguire l'onboarding. Quando

AWS IoT Core per Amazon Sidewalk riceve il log di controllo, confronta i numeri di serie nel log di controllo con i numeri di serie forniti. Se i numeri di serie corrispondono, l'attività di importazione avvia l'onboarding dei dispositivi in AWS IoT Core per Amazon Sidewalk. Per ulteriori informazioni, consultare Provisioning dei dispositivi Sidewalk mediante attività di importazione.

Provisioning dei dispositivi Sidewalk mediante attività di importazione

In questa sezione viene illustrato come effettuare il provisioning in blocco di dispositivi Sidewalk utilizzando la console AWS IoT, le operazioni API AWS IoT Core per Amazon Sidewalk o la AWS CLI. Nelle sezioni seguenti viene descritto come eseguire il provisioning in blocco dei dispositivi Sidewalk.

Argomenti

Funzionamento del provisioning in blocco Sidewalk

Nella procedura seguente viene illustrato il funzionamento del provisioning in blocco.

1. Avvio dell'attività di importazione di dispositivi wireless

   Per effettuare il provisioning in blocco dei dispositivi Sidewalk, è necessario creare un'attività di importazione e fornire il numero di serie di produzione Sidewalk (SMSN) dei dispositivi di cui eseguire l'onboarding in AWS IoT Core per Amazon Sidewalk. Il numero di serie di produzione Sidewalk (SMSN) dei dispositivi è stato ottenuto come un file CSV nella casella e-mail dopo che il produttore ha caricato i log di controllo in Amazon Sidewalk. Per ulteriori informazioni sul flusso di lavoro e come ottenere il log di controllo, consultare la pagina relativa alla produzione di dispositivi Amazon Sidewalk nella documentazione di Amazon Sidewalk.
2. Esecuzione del processo di importazione in background

   Quando AWS IoT Core per Amazon Sidewalk riceve la richiesta di attività di importazione, inizia a configurare gli oggetti e avvia un processo in background che esegue il polling del

sistema frequentemente. Dopo che il processo in background riceve le istruzioni dell'attività di importazione, inizia a leggere il file CSV. AWS IoT Core per Amazon Sidewalk verifica contemporaneamente se i log di controllo sono stati ricevuti da Amazon Sidewalk.

3. Creazione di record di dispositivi wireless

   Quando il log di controllo viene ricevuto da Amazon Sidewalk, AWS IoT Core per Amazon Sidewalk verifica se i numeri di serie nel log di controllo corrispondono ai valori SMSN nel file CSV. Se i numeri di serie corrispondono, AWS IoT Core per Amazon Sidewalk inizierà a creare record di dispositivi wireless per i dispositivi Sidewalk che corrispondono a questi numeri di serie. Dopo che è stato eseguito l'onboarding di tutti i dispositivi, l'attività di importazione viene contrassegnata come Completata.

Considerazioni chiave per il provisioning in blocco di Sidewalk

Di seguito sono riportate alcune considerazioni chiave quando si esegue il provisioning in blocco dei dispositivi Sidewalk in AWS IoT Core per Amazon Sidewalk.

- Il provisioning in blocco deve essere eseguito utilizzando la console AWS IoT o le operazioni API AWS IoT Core per Amazon Sidewalk nello stesso Account AWS in cui è stato creato il profilo del dispositivo.
- Prima di eseguire il provisioning in blocco dei dispositivi Sidewalk, il profilo del dispositivo deve già contenere informazioni sulla DAK che indicano il supporto di fabbrica. In caso contrario, il provisioning in blocco mediante la console AWS IoT o le operazioni API di provisioning in blocco potrebbero non andare a buon fine.
- Dopo aver avviato un'attività di importazione, possono essere necessari almeno 10 minuti per elaborare il file CSV, importare i dispositivi wireless ed eseguire l'onboarding in AWS IoT Core per Amazon Sidewalk.
- L'attività di importazione dei dispositivi wireless verrà eseguita per 90 giorni, una volta avviata. Durante questo periodo di tempo, viene verificato se i log di controllo sono stati ricevuti da Amazon Sidewalk. Se il log di controllo non viene ricevuto da Amazon Sidewalk entro 90 giorni, l'attività verrà contrassegnata come Completata con un messaggio che indica che è scaduta quando si visualizzano i dettagli dell'attività. Lo stato di onboarding dei dispositivi nell'attività di importazione che erano in attesa del log di controllo verrà contrassegnato come Non riuscito.
- Quando tenti di aggiornare un'attività di importazione già creata, puoi aggiungere solo ulteriori dispositivi all'attività. Puoi aggiungere nuovi dispositivi in qualsiasi momento dopo la creazione di un'attività di importazione e prima che l'attività venga avviata sui dispositivi che erano già stati

aggiunti all'attività di importazione. Se il file di aggiornamento contiene numeri di serie di dispositivi che esistono già nell'attività di importazione originale, questi numeri di serie verranno ignorati.

- Quando richiedi un'operazione di aggiornamento, lo stesso ruolo IAM utilizzato durante la creazione dell'attività di importazione verrà assunto per accedere al file CSV nel bucket Amazon S3.
- Un'attività di importazione può essere eliminata solo se è già stata completata o se l'aggiornamento dell'attività non è riuscito. L'aggiornamento di un'attività potrebbe non riuscire quando, ad esempio, è stato fornito un ruolo IAM errato o quando non è stato trovato un file bucket Amazon S3. Un'attività di importazione non può essere aggiornata o eliminata se si trova nello stato `PENDING`.
- Il file CSV importato nell'attività deve utilizzare il formato descritto nella sezione seguente.

Formato di file CSV

Il file CSV contenuto in un bucket Amazon S3 specificato per l'attività di importazione deve utilizzare il formato seguente:

- La riga 1 deve utilizzare la parola chiave `smsn`, che indica che il file CSV in corso di importazione contiene l'SMSN dei dispositivi da importare.
- La riga 2 e quelle successive devono contenere l'SMSN dei dispositivi di cui eseguire l'onboarding. L'SMSN del dispositivo deve essere nel formato a 64 caratteri esadecimali.

Il file JSON seguente mostra un formato di file CSV di esempio.

```
smsn
1C1A10B0AC0A200C012BBAC2CBB1B21CB12C0CA2AC1C1BB22CAA01C1B0B01122
B122C2B1121BACA2221001AC1B22012AAC11112C11C2A100C1C2B012A1100C10
02B222C110B0A210B0A0C2C112CCCAC21C1C0B0AA1221AB1022A2CC11B1B1122
C2C021CA1C111CCAB1221C0021C1C2AAA0AA1A2A01ABC10CBAACCA2A0121022A
0CB22C01BBC2CA2C0B11001121ACB2ABB0BB0121C2BA101C012CC2B20C011AC0
```

Come utilizzare il provisioning in blocco Sidewalk

Nella procedura seguente viene illustrato come utilizzare il provisioning in blocco Amazon Sidewalk.

1. Fornire i numeri di serie del dispositivo

   Per eseguire il provisioning in blocco dei dispositivi Sidewalk, occorre fornire i numeri di serie dei dispositivi di cui eseguire l'onboarding. Puoi eseguire il provisioning dei dispositivi utilizzando uno dei seguenti metodi.

   - Effettua il provisioning di ciascun dispositivo singolarmente utilizzando il numero di serie di produzione Sidewalk (SMSN). Questo metodo è utile quando desideri eseguire il test del flusso di lavoro ed eseguire l'onboarding del dispositivo più rapidamente senza dover caricare un file CSV con il ruolo IAM appropriato o attendere che i dispositivi siano pronti per eseguirne l'onboarding nell'attività.
   - Effettua il provisioning in blocco dei dispositivi fornendo un URL del bucket Amazon S3 contenente l'SMSN dei dispositivi di cui effettuare il provisioning in un file CSV. Questo metodo è particolarmente utile quando disponi di un numero elevato di dispositivi di cui eseguire l'onboarding. In questo caso, l'onboarding di ciascun dispositivo singolarmente può essere noioso. Invece, è sufficiente fornire il percorso del file CSV che è stato caricato in un bucket Amazon S3 e il ruolo IAM per accedere al file.

2. Ottenere l'attività di importazione e lo stato di onboarding dei dispositivi

   Per ogni attività di importazione creata, puoi recuperare informazioni sullo stato di onboarding dell'attività e sullo stato di onboarding dei dispositivi aggiunti all'attività. Puoi anche visualizzare ulteriori informazioni sullo stato, ad esempio un motivo per cui l'onboarding di un'attività o di un dispositivo non è andato a buon fine. Per ulteriori informazioni, consulta la pagina

3. (Facoltativo) Aggiornamento o eliminazione dell'attività di importazione

   Puoi aggiornare o eliminare l'attività di importazione creata in precedenza.

   - Puoi aggiornare un'attività di importazione e aggiungere ulteriori dispositivi all'attività in qualsiasi momento prima che l'attività venga avviata sui dispositivi che sono già stati aggiunti. AWS IoT Core per Amazon Sidewalk assume lo stesso ruolo IAM utilizzato durante la creazione dell'attività di importazione. Quando crei l'attività, specifica il nuovo file CSV contenente i numeri di serie dei dispositivi che desideri aggiungere all'attività.

     > **Note**
     >
     > Durante l'aggiornamento di un'attività di importazione esistente, puoi solo aggiungere dispositivi all'attività. AWS IoT Core per Amazon Sidewalk esegue un'operazione di unione tra i dispositivi già presenti nell'attività di importazione e i dispositivi che stai

tentando di aggiungere all'attività. Se il nuovo file contiene numeri di serie di dispositivi che esistono già nell'attività di importazione, questi numeri di serie verranno ignorati.

- Puoi eliminare un'attività di importazione che è già stata completata o un'attività di importazione che non è stato possibile aggiornare come quando le informazioni sul ruolo IAM non sono corrette o quando un file del bucket S3 non è disponibile durante la creazione o l'aggiornamento di un'attività.

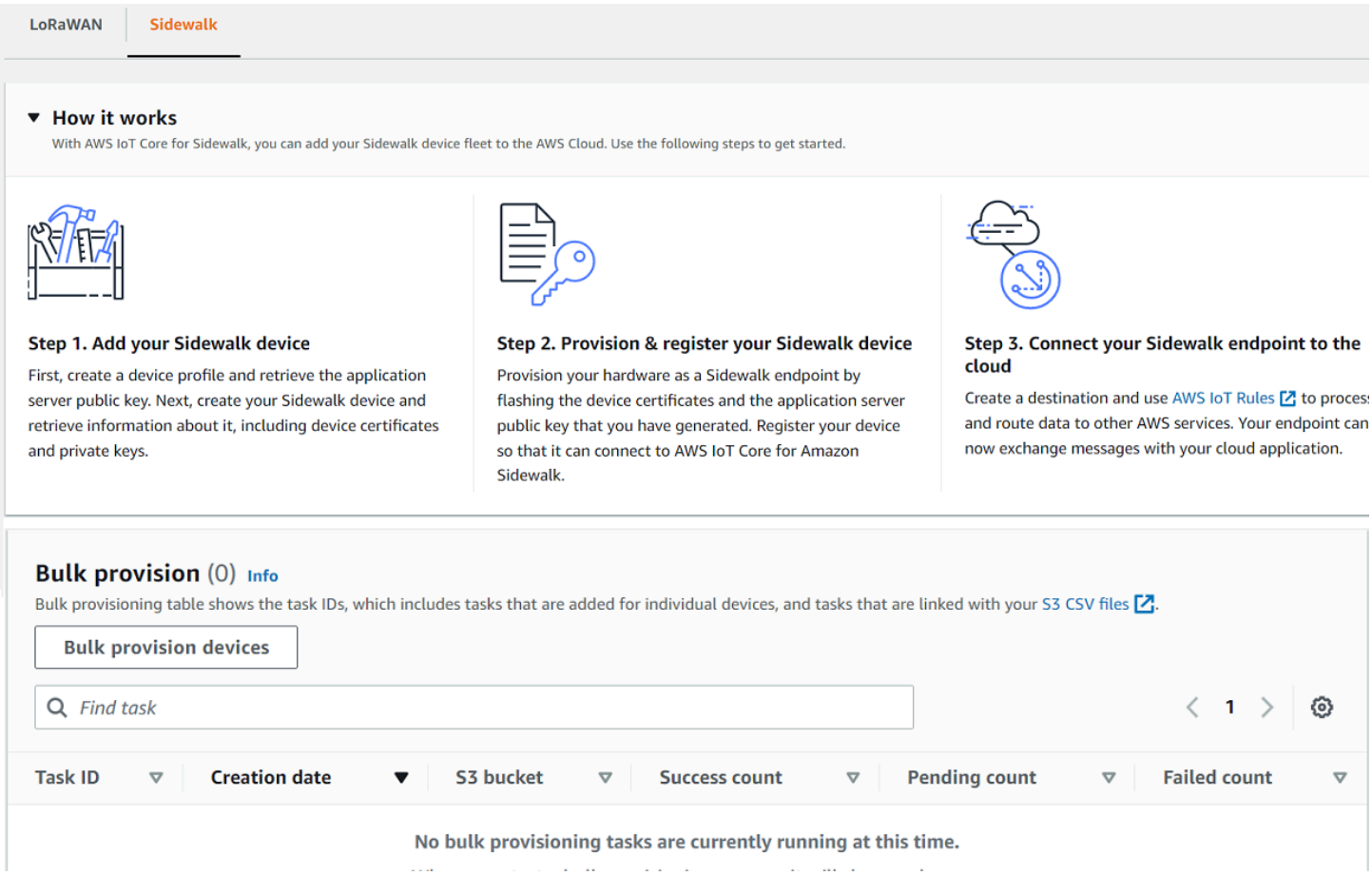
Argomenti

Provisioning in blocco di dispositivi Sidewalk

In questa sezione viene illustrato come effettuare il provisioning in blocco di dispositivi Sidewalk in AWS IoT Core per Amazon Sidewalk, utilizzando la console AWS IoT e la AWS CLI.

Provisioning in blocco di dispositivi Sidewalk (console)

Per aggiungere il dispositivo Sidewalk mediante la console AWS IoT, passa alla scheda Sidewalk dell'hub Dispositivi, scegli Dispositivi con provisioning in blocco, quindi esegui la procedura seguente.



1. Scelta del metodo di importazione

   Specifica la modalità di importazione dei dispositivi di cui eseguire l'onboarding in blocco in AWS IoT Core per Amazon Sidewalk.

   - Per effettuare il provisioning di singoli dispositivi utilizzando il relativo SMSN, scegli Effettua il provisioning di singoli dispositivi supportati in fabbrica.
   - Per effettuare il provisioning in blocco dei dispositivi fornendo un file CSV contenente un elenco di dispositivi e i relativi SMS, scegli Usa bucket S3.

2. Specifica dei dispositivi di cui eseguire l'onboarding

   A seconda del metodo scelto per eseguire l'onboarding dei dispositivi, aggiungi le informazioni sul dispositivo e i relativi numeri di serie.

   a. Se hai scelto Effettua il provisioning di singoli dispositivi supportati in fabbrica, specifica le seguenti informazioni:

i. Un Nome per ciascun dispositivo di cui eseguire l'onboarding. Il nome deve essere univoco in Account AWS e Regione AWS.

ii. Il relativo numero di serie di produzione Sidewalk (SMSN) nel campo Inserisci SMSN.

iii. Una Destinazione che descrive la regola IoT per instradare i messaggi dal dispositivo ad altri Servizi AWS.

b. Se hai scelto Usa bucket S3:

i. Fornisci le informazioni sulla Destinazione del bucket S3, costituite dalle informazioni sull'URL S3. Per fornire il file CSV, scegli Sfoglia S3, quindi seleziona il file CSV che desideri utilizzare.

AWS IoT Core per Amazon Sidewalk popola automaticamente l'URL S3, ovvero il percorso del file CSV nel bucket S3. Il formato del percorso è `s3://bucket_name/file_name`. Per visualizzare il file nella console Amazon Simple Storage Service, scegli View (Visualizza).

ii. Fornisci il ruolo S3 Provisioning, che consente ad AWS IoT Core per Amazon Sidewalk di accedere al file CSV nel bucket S3 per tuo conto. Puoi creare un nuovo ruolo di servizio o scegliere un ruolo esistente.

Per creare un nuovo ruolo, puoi fornire un Nome del ruolo o lasciare il campo vuoto per generare automaticamente un nome casuale.

iii. Fornisci una Destinazione che descrive la regola IoT per instradare i messaggi dal dispositivo ad altri Servizi AWS.

3. Avvio dell'attività di importazione

Fornisci eventuali tag opzionali come coppie nome-valore e scegli Invia per avviare l'attività di importazione dei dispositivi wireless.

Provisioning in blocco di dispositivi Sidewalk (CLI)

Per eseguire l'onboarding dei dispositivi Sidewalk nell'account per AWS IoT Core per Amazon Sidewalk, utilizza una delle seguenti operazioni API a seconda che si desideri aggiungere dispositivi singolarmente o fornendo il file CSV contenuto in un bucket S3.

- Caricamento di dispositivi in blocco utilizzando un file CSV S3

Per caricare i dispositivi in blocco fornendo il file CSV in un bucket S3, utilizza l'operazione API `StartWirelessDeviceImportTask` o il comando `start-wireless-device-import-task` AWS CLI. Durante la creazione dell'attività, specifica il percorso del file CSV nel bucket Amazon S3 e il ruolo IAM che concede ad AWS IoT Core per Amazon Sidewalk le autorizzazioni per accedere al file CSV.

Una volta avviata l'esecuzione dell'attività, AWS IoT Core per Amazon Sidewalk inizierà a leggere il file CSV e confronterà i numeri di serie (SMSN) nel file con le informazioni corrispondenti nel log di controllo ricevuto da Amazon Sidewalk. Quando i numeri di serie corrispondono, inizierà a creare record di dispositivi wireless corrispondenti a questi numeri di serie.

Il seguente comando mostra un esempio di creazione di un'attività di importazione:

```
aws iotwireless start-wireless-device-import-task \
    --cli-input-json "file://task.json"
```

Nell'esempio seguente viene mostrato il contenuto del file `task.json`.

Contenuto di task.json

```
{
    "DestinationName": "Sidewalk_Destination",
    "Sidewalk": {
        "DeviceCreationFile": "s3://import_task_bucket/import_file1",
        "Role": "arn:aws:iam::123456789012:role/service-role/ACF1zBEI"
    }
}
```

L'esecuzione di questo comando restituisce un ID e un ARN per l'attività di importazione.

```
{
    "Arn": "arn:aws:iotwireless:us-east-1:123456789012:ImportTask/a1b234c5-67ef-21a2-
a1b2-3cd4e5f6789a"
    "Id": "a1b234c5-67ef-21a2-a1b2-3cd4e5f6789a"
}
```

- Provisioning dei dispositivi singolarmente utilizzando il relativo SMSN

Per effettuare il provisioning dei dispositivi singolarmente utilizzando il relativo SMSN, utilizza l'operazione API StartSingleWirelessDeviceImportTask o il comando start-single-wireless-device-import-task AWS CLI. Durante la creazione dell'attività, specifica la destinazione Sidewalk e il numero di serie del dispositivo di cui desideri eseguire l'onboarding.

Quando il numero di serie corrisponde alle informazioni corrispondenti contenute nel log di controllo ricevuto da Amazon Sidewalk, l'attività verrà eseguita e creerà il record del dispositivo wireless.

Il seguente comando mostra un esempio di creazione di un'attività di importazione:

```
aws iotwireless start-single-wireless-device-import-task \
    --destination-name sidewalk_destination \
    --sidewalk
 '{"SidewalkManufacturingSn": "82B83C8B35E856F43CE9C3D59B418CC96B996071016DB1C3BE5901F0F3071A
```

L'esecuzione di questo comando restituisce un ID e un ARN per l'attività di importazione.

```
{
    "Arn": "arn:aws:iotwireless:us-east-1:123456789012:ImportTask/e2a5995e-743b-41f2-
a1e4-3ca6a5c5249f"
    "Id": "e2a5995e-743b-41f2-a1e4-3ca6a5c5249f"
}
```

Aggiornamento o eliminazione di attività di importazione

Se desideri aggiungere ulteriori dispositivi a un'attività di importazione, puoi aggiornare l'attività. Inoltre, puoi eliminare un'attività se non è più richiesta o se non è andata a buon fine. Per informazioni su quando aggiornare o eliminare un'attività, consultare Come utilizzare il provisioning in blocco Sidewalk.

> **Warning**
>
> Le operazioni di eliminazione sono permanenti e non possono essere annullate. L'eliminazione di un'attività di importazione già completata non rimuoverà i dispositivi finali di cui è già stato eseguito l'onboarding utilizzando l'attività.

Per aggiornare o eliminare attività di importazione:

- Utilizzo della console di AWS IoT

  Nella procedura seguente viene illustrato come aggiornare o eliminare le attività di importazione mediante la console AWS IoT.

  Per aggiornare un'attività di importazione:

  1. Passa all'hub di Dispositivi Sidewalk della console AWS IoT.
  2. Scegli l'attività di importazione che desideri aggiornare, quindi seleziona Modifica.
  3. Fornisci un altro file S3 contenente i numeri di serie dei dispositivi che desideri aggiungere all'attività, quindi scegli Invia.

  Per eliminare un'attività di importazione:

  1. Passa all'hub di Dispositivi Sidewalk della console AWS IoT.
  2. Scegli l'attività che desideri eliminare, quindi seleziona Elimina.
- Utilizzo dell'API AWS IoT Wireless o della AWS CLI

  Utilizza le seguenti operazioni API AWS IoT Wireless o i comandi dell'interfaccia a riga di comando per aggiornare o eliminare l'attività di importazione.

  - API **UpdateWirelessDeviceImportTask** o interfaccia a riga di comando **update-wireless-device-import-task**

    Questa operazione API aggiunge il contenuto di un file CSV Amazon S3 a un'attività di importazione esistente. Puoi aggiungere solo numeri di serie di dispositivi che in precedenza non erano inclusi nell'attività.
  - API **DeleteWirelessDeviceImportTask** o interfaccia a riga di comando **delete-wireless-device-import-task**

    Questa operazione API elimina l'attività di importazione contrassegnata per l'eliminazione utilizzando l'ID dell'attività di importazione.

Visualizzazione dell'attività di importazione e dello stato di onboarding dei dispositivi

Le attività di importazione dei dispositivi wireless e i dispositivi Sidewalk che sono stati aggiunti all'attività possono avere uno dei seguenti messaggi di stato. Questi messaggi verranno visualizzati

nella console AWS IoT o quando si utilizza una delle operazioni API AWS IoT Wireless o i comandi AWS CLI per recuperare informazioni su queste attività e i relativi dispositivi.

Visualizzazione delle informazioni sullo stato dell'attività di importazione

Dopo aver creato un'attività di importazione, puoi visualizzare l'attività di importazione creata e lo stato di onboarding dei dispositivi aggiunti all'attività. Lo stato di onboarding indica il numero di dispositivi in attesa di onboarding, il numero di dispositivi di cui è stato eseguito l'onboarding e il numero di dispositivi il cui onboarding non è andato a buon fine.

Quando un'attività di importazione è appena stata creata, l'opzione Conteggio in sospeso visualizzerà un valore che corrisponde al numero di dispositivi aggiunti. Quando l'attività viene avviata e il file CSV viene letto per creare i record di dispositivi wireless, il Conteggio in sospeso diminuisce e il Conteggio operazioni riuscite aumenta man mano che viene eseguito l'onboarding dei dispositivi. Se l'onboarding di un dispositivo non va a buon fine, il Conteggio non riuscito aumenta.

Per visualizzare l'attività di importazione e lo stato di onboarding dei dispositivi:

- Utilizzo della console di AWS IoT

  Nell'hub di Dispositivi Sidewalk della console AWS IoT, puoi visualizzare le attività di importazione create e un conteggio di riepilogo delle informazioni sullo stato di onboarding dei dispositivi. Se visualizzi i dettagli di una qualsiasi delle attività di importazione create, vengono mostrate informazioni aggiuntive sullo stato di onboarding dei dispositivi.
- Utilizzo dell'API AWS IoT Wireless o della AWS CLI

  Per visualizzare lo stato di onboarding dei dispositivi, utilizza una delle seguenti operazioni API AWS IoT Wireless o il comando AWS CLI corrispondente.

  - API **`ListWirelessDeviceImportTasks`** o interfaccia a riga di comando **`list-wireless-device-import-tasks`**

    Questa operazione API restituisce informazioni su tutte le attività di importazione che sono state aggiunte all'account per AWS IoT Wireless e il relativo stato. Restituisce inoltre un conteggio del riepilogo dello stato di onboarding dei dispositivi Sidewalk in queste attività.
  - API **`ListDevicesForWirelessDeviceImportTask`** o interfaccia a riga di comando **`list-devices-for-wireless-device-import-task`**

Questa operazione API restituisce informazioni sull'attività di importazione specificata e sul relativo stato e informazioni su tutti i dispositivi Sidewalk che sono stati aggiunti all'attività di importazione e le relative informazioni sullo stato di onboarding.

- API **`GetWirelessDeviceImportTask`** o interfaccia a riga di comando **`get-wireless-device-import-task`**

  Questa operazione API restituisce informazioni sull'attività di importazione specificata e sul relativo stato e un conteggio del riepilogo dello stato di onboarding dei dispositivi Sidewalk in tale attività.

Stato dell'attività di importazione

Le attività di importazione create in Account AWS possono avere uno dei seguenti messaggi di stato. Lo stato indica se l'attività di importazione ha avviato l'elaborazione, è stata completata o non è andata a buon fine. Puoi anche utilizzare la console AWS IoT o il parametro `StatusReason` di una qualsiasi delle operazioni API AWS IoT Wireless per recuperare dettagli sullo stato aggiuntivi.

- INIZIALIZZAZIONE

  AWS IoT Core per Amazon Sidewalk ha ricevuto la richiesta di attività di importazione dei dispositivi wireless e sta configurando l'attività.

- INIZIALIZZATO

  AWS IoT Core per Amazon Sidewalk ha completato la configurazione dell'attività di importazione ed è in attesa dell'arrivo del log di controllo in modo da poter importare i dispositivi utilizzando i relativi numeri di serie (SMSN) e continuare l'elaborazione dell'attività.

- PENDING

  L'operazione di importazione è in attesa in coda per essere elaborata. AWS IoT Core per Amazon Sidewalk sta valutando altre attività presenti nella coda di elaborazione.

- COMPLETA

  L'attività di importazione è stata elaborata e completata.

- Non riuscito

L'attività di importazione o l'attività del dispositivo non è riuscita. Puoi utilizzare il parametro `StatusReason` per identificare il motivo della mancata riuscita dell'attività di importazione, ad esempio un'eccezione di convalida.

- ELIMINAZIONE IN CORSO

  L'attività di importazione è stata contrassegnata per l'eliminazione ed è in fase di eliminazione.

Stato di onboarding del dispositivo

I dispositivi Sidewalk che sono stati aggiunti all'attività possono avere uno dei seguenti messaggi di stato. Lo stato indica se i dispositivi sono pronti per eseguire l'onboarding, se l'onboarding è stato effettuato o se l'onboarding non è andato a buon fine. Puoi anche utilizzare la console AWS IoT o il parametro `OnboardingStatusReason` di una qualsiasi delle operazioni API AWS IoT Wireless, `ListDevicesForWirelessDeviceImportTask`, per recuperare dettagli sullo stato aggiuntivi.

- INIZIALIZZATO

  AWS IoT Core per Amazon Sidewalk ha completato la configurazione dell'attività di importazione ed è in attesa dell'arrivo del log di controllo in modo da poter importare i dispositivi utilizzando i relativi numeri di serie (SMSN) e continuare l'elaborazione dell'attività.
- PENDING

  L'attività di importazione è in attesa in coda per essere elaborata e per avviare l'onboarding dei dispositivi nell'attività. AWS IoT Core per Amazon Sidewalk sta valutando altre attività presenti nella coda di elaborazione.
- ONBOARDING COMPLETATO

  L'onboarding del dispositivo Sidewalk è stato correttamente eseguito nell'attività di importazione.
- Non riuscito

  L'attività di importazione o l'attività del dispositivo non è andata a buon fine e l'onboarding del dispositivo Sidewalk nell'attività non è riuscito. È possibile utilizzare il parametro `OnboardingStatusReason` per recuperare ulteriori dettagli sul motivo per cui l'onboarding del dispositivo non è riuscito.

Sicurezza in Wireless AWS IoT

Per AWS, la sicurezza del cloud ha la massima priorità. In quanto cliente AWS, è possibile trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle organizzazioni più esigenti a livello di sicurezza.

La sicurezza è una responsabilità condivisa tra te e AWS. Il modello di responsabilità condivisa descrive questo modello come sicurezza del cloud e sicurezza nel cloud:

- La sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce i servizi AWS nel cloud AWS. AWS fornisce inoltre servizi che puoi utilizzare in sicurezza. Revisori di terze parti testano regolarmente e verificano l'efficacia della nostra sicurezza nell'ambito dei Programmi di conformità AWS. Per informazioni sui programmi di conformità applicabili a Wireless AWS IoT, consulta Servizi AWS coperti dal programma di compliance.
- Sicurezza nel cloud: la tua responsabilità è determinata dal servizio AWS che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa quando si utilizza Wireless AWS IoT. Illustra come configurare Wireless AWS IoT per soddisfare gli obiettivi di sicurezza e conformità. Inoltre fornisce informazioni su come utilizzare gli altri servizi AWS che consentono di monitorare e proteggere le risorse Wireless AWS IoT.

Indice

Protezione dei dati in Wireless AWS IoT

Il modello di responsabilità condivisa di AWS si applica alla protezione dei dati in Wireless AWS IoT. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale

che esegue tutto l'Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. Inoltre, sei responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS che utilizzi. Per ulteriori informazioni sulla privacy dei dati, vedi Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog AWS Shared Responsibility Model and GDPR nel Blog sulla sicurezza AWS.

Per garantire la protezione dei dati, ti suggeriamo di proteggere le credenziali Account AWS e di configurare singoli utenti con AWS IAM Identity Center o AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Utilizza SSL/TLS per comunicare con le risorse AWS. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura la registrazione di log sulle attività di API e utenti con AWS CloudTrail.
- Utilizza le soluzioni di crittografia AWS, insieme a tutti i controlli di sicurezza predefiniti in Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se necessiti di moduli crittografici convalidati FIPS 140-2 quando accedi ad AWSattraverso un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Questo vale anche nel caso in cui utilizzi Wireless AWS IoT o altri servizi Servizi AWS mediante la console, l'API, la AWS CLI o gli AWS o gli AWS SDK. I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Crittografia dei dati in AWS IoT Wireless

Per impostazione predefinita, vengono crittografati i dati in transito e a riposo AWS IoT Wireless. AWS IoT Wirelessnon supporta chiavi gestite AWS KMS dal cliente da AWS KMS key. Per crittografare i dati, AWS IoT Wireless utilizza solo un Chiave di proprietà di AWS.

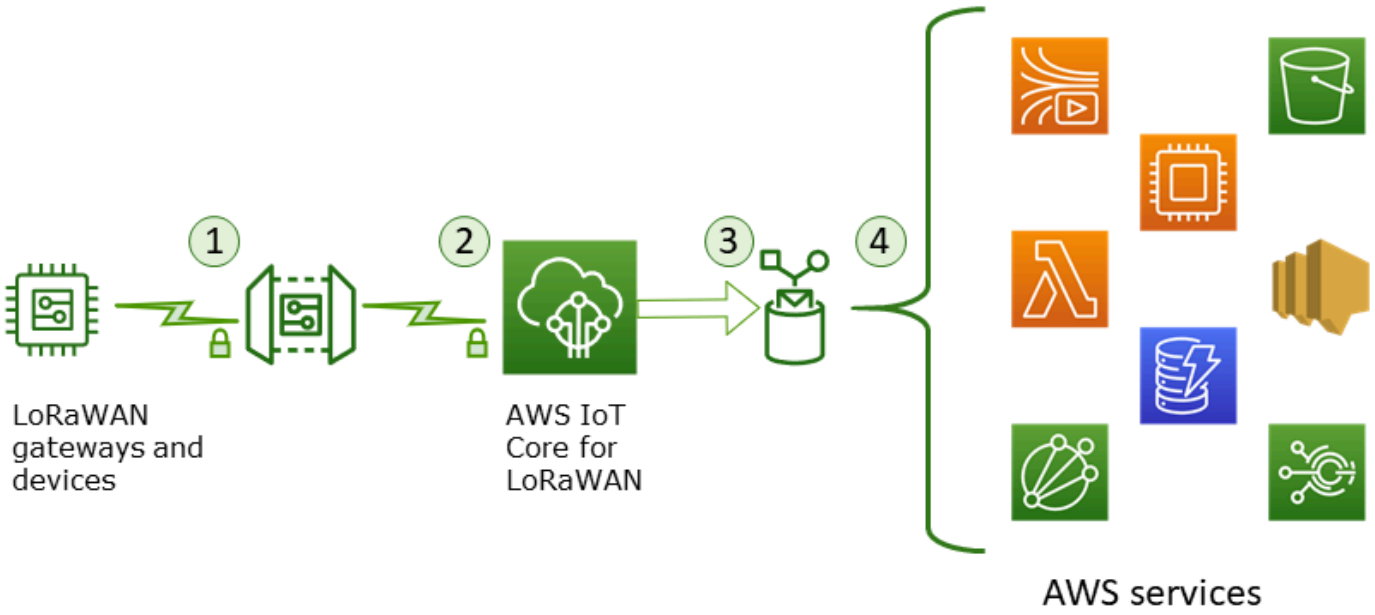
Sicurezza dei dati e del trasporto con AWS IoT Core per LoRaWAN

AWS IoT Core per LoRaWAN utilizza i seguenti metodi per proteggere i dati e le comunicazioni tra dispositivi LoRaWAN, gateway e AWS IoT Core per LoRaWAN:

- Le best practice di sicurezza seguite dai dispositivi quando comunicano con i gateway LoRaWAN, come descritto nel whitepaper LoRaWAN Security.
- La sicurezza utilizzata da AWS IoT Core per connettere i gateway ad AWS IoT Core per LoRaWAN e inviare i dati ad altri servizi AWS. Per ulteriori informazioni, consultare Protezione dati in AWS IoT Core.

Come vengono protetti i dati in tutto il sistema

Questo diagramma individua gli elementi chiave di un sistema LoRaWAN collegato ad AWS IoT Core per LoRaWAN per identificare come sono protetti i dati.



1. Il dispositivo wireless LoRaWAN crittografa i suoi messaggi binari utilizzando la modalità CTR AES128 prima di trasmetterli.
2. Connessioni gateway a AWS IoT Core per LoRaWAN sono garantite da TLS come descritto in Sicurezza del trasporto in AWS IoT. AWS IoT Core per LoRaWAN decripta il messaggio binario e codifica il payload del messaggio binario decriptato come stringa base64.

3. Il messaggio codificato in base 64 risultante viene inviato come payload del messaggio alla regola di AWS IoT descritta nella destinazione assegnata al dispositivo. I dati all'interno dei servizi AWS vengono crittografati utilizzando chiavi di proprietà AWS.
4. La regola AWS IoT indirizza i dati del messaggio ai servizi descritti nella configurazione della regola. I dati all'interno di AWS vengono crittografati utilizzando chiavi di proprietà AWS.

Sicurezza del trasporto di dispositivi e gateway LoRaWAN

Dispositivi LoRaWAN e archivio AWS IoT Core per LoRaWAN per le chiavi di root pre-condivise. Le chiavi di sessione sono derivate da entrambi i dispositivi LoRaWAN e AWS IoT Core per LoRaWAN seguendo i protocolli. Le chiavi di sessione simmetriche vengono utilizzate per la crittografia e la decrittografia in una modalità CTR standard AES-128. Un codice MIC (Message Integrity Code) a 4 byte viene utilizzato anche per controllare l'integrità dei dati seguendo un algoritmo CMAC AES-128 standard. Le chiavi di sessione possono essere aggiornate utilizzando il processo Join/Rejoin.

La pratica di sicurezza per i gateway LoRa è descritta nelle specifiche LoRaWAN. I gateway LoRa si connettono ad AWS IoT Core per LoRaWAN attraverso un socket Web utilizzando una `Basics Station`. AWS IoT Core per LoRaWAN supporta solo `Basics Station` versione 2.0.4 e successive.

Prima di stabilire la connessione web socket, AWS IoT Core per LoRaWAN utilizza la modalità di autenticazione del server e del client TLS per autenticare il gateway. Per garantire la riservatezza del protocollo LoRaWAN, si utilizza TLS versione 1.2. Il supporto TLS è disponibile in diversi linguaggi di programmazione e sistemi operativi. I dati all'interno dei servizi AWS sono crittografati dallo specifico servizio di AWS. Per ulteriori informazioni sulla crittografia dei dati su altri servizi AWS, consultare la documentazione di sicurezza per tale servizio.

AWS IoT Core per LoRaWAN gestisce anche un server di configurazione e aggiornamento (CUPS) che configura e aggiorna i certificati e le chiavi utilizzate per l'autenticazione TLS.

Identity and Access Management per Wireless AWS IoT

AWS Identity and Access Management (IAM) è un Servizio AWSche consente agli amministratori di controllare in modo sicuro l'accesso alle risorse AWS. Gli amministratori IAM controllano chi può essere autenticato (ha effettuato l'accesso) e autorizzato (dispone di autorizzazioni) a utilizzare le risorse Wireless AWS IoT. IAM è un Servizio AWS il cui uso non comporta costi aggiuntivi.

Argomenti

Destinatari

Le modalità di utilizzo di AWS Identity and Access Management (IAM) cambiano in base alle operazioni eseguite in Wireless AWS IoT.

Utente del servizio: se utilizzi il servizio Wireless AWS IoT per eseguire il tuo processo, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. All'aumentare del numero di funzionalità Wireless AWS IoT utilizzate per il lavoro, potrebbero essere necessarie ulteriori autorizzazioni. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di Wireless AWS IoT, consulta Risoluzione dei problemi relativi ad accesso e identità Wireless AWS IoT.

Amministratore del servizio: se sei il responsabile delle risorse di Wireless AWS IoT della tua azienda, probabilmente disponi dell'accesso completo a Wireless AWS IoT. Il tuo compito è determinare le caratteristiche e le risorse Wireless AWS IoT a cui gli utenti del servizio devono accedere. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM con Wireless AWS IoT, consulta Come funziona Wireless AWS IoT con IAM.

Amministratore IAM: un amministratore IAM potrebbe essere interessato a ottenere dei dettagli su come scrivere policy per gestire l'accesso a Wireless AWS IoT. Per visualizzare policy basate su identità di Wireless AWS IoT di esempio che puoi utilizzare in IAM, consulta Esempi di policy basate su identità di Wireless AWS IoT.

Autenticazione con identità

L'autenticazione è la procedura di accesso ad AWS con le credenziali di identità. Devi essere autenticato (connesso a AWS) come utente root Utente root dell'account AWS, come utente IAM o assumere un ruolo IAM.

Puoi accedere ad AWS come identità federata utilizzando le credenziali fornite attraverso un'origine di identità. Gli utenti AWS IAM Identity Center (Centro identità IAM), l'autenticazione Single Sign-On (SSO) dell'azienda e le credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Se accedi ad AWS tramite la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere alla AWS Management Console o al portale di accesso AWS. Per ulteriori informazioni sull'accesso ad AWS, consulta la sezione Come accedere al tuo Account AWS nella Guida per l'utente di Accedi ad AWS.

Se accedi ad AWS in modo programmatico, AWS fornisce un Software Development Kit (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le richieste utilizzando le tue credenziali. Se non utilizzi gli strumenti AWS, devi firmare le richieste personalmente. Per ulteriori informazioni sulla firma delle richieste, consulta Firma delle richieste AWS nella Guida per l'utente IAM.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. AWS consiglia ad esempio di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza dell'account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWS nella Guida per l'utente di IAM.

Utente root di un Account AWS

Quando crei un Account AWS, inizi con una singola identità di accesso che ha accesso completo a tutti i Servizi AWS e le risorse nell'account. Tale identità è detta utente root Account AWS ed è possibile accedervi con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzarle per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.

Utenti e gruppi IAM

Un utente IAM è una identità all'interno del tuo Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, per casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente di IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato Amministratori IAM e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente di IAM.

Ruoli IAM

> **Note**
>
> AWS IoT Wireless non supporta ruoli di servizio e ruoli collegati al servizio.

Un ruolo IAM è un'identità all'interno di un Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. È possibile assumere temporaneamente un ruolo IAM nella AWS Management Console mediante lo scambio di ruoli. È possibile assumere un ruolo chiamando un'azione AWS CLI o API AWS oppure utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente di IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per ulteriori informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center.
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, per alcuni dei Servizi AWS, è possibile collegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.
- Accesso multi-servizio: alcuni Servizi AWS utilizzano funzionalità in altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Inoltro delle sessioni di accesso (FAS): quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, tale utente o ruolo viene considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che effettua la chiamata a un Servizio AWS, combinate con il Servizio AWS richiedente, per effettuare richieste a servizi a valle. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che necessita di interazioni con altri Servizi AWS o risorse per essere portata a termine. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM assunto da un servizio per eseguire operazioni per conto dell'utente. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.

  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati ai servizi sono visualizzati nell'account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- Applicazioni in esecuzione su Amazon EC2: è possibile utilizzare un ruolo IAM per gestire credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 che eseguono richieste di AWS CLIo dell'API AWS. Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un ruolo AWS a un'istanza EC2, affinché sia disponibile per tutte le relative applicazioni, puoi creare un profilo dell'istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente di IAM.

Gestione dell'accesso con policy

Per controllare l'accesso a AWS è possibile creare policy e collegarle a identità o risorse AWS. Una policy è un oggetto in AWS che, quando associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste policy quando un principale IAM (utente, utente root o sessione ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle policy viene archiviata in AWSsotto forma di documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWSJSON per specificare l'accesso ai diversi elementi. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'azione

`iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dalla AWS Management Console, la AWS CLI o l'API AWS.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono incorporate direttamente in un singolo utente, gruppo o ruolo. Le policy gestite sono policy autonome che possono essere collegate a più utenti, gruppi e ruoli in Account AWS. Le policy gestite includono le policy gestite da AWS e le policy gestite dal cliente. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente di IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o Servizi AWS.

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy gestite da AWS da IAM in una policy basata su risorse.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3, AWS WAF e Amazon VPC sono esempi di servizi che supportano le ACL. Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta altri tipi di policy meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Policy di controllo dei servizi (SCP): le SCP sono policy JSON che specificano il numero massimo di autorizzazioni per un'organizzazione o unità organizzativa (OU) in AWS Organizations. AWS Organizationsè un servizio per il raggruppamento e la gestione centralizzata degli Account AWSmultipli di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. La SCP limita le autorizzazioni per le entità negli account membri, compreso ogni Utente root dell'account AWS. Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations.
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente di IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella Guida per l'utente di IAM.

Come funziona Wireless AWS IoT con IAM

Prima di utilizzare l'IAM per gestire l'accesso a Wireless AWS IoT, è necessario comprendere quali caratteristiche IAM sono disponibili per l'uso con Wireless AWS IoT. Per ottenere un quadro generale del funzionamento di Wireless AWS IoT e altri servizi AWS con IAM, consulta AWS Services That Work with IAM nella Guida per l'utente IAM.

Funzionalità IAM che è possibile utilizzare con AWS IoT Wireless

Funzionalità IAM	Supporto di AWS IoT Wireless
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì
Liste di controllo degli accessi (ACL)	No
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
☻Ruoli di servizio	No
Ruoli collegati al servizio	No

Argomenti

- Policy basate su identità di Wireless AWS IoT
- Policy basate su risorse all'interno di AWS IoT Wireless
- Operazioni di policy
- Risorse di policy
- Chiavi di condizione

- Liste di controllo degli accessi (ACL)
- ABAC con AWS IoT Wireless
- Utilizzo di credenziali temporanee con AWS IoT Wireless
- Autorizzazioni del principale tra servizi per AWS IoT Wireless
- Ruoli di servizio
- Ruoli collegati ai servizi per l'AWS IoT Wireless

Policy basate su identità di Wireless AWS IoT

Supporta le policy basate su identità	Sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Esempi

Per visualizzare esempi di policy basate su identità di Wireless AWS IoT, consulta Esempi di policy basate su identità di Wireless AWS IoT.

Policy basate su risorse all'interno di AWS IoT Wireless

Supporta le policy basate su risorse	No

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy

dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o Servizi AWS.

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando l'entità principale e la risorsa si trovano in diversi Account AWS, un amministratore IAM nell'account attendibile deve concedere all'entità principale (utente o ruolo) anche l'autorizzazione per accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Operazioni di policy

Supporta le azioni di policy	Sì

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a una policy. Le azioni di policy hanno spesso lo stesso nome dell'operazione API AWS. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Le operazioni delle policy in Wireless AWS IoT utilizzano il seguente prefisso prima dell'operazione: `iotwireless:`. Ad esempio, per concedere a qualcuno l'autorizzazione a elencare tutti gli oggetti IoT registrati nel proprio account Account AWS con l'API `ListWirelessDevices`, puoi includere l'operazione `iotwireless:ListWirelessDevices` nella relativa policy. Le istruzioni della policy devono includere un elemento `Action` o `NotAction`. Wireless AWS IoT definisce un proprio insieme di operazioni che descrivono le attività che puoi eseguire con quel servizio.

Per specificare più operazioni in una sola istruzione, separa ciascuna di esse con una virgola come mostrato di seguito:

```
"Action": [
      "iotwireless:ListMulticastGroups",
      "iotwireless:ListFuotaTasks"
   ]
```

È possibile specificare più operazioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le operazioni che iniziano con la parola `Get`, includi la seguente operazione:

```
"Action": "iotwireless:Get*"
```

Per un elenco di operazioni di Wireless AWS IoT, consulta Operazioni definite da Wireless AWS IoT nella Guida per l'utente di IAM.

Risorse di policy

Supporta le risorse di policy	Sì

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'azione. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Il servizio AWS IoT Wireless dispone del seguente ARN:

```
arn:${Partition}:iotwireless:${Region}:${Account}:${Resource}/${Resource-id}
```

Per ulteriori informazioni sul formato degli ARN, consulta Nome della risorsa Amazon (ARN) e spazi dei nomi del servizio AWS.

Ad esempio, per specificare la configurazione dell'analizzatore di rete `NAConfig1` nell'istruzione, utilizza il seguente ARN:

```
"Resource": "arn:aws:iotwireless:us-east-1:123456789012:NetworkAnalyzerConfiguration/
NAConfig1"
```

Per specificare tutte le attività FUOTA che appartengono a un account specifico, utilizza il carattere jolly (*):

```
"Resource": "arn:aws:iotwireless:us-east-1:123456789012:FuotaTask/*"
```

Alcune operazioni Wireless AWS IoT, ad esempio quelle per la creazione di risorse, non possono essere eseguite su una determinata risorsa. In questi casi, è necessario utilizzare il carattere jolly (*).

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

Molte operazioni API di AWS IoT Wireless coinvolgono più risorse. Ad esempio, `AssociateWirelessDeviceWithThing` associa un dispositivo wireless a un oggetto AWS IoT, quindi un utente IAM deve disporre delle autorizzazioni per utilizzare il dispositivo e un oggetto IoT. Per specificare più risorse in una singola istruzione, separa gli ARN con le virgole.

```
"Resource": [
      "WirelessDevice",
      "thing"
```

Per un elenco dei tipi di risorsa di Wireless AWS IoT e dei rispettivi ARN, consulta Resources Defined by AWS IoT Wireless nella Guida per l'utente di IAM. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta Operazioni definite da AWS IoT Wireless.

Chiavi di condizione

Supporta le chiavi di condizione delle policy specifiche del servizio	Sì

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND` logica. Se specifichi più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione `OR` logica. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche per il servizio. Per visualizzare tutte le chiavi di condizione globali di AWS, consulta Chiavi di contesto delle condizioni globali di AWS nella Guida per l'utente di IAM.

Wireless AWS IoT definisce il proprio set di chiavi di condizione e, inoltre, supporta l'uso di alcune chiavi di condizione globali. Per visualizzare tutte le chiavi di condizione globali di AWS, consulta Chiavi di contesto delle condizioni globali di AWS nella Guida per l'utente IAM. Per visualizzare un elenco delle chiavi di condizione di Wireless AWS IoT, consulta Chiavi di condizione per AWS IoT Wireless nella Guida per l'utente di IAM. Per informazioni su operazioni e risorse con cui è possibile utilizzare una chiave di condizione, consulta Operazioni definite da AWS IoT Wireless.

Liste di controllo degli accessi (ACL)

Supporta le ACL	No

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni ad accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con AWS IoT Wireless

Supporta ABAC (tag nelle policy)	Sì

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, tali attributi sono denominati tag. È possibile collegare dei tag alle entità IAM (utenti o ruoli) e a numerose risorse AWS. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Che cos'è ABAC? nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

È possibile associare tag alle risorse di Wireless AWS IoT o passare tag in una richiesta a Wireless AWS IoT. Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `YOUR-SERVICE-PREFIX:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`. Per ulteriori informazioni sul tagging delle risorse Wireless AWS IoT, consulta Tagging delle risorse AWS IoT Wireless.

Utilizzo di credenziali temporanee con AWS IoT Wireless

Supporta le credenziali temporanee	Sì

Alcuni Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, inclusi i Servizi AWS che funzionano con le credenziali temporanee, consulta Servizi AWS supportati da IAM nella Guida per l'utente IAM.

Le credenziali temporanee sono utilizzate se si accede alla AWS Management Console utilizzando qualsiasi metodo che non sia la combinazione di nome utente e password. Ad esempio, quando accedi ad AWS utilizzando il collegamento Single Sign-On (SSO) della tua azienda, tale processo crea in automatico credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente di IAM.

È possibile creare manualmente credenziali temporanee utilizzando la AWS CLIo l'API AWS. È quindi possibile utilizzare tali credenziali temporanee per accedere ad AWS. AWSconsiglia di generare le credenziali temporanee dinamicamente anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Autorizzazioni del principale tra servizi per AWS IoT Wireless

Supporta sessioni di accesso diretto (FAS)	Sì

Quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, si viene considerati un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'azione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che effettua la chiamata a un Servizio AWS, combinate con il Servizio AWS richiedente, per effettuare richieste a servizi a valle. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che necessita di interazioni con altri Servizi AWS o risorse per essere portata a termine. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.

Ruoli di servizio

Supporta i ruoli di servizio	No

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per

ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.

Ruoli collegati ai servizi per l'AWS IoT Wireless

Supporta i ruoli collegati ai servizi	No

Un ruolo collegato ai servizi è un tipo di ruolo di servizio che è collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati ai servizi sono visualizzati nell'account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Esempi di policy basate su identità di Wireless AWS IoT

Per impostazione predefinita, gli utenti e i ruoli IAM non dispongono dell'autorizzazione per creare o modificare risorse Wireless AWS IoT. Inoltre, non sono in grado di eseguire attività utilizzando la AWS Management Console, AWS CLI o un'API AWS. Un amministratore IAM deve creare policy IAM che concedono a utenti e ruoli l'autorizzazione per eseguire operazioni API specifiche sulle risorse specificate di cui hanno bisogno. L'amministratore deve quindi allegare queste policy a utenti o IAM che richiedono tali autorizzazioni.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy nella scheda JSON nella Guida per l'utente IAM.

Argomenti

- Best practice delle policy
- Utilizzo della console Wireless AWS IoT
- Consentire agli utenti di visualizzare le loro autorizzazioni
- Autorizzazioni necessarie per eseguire azioni sui dispositivi wireless AWS IoT Wireless

Best practice delle policy

Le policy basate su identità determinano se qualcuno può creare, accedere o eliminare risorse Wireless AWS IoT nel tuo account. Queste operazioni possono comportare costi aggiuntivi per

l'Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Nozioni di base sulle policy gestite da AWSe passaggio alle autorizzazioni con privilegio minimo: per le informazioni di base su come concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy gestite da AWSche concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo Account AWS. Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente di AWSspecifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi inoltre utilizzare le condizioni per concedere l'accesso alle operazioni di servizio, ma solo se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente di IAM.
- Richiesta dell'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o utenti root nel tuo Account AWS, attiva MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console Wireless AWS IoT

Per accedere alla console Wireless AWS IoT, è necessario disporre di un set di autorizzazioni minimo. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli relativi alle risorse Wireless AWS IoT nell'account AWS. Se crei una policy basata su identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti e ruoli IAM) associate a tale policy.

Per garantire che tali entità possano ancora utilizzare la console Wireless AWS IoT, collega anche la seguente policy gestita da AWS alle entità. Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente di IAM:

```
AWSIoTWirelessFullAccess
```

Non sono necessarie le autorizzazioni minime della console per gli utenti che effettuano chiamate solo alla AWS CLIo all'API AWS. Al contrario, puoi accedere solo alle operazioni che soddisfano l'operazione API che stai cercando di eseguire.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono allegate alla relativa identità utente. La policy include le autorizzazioni per completare questa azione sulla console o a livello di programmazione utilizzando la AWS CLIo l'API AWS.

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

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

Autorizzazioni necessarie per eseguire azioni sui dispositivi wireless AWS IoT Wireless

Puoi utilizzare le condizioni nella policy basata sulle identità per controllare l'accesso alle azioni Wireless AWS IoT. Questo esempio mostra come creare una policy che consenta la creazione e la gestione dei dispositivi. Tuttavia, l'autorizzazione viene concessa solo se il valore del tag dell'oggetto `0wner` corrisponde a quello del nome utente. Questa policy concede anche le autorizzazioni necessarie per completare questa azione nella console.

```
{
 "Version": "2012-10-17",
 "Statement": [{
    "Sid": "VisualEditor0",
    "Effect": "Allow",
    "Action": [
              "iotwireless:CreateWirelessDevice",
              "iotwireless:GetWirelessDevice",
              "iotwireless:ListWirelessDevices",
              "iotwireless:UpdateWirelessDevice",
              "iotwireless:DeleteWirelessDevice"
           ],
    "Resource": "*"
    }
 ]
}
```

La policy contiene una dichiarazione che concede l'autorizzazione all'uso delle azioni `CreateWirelessDevice`, `GetWirelessDevice`, `ListWirelessDevices`, `UpdateWirelessDevice`, e `DeleteWirelessDevice`. AWS IoT Wireless chiama questi metodi per creare e gestire i dispositivi wireless.

La policy non specifica l'elemento Principale poiché in una policy basata su identità non si specifica il principale che ottiene l'autorizzazione. Quando alleghi una policy a un utente, l'utente è il principale implicito. Quando colleghi una policy di autorizzazioni a un ruolo IAM, il principale identificato nella policy di attendibilità del ruolo ottiene le autorizzazioni.

Policy gestite da AWS per AWS IoT Wireless

Per aggiungere le autorizzazioni a utenti, gruppi e ruoli, è più semplice utilizzare policy gestite da AWS piuttosto che scrivere le policy in autonomia. La creazione di policy gestite dai clienti IAM che forniscono al tuo team solo le autorizzazioni di cui ha bisogno richiede tempo e competenza. Per iniziare rapidamente, utilizza le nostre policy gestite da AWS. Queste policy coprono i casi d'uso comuni e sono disponibili nel tuo Account AWS. Per ulteriori informazioni sulle policy gestite da AWS, consulta Policy gestite da AWS nella Guida per l'utente di IAM.

I servizi AWS mantengono e aggiornano le policy gestite da AWS. Non è possibile modificare le autorizzazioni nelle policy gestite da AWS. I servizi occasionalmente aggiungono altre autorizzazioni a una policy gestita da AWS per supportare nuove funzionalità. Questo tipo di aggiornamento interessa tutte le identità (utenti, gruppi e ruoli) a cui è collegata la policy. È più probabile che i servizi aggiornino una policy gestita da AWS quando viene avviata una nuova funzionalità o quando diventano disponibili nuove operazioni. I servizi non rimuovono le autorizzazioni da una policy gestita da AWS, pertanto gli aggiornamenti delle policy non interrompono le autorizzazioni esistenti.

Inoltre, AWS supporta policy gestite per le funzioni di processi che coprono più servizi. Ad esempio, la policy gestita da AWS ReadOnlyAccess fornisce accesso in sola lettura a tutti i servizi e le risorse AWS. Quando un servizio avvia una nuova funzionalità, AWS aggiunge autorizzazioni di sola lettura per nuove operazioni e risorse. Per l'elenco e la descrizione delle policy di funzione dei processi, consulta la sezione Policy gestite da AWS per funzioni di processi nella Guida per l'utente di IAM.

Policy gestita da AWS: AWSIoTWirelessDataAccess

È possibile allegare la policy `AWSIoTWirelessDataAccess`alle identità IAM.

Questa policy concede all'identità associata le autorizzazioni per l'accesso per inviare dati ai dispositivi LoRaWAN e Sidewalk usando l'API `SendDataToWirelessDevice`. Per visualizzare questa policy nella AWS Management Console, consulta AWSIoTWirelessDataAccess.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `iotwireless` – Recupera dati AWS IoT Wireless.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iotwireless:SendDataToWirelessDevice"
            ],
            "Resource": "*"
        }
    ]
}
```

Policy gestita da AWS: AWSIoTWirelessFullAccess

È possibile allegare la policy `AWSIoTWirelessFullAccess`alle identità IAM.

Questa policy concede all'identità associata le autorizzazioni per l'accesso a tutte le operazioni AWS IoT Wireless. Per visualizzare questa policy nella AWS Management Console, consulta AWSIoTWirelessFullAccess.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `iotwireless` – Recupera i dati AWS IoT Wireless ed esegui tutte le operazioni AWS IoT Wireless.

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

Policy gestita da AWS: AWSIoTWirelessFullPublishAccess

È possibile allegare la policy `AWSIoTWirelessFullPublishAccess`alle identità IAM.

Questa policy concede all'identità associata le autorizzazioni per l'accesso limitato per pubblicare sulle regole AWS IoT per conto dell'utente. Per visualizzare questa policy nella AWS Management Console, consulta `AWSIoTWirelessFullPublishAccess`.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `iot` – Esegui operazioni per ottenere l'URL dell'endpoint e pubblicarlo nel motore delle regole AWS IoT.

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

Policy gestita da AWS: AWSIoTWirelessLogging

È possibile allegare la policy `AWSIoTWirelessLogging`alle identità IAM.

Questa policy concede all'identità associata le autorizzazioni per l'accesso per creare gruppi di file di log Amazon CloudWatch e trasmettere i registri ai gruppi. Questa policy è collegata al ruolo di logging di CloudWatch. Per visualizzare questa policy nella AWS Management Console, consulta `AWSIoTWirelessLogging`.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `logs`: recupera registri CloudWatch. Permette anche la creazione di gruppi di file di log CloudWatch e registri di streaming nei gruppi.

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

Policy gestita da AWS: AWSIoTWirelessReadOnlyAccess

È possibile allegare la policy `AWSIoTLogging`alle identità IAM.

Questa policy concede all'identità associata le autorizzazioni per l'accesso in sola lettura alle operazioni AWS IoT Wireless. Per visualizzare questa policy nella AWS Management Console, consulta `AWSIoTWirelessReadOnlyAccess`.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `logs` – Esegui operazioni API AWS IoT Wireless `List` e `Get`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iotwireless:List*",
                "iotwireless:Get*"
```

```
            ],
            "Resource": "*"
        }
    ]
}
```

Policy gestita da AWS: AWSIoTWirelessGatewayCertManager

È possibile allegare la policy `AWSIoTWirelessGatewayCertManager`alle identità IAM.

Questa policy concede all'identità associata l'autorizzazione per creare, elencare e descrivere i certificati AWS IoT. Per visualizzare questa policy nella AWS Management Console, consulta `AWSIoTWirelessGatewayCertManager.`

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `iot` – Esegui azioni per creare, descrivere ed elencare i certificati.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IoTWirelessGatewayCertManager",
            "Effect": "Allow",
            "Action": [
                "iot:CreateKeysAndCertificate",
                "iot:DescribeCertificate",
                "iot:ListCertificates"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS IoT Wireless; aggiornamenti alle policy gestite da AWS

Visualizza i dettagli sugli aggiornamenti alle policy gestite da AWS per AWS IoT Wireless da quando questo servizio ha iniziato a tenere traccia delle modifiche. Per gli avvisi automatici sulle modifiche apportate a questa pagina, sottoscrivi il feed RSS nella pagina della cronologia dei documenti AWS IoT Wireless.

Modifica	Descrizione	Data
AWS IoT Wireless ha iniziato il rilevamento delle modifiche	AWS IoT Wireless ha iniziato il rilevamento delle modifiche per le relative policy gestite da AWS.	18 maggio 2022

Risoluzione dei problemi relativi ad accesso e identità Wireless AWS IoT

Usa le informazioni seguenti per diagnosticare e risolvere i problemi comuni che possono verificarsi durante l'utilizzo di Wireless AWS IoT.

Argomenti

- Non dispongo dell'autorizzazione a eseguire un'operazione in Wireless AWS IoT
- Desidero visualizzare le mie chiavi di accesso
- Sono un amministratore e desidero consentire ad altri utenti di accedere a Wireless AWS IoT
- Voglio consentire alle persone esterne al mio account AWS di accedere alle mie risorse Wireless AWS IoT

Non dispongo dell'autorizzazione a eseguire un'operazione in Wireless AWS IoT

Se la AWS Management Console indica che non hai l'autorizzazione a eseguire un'operazione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è la persona da cui si sono ricevuti il nome utente e la password.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` cerca di utilizzare la console per visualizzare i dettagli relativi a un *`WirelessDevice`* ma non dispone di autorizzazioni `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
```

In questo caso, Mateo richiede al suo amministratore di aggiornare le policy per poter accedere alla risorsa *my-LoRaWAN-device* utilizzando l'operazione `YOUR-SERVICE-PREFIX:GetWirelessDevice`.

Desidero visualizzare le mie chiavi di accesso

Dopo aver creato le chiavi di accesso utente IAM, è possibile visualizzare il proprio ID chiave di accesso in qualsiasi momento. Tuttavia, non è possibile visualizzare nuovamente la chiave di accesso segreta. Se perdi la chiave segreta, dovrai creare una nuova coppia di chiavi di accesso.

Le chiavi di accesso sono composte da due parti: un ID chiave di accesso (ad esempio `AKIAIOSFODNN7EXAMPLE`) e una chiave di accesso segreta (ad esempio, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Come un nome utente e una password, è necessario utilizzare sia l'ID chiave di accesso sia la chiave di accesso segreta insieme per autenticare le richieste dell'utente. Gestisci le tue chiavi di accesso in modo sicuro mentre crei il nome utente e la password.

> **Important**
>
> Non fornire le chiavi di accesso a terze parti, neppure per aiutare a trovare l'ID utente canonico. Se lo facessi, daresti a qualcuno accesso permanente al tuo Account AWS.

Quando crei una coppia di chiavi di accesso, ti viene chiesto di salvare l'ID chiave di accesso e la chiave di accesso segreta in una posizione sicura. La chiave di accesso segreta è disponibile solo al momento della creazione. Se si perde la chiave di accesso segreta, è necessario aggiungere nuove chiavi di accesso all'utente IAM. È possibile avere massimo due chiavi di accesso. Se se ne hanno già due, è necessario eliminare una coppia di chiavi prima di crearne una nuova. Per visualizzare le istruzioni, consulta Gestione delle chiavi di accesso nella Guida per l'utente di IAM.

Sono un amministratore e desidero consentire ad altri utenti di accedere a Wireless AWS IoT

Per consentire ad altri utenti di accedere a Wireless AWS IoT, devi creare un'entità IAM (utente o ruolo) per la persona o l'applicazione che richiede l'accesso. Tale utente o applicazione utilizzerà le credenziali dell'entità per accedere ad AWS. Dovrai quindi collegare all'entità una policy che conceda le autorizzazioni corrette in Wireless AWS IoT.

Per iniziare immediatamente, consulta Creazione dei primi utenti e gruppi delegati IAM nella Guida per l'utente di IAM.

Voglio consentire alle persone esterne al mio account AWS di accedere alle mie risorse Wireless AWS IoT

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per capire se Wireless AWS IoT supporta queste funzionalità, consulta Come funziona Wireless AWS IoT con IAM.
- Per informazioni su come garantire l'accesso alle risorse negli Account AWSche possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS in tuo possesso nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso alle risorse ad Account AWS di terze parti, consulta Fornire l'accesso agli Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consultare Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Convalida della conformità per Wireless AWS IoT

Revisori di terze parti valutano la sicurezza e la conformità di Wireless AWS IoT come parte di più programmi di conformità di AWS. Questi includono SOC, PCI, FedRAMP, HIPAA e altri.

Per un elenco dei servizi AWS coperti da programmi di conformità specifici, consulta Servizi AWS coperti dal programma di compliance. Per informazioni generali, consulta Programmi di conformità AWS.

È possibile scaricare i report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Download di report in AWS Artifact.

La responsabilità di conformità durante l'utilizzo di Wireless AWS IoT è determinata dalla riservatezza dei dati, dagli obiettivi di conformità dell'azienda e dalle normative vigenti. Per semplificare il rispetto della conformità, AWS mette a disposizione le seguenti risorse:

- Security and Compliance Quick Start Guides (Guide Quick Start Sicurezza e compliance) (Guide Quick Start Sicurezza e compliance): queste guide alla distribuzione illustrano considerazioni relative all'architettura e forniscono procedure per la distribuzione di ambienti di base incentrati sulla sicurezza e sulla conformità su AWS.
- Whitepaper sulla progettazione per la sicurezza HIPAA e la conformità: questo whitepaper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni conformi ai requisiti HIPAA.
- Risorse per la conformità AWS: una raccolta di cartelle di lavoro e guide suddivise per settore e area geografica.
- Valutazione delle risorse con le regole nella Guida per gli sviluppatori di AWS Config: AWS Config valuta il livello di conformità delle configurazioni delle risorse con pratiche interne, linee guida e regolamenti industriali.
- AWS Security Hub: Questo servizio AWS fornisce una visione completa dello stato di sicurezza all'interno di AWS che consente di verificare la conformità con gli standard e le best practice di sicurezza del settore.

Resilienza in Wireless AWS IoT

L'infrastruttura globale di AWS è basata su regioni AWS e zone di disponibilità. Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, connesse tramite reti altamente ridondanti, a bassa latenza e throughput elevato. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni su Regioni e zone di disponibilità AWS, consulta Infrastruttura globale di AWS.

Sicurezza dell'infrastruttura in Wireless AWS IoT

In qualità di servizio gestito, Wireless AWS IoT è protetto dalle procedure di sicurezza di rete globali AWS descritte nel whitepaper Amazon Web Services: panoramica dei processi di sicurezza.

Utilizza le chiamate all'API pubblicate da AWS per accedere a Wireless AWS IoT tramite la rete. I client devono supportare Transport Layer Security (TLS) 1.0 o versioni successive. È consigliabile TLS 1.2 o versioni successive. I client devono, inoltre, supportare le suite di cifratura con PFS (Perfect Forward Secrecy), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate tramite un ID chiave di accesso e una chiave di accesso segreta associata a un principal IAM. In alternativa, è possibile utilizzare AWS Security Token Service (AWS STS) per generare le credenziali di sicurezza temporanee per firmare le richieste.

Monitoraggio delle risorse AWS IoT Wireless con i file di log Amazon CloudWatch

Il monitoraggio è importante per garantire l'affidabilità, la disponibilità e le prestazioni di Wireless AWS IoT e delle altre soluzioni AWS. Puoi utilizzare il monitoraggio sia per i tuoi dispositivi LoRaWAN che Sidewalk e ottenere messaggi informativi ed errori sin dal momento dell'onboarding in AWS IoT Wireless.

Si consiglia di raccogliere i dati di monitoraggio da tutte le parti della soluzione AWS per semplificare il debug di un errore multipunto, nel caso in cui se ne verifichi uno. Iniziare creando un piano di monitoraggio che risponda alle seguenti domande. Se non si è sicuri di come rispondere, è comunque possibile continuare ad abilitare la registrazione e stabilire le baseline delle prestazioni.

- Quali sono gli obiettivi del monitoraggio?
- Quali risorse verranno monitorate?
- Con quale frequenza eseguirai il monitoraggio di queste risorse?
- Quali strumenti di monitoraggio verranno usati?
- Chi eseguirà i processi di monitoraggio?
- Chi deve ricevere una notifica quando si verifica un problema?

La fase successiva consiste nell'abilitare la registrazione o nello stabilire una baseline per le prestazioni normali di Wireless AWS IoT nell'ambiente, misurando le prestazioni in diversi momenti e con condizioni di carico differenti. Mentre si effettua il monitoraggio di Wireless AWS IoT, mantieni i dati cronologici di monitoraggio in modo da poterli confrontare con i dati delle prestazioni correnti. Questo permette di identificare i normali modelli di prestazioni e le anomalie di prestazioni e definire metodi per risolvere i problemi.

Strumenti di monitoraggio

AWS fornisce gli strumenti di monitoraggio seguenti per tenere sotto controllo Wireless AWS IoT, segnalare un problema e intervenire automaticamente quando necessario:

- Amazon CloudWatch monitora le risorse AWS e le applicazioni che esegui su AWS in tempo reale. Puoi raccogliere i parametri e tenerne traccia, creare pannelli di controllo personalizzati e impostare allarmi per inviare una notifica o intraprendere azioni quando un parametro specificato raggiunge

una determinata soglia. Ad esempio, puoi impostare CloudWatch perché tenga traccia dell'uso della CPU o di altri parametri delle tue istanze Amazon EC2 e avviare automaticamente nuove istanze quando necessario. Per ulteriori informazioni, consultare la Guida per l'utente di Amazon CloudWatch.

- L'analizzatore di rete ti consente di monitorare le tue risorse LoRaWAN, che includono dispositivi e gateway LoRaWAN, riduce il tempo necessario per configurare una connessione per iniziare a ricevere messaggi di traccia, fornendo informazioni di log just-in-time. Per ulteriori informazioni, consultare Monitoraggio del parco istanze di risorse wireless in tempo reale utilizzando l'analizzatore di rete.

Come monitorare le risorse utilizzando Amazon CloudWatch

Puoi monitorare Wireless AWS IoT utilizzando Amazon CloudWatch, che raccoglie i dati non elaborati e li elabora trasformandoli in parametri leggibili quasi in tempo reale. Queste statistiche vengono conservate per un periodo di 15 mesi, per permettere l'accesso alle informazioni storiche e offrire una prospettiva migliore sulle prestazioni del servizio o dell'applicazione Web. È anche possibile impostare allarmi che controllano determinate soglie e inviare notifiche o intraprendere azioni quando queste soglie vengono raggiunte. Per ulteriori informazioni, consultare la Guida per l'utente di Amazon CloudWatch.

Per registrare e monitorare le risorse AWS IoT Wireless, attieniti alla procedura descritta di seguito:

1. Crea un ruolo di registrazione per registrare le tue risorse AWS IoT Wireless, come descritto in Creare un ruolo di registrazione e una policy per AWS IoT Wireless.
2. I messaggi di log nella console CloudWatch Logs hanno un livello di log predefinito di `ERROR`, che è meno dettagliato e contiene solo informazioni sugli errori. Se desideri visualizzare messaggi più dettagliati, è consigliabile utilizzare la CLI per configurare prima la registrazione, come descritto in Configurazione della registrazione per risorse AWS IoT Wireless.
3. Successivamente, è possibile monitorare le risorse visualizzando le voci di registro nella console CloudWatch Logs. Per ulteriori informazioni, consultare Visualizza voci di registro AWS IoT Wireless CloudWatch.
4. È possibile creare espressioni di filtro utilizzando Gruppi di log ma è consigliabile innanzitutto creare filtri semplici e visualizzare le voci di registro nei gruppi di log, quindi passare a CloudWatch Insights per creare query per filtrare le voci del registro in base alla risorsa o all'evento che si sta monitorando. Per ulteriori informazioni, consultare Usa CloudWatch Insights per filtrare i log per AWS IoT Wireless.

Configurazione della registrazione per AWS IoT Wireless

Prima di poter monitorare e registrare l'attività di AWS IoT, abilita prima la registrazione per le risorse AWS IoT Wireless utilizzando la CLI o l'API.

Quando si considera come configurare la registrazione AWS IoT Wireless, la configurazione di registrazione di default determina la modalità di registrazione dell'attività AWS IoT se non diversamente specificato. Per iniziare, è possibile ottenere log dettagliati con un livello di log predefinito di `INFO`.

Dopo aver esaminato i registri iniziali, è possibile modificare il livello di log predefinito su `ERROR`, un livello meno dettagliato e impostare un livello di log più dettagliato specifico delle risorse per le risorse che potrebbero richiedere maggiore attenzione. I livelli di log possono essere modificati ogni volta che vuoi.

I seguenti argomenti mostrano come configurare la registrazione per le risorse AWS IoT Wireless.

Argomenti

Creare un ruolo di registrazione e una policy per AWS IoT Wireless

Di seguito viene illustrato come creare un ruolo di registrazione solo per le risorse AWS IoT Wireless. Se desideri creare anche un ruolo di registrazione per AWS IoT Core, consulta https://docs.aws.amazon.com/iot/latest/developerguide/create-logging-role.html.

Creazione di un ruolo di registrazione per AWS IoT Wireless

Prima di poter abilitare la registrazione, è necessario creare un ruolo IAM e una policy che conceda ad AWS l'autorizzazione per monitorare l'attività AWS IoT Wireless per conto dell'utente.

Creazione di ruolo IAM per la registrazione

Per creare un ruolo di registrazione per AWS IoT Wireless, apri l'Hub ruoli della console IAM e scegli Crea ruolo.

1. In Seleziona tipo di entità attendibile, scegli Un altro account AWS.

2. In Account ID (ID account), inserisci il tuo account AWS ID, quindi scegli Next: Permissions (Successivo: Autorizzazioni).
3. Nella casella di ricerca immetti **`AWSIoTWirelessLogging`**.
4. Seleziona la casella accanto alla policy denominata AWSIoTWirelessLogging e quindi Next: Tags (Successivo: Tag).
5. Seleziona Successivo: Revisione.
6. In Role name (Nome ruolo) immetti **`IoTWirelessLogsRole`** e quindi seleziona Create role (Crea ruolo).

Modifica la relazione di fiducia per il ruolo IAM

Nel messaggio di conferma visualizzato dopo avere eseguito il passaggio precedente, scegli il nome del ruolo creato, IoTWirelessLogsRole. Successivamente, modificherai il ruolo per aggiungere la seguente relazione di attendibilità.

1. Nella sezione del ruolo Summary (Riepilogo) IoTWirelessLogsRole, scegli l'opzione Trust relationships (Relazioni di trust), quindi scegli Edit trust relationship (Modifica relazione di trust).
2. In Policy Document (Documento policy), modifica la proprietà `Principal` affinché appaia come il seguente.

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

   Dopo aver modificato la proprietà `Principal`, il documento completo di policy dovrebbe essere simile al seguente.

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

```
  ]
}
```

3. Per salvare le modifiche, scegli Update Trust Policy (Aggiorna policy di attendibilità).

Policy di registrazione per AWS IoT Wireless

Nei documenti seguenti relativi alle policy sono contenute la policy del ruolo e la policy di trust che permettono ad AWS IoT Wireless di inviare le voci di registro a CloudWatch per conto dell'utente.

> **Note**
>
> Il documento di policy AWS gestito è stato creato automaticamente al momento della creazione del ruolo di registrazione, IoTWirelessLogsRole.

Policy del ruolo

Di seguito viene mostrato il documento della policy di ruolo.

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

Policy di trust solo per registrare le attività di AWS IoT Wireless

Di seguito viene illustrata la policy di trust solo per la registrazione all'attività AWS IoT Wireless.

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

Se è stato creato il ruolo IAM per registrare anche nell'attività di AWS IoT Core, i documenti di policy consentono di registrare entrambe le attività. Per informazioni su come creare un ruolo di registrazione per AWS IoT Core, consulta https://docs.aws.amazon.com/iot/latest/developerguide/create-logging-role.html.

Passaggi successivi

L'utente ha imparato a creare un ruolo di registrazione per registrare le tue risorse AWS IoT Wireless. Per impostazione predefinita, i log hanno un livello di `ERROR`, quindi se desideri visualizzare solo le informazioni di errore, vai su Visualizza voci di registro AWS IoT Wireless CloudWatch per monitorare le risorse wireless visualizzando le voci di log.

Per ulteriori informazioni sulle voci di log, è possibile configurare il livello di log predefinito per le risorse o per i diversi tipi di eventi, ad esempio impostando il livello di log su `INFO`. Per informazioni sulla configurazione della registrazione per le risorse, consulta Configurazione della registrazione per risorse AWS IoT Wireless.

Configurazione della registrazione per risorse AWS IoT Wireless

Per configurare la registrazione per le risorse AWS IoT Wireless, puoi utilizzare l'API o la CLI. Quando inizi a monitorare le risorse AWS IoT Wireless, puoi utilizzare la configurazione di default. A tale scopo, puoi saltare questo argomento e procedere a Monitoraggio di AWS IoT Wireless tramite CloudWatch Logs per monitorare i log.

Dopo aver avviato il monitoraggio dei log, è possibile utilizzare l'interfaccia della riga di comando per modificare i livelli di log in un'opzione più dettagliata, ad esempio fornendo `INFO` e informazioni sul livello `ERROR` e abilitare la registrazione per ulteriori risorse.

Risorse AWS IoT Wireless e livelli di registro

Prima di utilizzare l'API o l'interfaccia della riga di comando, utilizza la tabella seguente per informazioni sui diversi livelli di log e sulle risorse per cui è possibile configurare la registrazione. La tabella mostra i parametri visualizzati nei registri di CloudWatch quando si monitorano le risorse. La modalità di configurazione della registrazione per le risorse determinerà i log visualizzati nella console.

Per informazioni sull'aspetto di un esempio di registro CloudWatch e su come è possibile utilizzare questi parametri per registrare informazioni utili sulle risorse AWS IoT Wireless, consulta Visualizza voci di registro AWS IoT Wireless CloudWatch.

Livelli di registro e risorse

Nome	Valori possibili	Descrizione
`logLevel`	`INFO`, `ERROR` o `DISABLED`	• `ERROR`: mostra qualsiasi errore che provoca la mancata riuscita di un'operazione. I log includono solo informazioni per il livello `ERROR`. • `INFO`: fornisce informazioni di alto livello sul flusso di oggetti. I log includono informazioni per i livelli `INFO` e `ERROR`. • `DISABLED`: disabilita ogni registrazione.
`resource`	`WirelessGateway` o `WirelessDevice`	Il tipo di risorsa, che può essere `WirelessGateway` o `WirelessDevice` .
`wirelessGatewayType`	`LoRaWAN`	Il tipo di gateway wireless, quando `resource` è `WirelessGateway` , che è sempre LoRaWAN.
`wirelessDeviceType`	`LoRaWAN` o `Sidewalk`	Il tipo di dispositivo wireless, quando `resource` è `WirelessDevice` , che può essere `LoRaWAN` o `Sidewalk`.

Nome	Valori possibili	Descrizione
`wirelessGatewayId`	-	L'identificatore del gateway wireless, quando `resource` è `WirelessGateway` .
`wirelessDeviceId`	-	L'identificatore del dispositivo wireless, quando `resource` è `WirelessDevice` .
`event`	`Join`, `Rejoin`, `Registration` , `Uplink_data` , `Downlink_data` , `CUPS_Request` e `Certificate`	Il tipo di evento registrato, che dipende dal fatto che la risorsa che stai registrando sia un dispositivo wireless o un gateway wireless. Per ulteriori informazioni, consultare Visualizza voci di registro AWS IoT Wireless CloudWatch.

API di registrazione AWS IoT Wireless

Per configurare la registrazione di controllo, puoi usare le operazioni API seguenti. Nella tabella viene inoltre illustrata una policy IAM di esempio che è necessario creare per l'utilizzo delle operazioni API. Nella sezione seguente viene descritto come utilizzare le API per configurare i livelli di log delle risorse.

Registrazione di operazioni API

Nome API	Descrizione	Policy IAM di esempio
GetLogLevelsByResourceTypes	Restituisce i livelli di log predefiniti correnti o i livelli di log in base ai tipi di risorse, che possono includere opzioni di log per dispositivi wireless o gateway wireless.	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "iotwireless:GetLogLevelsByResourceTypes"`

Nome API	Descrizione	Policy IAM di esempio
		], "Resource": ["*"] }] }

GetResourceLogLevel	Restituisce l'override a livello di log per un determinato identificatore di risorsa e tipo di risorsa. La risorsa può essere un dispositivo wireless o un gateway wireless.	{
		"Version":
		"2012-10-17",
		"Statement": [
		
		{
		"Effect":
		"Allow",
		"Action": [
		
		"iotwireless:GetRe
		sourceLogLevel"
		
		],
		
		"Resource":
		[
		
		"arn:aws:iotwirele
		ss:us-east-1:12345
		6789012:WirelessDe
		vice/012bc537-ab12
		-cd3a-d00e-1f0e20c
		1204a",
		]
		}
		]
		}

Nome API	Descrizione	Policy IAM di esempio
PutResourceLogLevel	Imposta l'override a livello di log per un determinato identificatore di risorsa e tipo di risorsa. La risorsa può essere un gateway wireless o un dispositivo wireless. **Note** Questa API ha un limite di 200 sostituzioni a livello di registro per account.	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "iotwireless:PutResourceLogLevel" ], "Resource": [ "arn:aws:iotwireless:us-east-1:123456789012:WirelessDevice/012bc537-ab12-cd3a-d00e-1f0e20c1204a", ] } ] }`

Nome API	Descrizione	Policy IAM di esempio
ResetAllResourceLogLevels	Rimuove le sostituzioni a livello di log per tutte le risorse che includono sia gateway wireless che dispositivi wireless. **Note** Questa API non influisce sui livelli di log impostati utilizzando l'opzione API `UpdateLogLevelsByResourceTypes` .	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "iotwireless:ResetAllResourceLogLevels" ], "Resource": [ "arn:aws:iotwireless:us-east-1:123456789012:WirelessDevice/*", "arn:aws:iotwireless:us-east-1:123456789012:WirelessGateway/* ] } ] }`

Nome API	Descrizione	Policy IAM di esempio
ResetResourceLogLevel	Rimuove l'override a livello di log per un determinato identificatore di risorsa e tipo di risorsa. La risorsa può essere un gateway wireless o un dispositivo wireless.	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "iotwireless:ResetResourceLogLevel" ], "Resource": [ "arn:aws:iotwireless:us-east-1:123456789012:WirelessDevice/012bc537-ab12-cd3a-d00e-1f0e20c1204a", ] } ] }`

Nome API	Descrizione	Policy IAM di esempio
UpdateLogLevelsByResourceTypes	Imposta il livello di log predefinito o i livelli di log in base ai tipi di risorse. È possibile utilizzare questa API per le opzioni di log per dispositivi wireless o gateway wireless e controllare i messaggi di log che verranno visualizzati in CloudWatch. **Note** Gli eventi sono facoltativi e il tipo di evento è associato al tipo di risorsa. Per ulteriori informazioni, consultare Eventi e tipi di risorse.	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "iotwireless:UpdateLogLevelsByResourceTypes" ], "Resource": [ "*" ] } ] }`

Configurare i livelli di log delle risorse utilizzando la CLI

In questa sezione viene descritto come configurare i livelli di registro per le risorse AWS IoT Wireless utilizzando l'API o la AWS CLI.

Prima di utilizzare la CLI:

- Assicurati di aver creato la policy IAM per l'API per cui desideri eseguire il comando CLI, come descritto in precedenza.
- Hai bisogno dell'Amazon Resource Name (ARN) del ruolo che desideri utilizzare. Se è necessario creare un ruolo da utilizzare per la registrazione, consulta Creare un ruolo di registrazione e una policy per AWS IoT Wireless.

Perché usare AWS CLI

Per impostazione predefinita, se crei il ruolo IAM, `IoTWirelessLogsRole`, come descritto in Creare un ruolo di registrazione e una policy per AWS IoT Wireless, vedrai i log di CloudWatch nella AWS Management Console che hanno un livello di log predefinito di `ERROR`. Per modificare il livello di registro di default per tutte le risorse o per risorse specifiche, utilizza l'API di registrazione wireless AWS IoT Wireless o CLI.

Come utilizzare AWS CLI

Le operazioni API possono essere classificate nei seguenti tipi a seconda che si desideri configurare i livelli di log per tutte le risorse o per risorse specifiche:

- Le operazioni dell'API `GetLogLevelsByResourceTypes` e `UpdateLogLevelsByResourceTypes` possono recuperare e aggiornare i livelli di log per tutte le risorse del tuo account che sono di un tipo specifico, ad esempio un gateway wireless, o un dispositivo LoRaWAN o Sidewalk.
- Le operazioni dell'API `GetResourceLogLevel`, `PutResourceLogLevel`, e `ResetResourceLogLevel` possono recuperare, aggiornare e reimpostare i livelli di log delle singole risorse specificate utilizzando un identificatore di risorsa.
- L'operazione API `ResetAllResourceLogLevels` reimposta l'override a livello di log su `null` per tutte le risorse per le quali è stato specificato un override a livello di log utilizzando l'API `PutResourceLogLevel`.

Per utilizzare l'interfaccia a riga di comando per configurare la registrazione specifica delle risorse per AWS IoT

> **Note**
>
> È inoltre possibile eseguire questa procedura con l'API utilizzando i metodi dell'API AWS corrispondenti ai comandi CLI illustrati di seguito.

1. Per impostazione predefinita, tutte le risorse hanno il livello di log impostato su `ERROR`. Per impostare i livelli di log predefiniti o i livelli di log in base ai tipi di risorse per tutte le risorse dell'account, utilizza il comando update-log-levels-by-resource-types. L'esempio seguente mostra come puoi creare un file JSON, `Input.json`, e fornirlo come input per il comando CLI.

È possibile utilizzare questo comando per disabilitare selettivamente la registrazione o ignorare il livello di log predefinito per tipi specifici di risorse ed eventi.

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

dove:

WirelessDeviceLogOptions

Elenco delle opzioni di log per un dispositivo wireless. Ogni opzione di log include il tipo di dispositivo wireless (Sidewalk o LoRaWAN) e un elenco di opzioni di log eventi del dispositivo wireless. Ogni opzione di log eventi del dispositivo wireless può includere facoltativamente il tipo di evento e il relativo livello di log.

WirelessGatewayLogOptions

Elenco delle opzioni di log per un gateway wireless. Ogni opzione di log include il tipo di gateway wireless (LoRaWAN) e un elenco di opzioni di log eventi del gateway wireless. Ogni opzione di log eventi del gateway wireless può includere facoltativamente il tipo di evento e il relativo livello di log.

DefaultLogLevel

Livello di log da utilizzare per tutte le risorse. I valori validi sono`ERROR`, `INFO` e `DISABLED`. Il valore predefinito è `INFO`.

LogLevel

Livello di log che si desidera utilizzare per i singoli tipi di risorse ed eventi. Questi livelli di log sovrascrivono il livello di log predefinito, ad esempio il livello di log `INFO` per il gateway LoRaWAN e i livelli di log `DISABLED` e `ERROR` per i due tipi di evento.

Nel comando di esempio seguente viene utilizzato un file di input `Input.json` per fornire il codice della funzione al comando. Il comando non produce output.

```
aws iotwireless update-log-levels-by-resource-types \
```

```
    --cli-input-json Input.json
```

Se desideri rimuovere le opzioni di log sia per i dispositivi wireless che per i gateway wireless, esegui il comando seguente.

```
{
    "DefaultLogLevel":"DISABLED",
    "WirelessDeviceLogOptions": [],
    "WireslessGatewayLogOptions":[]
}
```

2. Il comando update-log-levels-by-resource-types non restituisce alcun output. Utilizza il comando get-log-levels-by-resource-types per recuperare le informazioni di registrazione specifiche delle risorse. Il comando restituisce il livello di log predefinito e le opzioni di log del dispositivo wireless e del gateway wireless.

> **Note**
>
> Il comando get-log-levels-by-resource-types non è in grado di recuperare direttamente i livelli di log nella console CloudWatch. Puoi utilizzare il comando get-log-levels-by-resource-types per ottenere le informazioni più recenti a livello di log specificate per le risorse utilizzando il comando update-log-levels-by-resource-types.

```
aws iotwireless get-log-levels-by-resource-types
```

Quando si esegue il comando seguente, restituisce le informazioni di registrazione più recenti specificate con update-log-levels-by-resource-types. Ad esempio, se rimuovi le opzioni di log dei dispositivi wireless, get-log-levels-by-resource-types restituirà questo valore come `null`.

```
{
    "DefaultLogLevel": "INFO",
    "WirelessDeviceLogOptions": null,
     "WirelessGatewayLogOptions":
      [
        {
         "Type": "LoRaWAN",
         "LogLevel": "INFO",
         "Events":
```

```
          [
            {
             "Event": "CUPS_Request",
             "LogLevel": "DISABLED"
            },
            {
              "Event": "Certificate",
              "LogLevel": "ERROR"
            }
          ]
        }
      ]
}
```

3. Per controllare i livelli di log per singoli gateway wireless o risorse di dispositivi wireless, utilizza i seguenti comandi CLI:

   - put-resource-log-level
   - get-resource-log-level
   - reset-resource-log-level

   Per un esempio su quando utilizzare questi CLI, supponi di disporre di un numero elevato di dispositivi wireless o gateway che vengono registrati nell'account. Se desideri risolvere gli errori solo per alcuni dispositivi wireless, puoi disabilitare la registrazione per tutti i dispositivi wireless impostando `DefaultLogLevel` su `DISABLED` e utilizzando put-resource-log-level per impostare il `LogLevel` su `ERROR`, solo per i dispositivi nel tuo account.

   ```
   aws iotwireless put-resource-log-level \
       --resource-identifier
       --resource-type WirelessDevice
       --log-level ERROR
   ```

   In questo esempio, il comando imposta il livello di log su `ERROR` solo per la risorsa del dispositivo wireless specificata mentre i log per tutte le altre risorse sono disabilitati. Il comando non produce output. Per recuperare queste informazioni e verificare che i livelli di log siano stati impostati, utilizza il comando get-resource-log-level.

4. Nel passaggio precedente, dopo aver eseguito il debug del problema e risolto l'errore, puoi eseguire il comando reset-resource-log-level per reimpostare il livello di log per tale risorsa su `null`. Se hai usato il comando `put-resource-log-level` per impostare l'override a livello

di log per più dispositivi wireless o risorse gateway, ad esempio per la risoluzione dei problemi relativi a più dispositivi, puoi ripristinare le sostituzioni a livello di log su `null` per tutte quelle risorse che usano il comando reset-all-resource-log-levels.

```
aws iotwireless reset-all-resource-log-levels
```

Il comando non produce output. Per recuperare le informazioni di registrazione per le risorse, esegui il comando get-resource-log-level.

Fasi successive

Hai appreso come creare il ruolo di registrazione e utilizzare l'API AWS IoT Wireless wireless per configurare la registrazione per le tue risorse AWS IoT Core per LoRaWAN. Successivamente, per ulteriori informazioni sul monitoraggio delle voci di log, vai a Monitoraggio di AWS IoT Wireless tramite CloudWatch Logs.

Monitoraggio di AWS IoT Wireless tramite CloudWatch Logs

AWS IoT Core per LoRaWANha più di 50 voci di registro CloudWatch abilitate per impostazione predefinita. Ogni voce di log descrive il tipo di evento, il livello di log e il tipo di risorsa. Per ulteriori informazioni, consultare Risorse AWS IoT Wireless e livelli di registro.

Come monitorare le tue risorse AWS IoT Wireless

Quando la registrazione è abilitata per AWS IoT Wireless, AWS IoT Wireless invia eventi di stato per ogni messaggio poiché passa dai dispositivi attraverso AWS IoT e ritorno. Per impostazione predefinita, le voci di registro AWS IoT Wireless hanno un livello di errore di default. Quando si abilita la registrazione come descritto in Creare un ruolo di registrazione e una policy per AWS IoT Wireless, nella console CloudWatch verranno visualizzati messaggi con un livello di log predefinito di `ERROR`. Utilizzando questo livello di log, i messaggi visualizzeranno solo le informazioni di errore per tutti i dispositivi wireless e le risorse del gateway in uso.

Se desideri che i registri visualizzino informazioni aggiuntive, ad esempio quelle che dispongono di un livello di registro di `INFO` o desideri disabilitare i registri per alcuni dispositivi e mostrare i messaggi di registro solo per alcuni dispositivi, puoi usare l'API di registrazione AWS IoT Wireless. Per ulteriori informazioni, consultare Configurare i livelli di log delle risorse utilizzando la CLI.

È inoltre possibile creare espressioni di filtro per visualizzare solo i messaggi richiesti.

Prima di poter visualizzare i registri AWS IoT Wireless nella console

Per rendere il gruppo di log /aws/iotwireless visibile nella console CloudWatch, è necessario effettuare le seguenti operazioni.

- Registrazione abilitata in AWS IoT Wireless. Per ulteriori informazioni su come abilitare la registrazione in AWS IoT Wireless, consulta Configurazione della registrazione per AWS IoT Wireless.
- Alcune voci di registro sono state scritte eseguendo le operazioni AWS IoT Wireless.

Per creare e utilizzare espressioni di filtro in modo più efficace, ti consigliamo di provare a utilizzare CloudWatch Insights come descritto nei seguenti argomenti. Ti consigliamo inoltre di seguire gli argomenti nell'ordine in cui sono presentati qui. Questo ti aiuterà a usare CloudWatch Gruppi di log per conoscere i diversi tipi di risorse, i relativi tipi di eventi e i livelli di log che è possibile utilizzare per visualizzare le voci di log nella console. Puoi quindi imparare come creare espressioni di filtro utilizzando CloudWatch Insights per ottenere informazioni più utili dalle tue risorse.

Argomenti

- Visualizza voci di registro AWS IoT Wireless CloudWatch
- Usa CloudWatch Insights per filtrare i log per AWS IoT Wireless

Visualizza voci di registro AWS IoT Wireless CloudWatch

Dopo aver configurato la registrazione per AWS IoT Wireless come descritto in Creare un ruolo di registrazione e una policy per AWS IoT Wireless e aver scritto alcune voci di log, è possibile visualizzare le voci di log nella console CloudWatch eseguendo il seguente passaggio.

Visualizzazione dei log AWS IoT nella console dei gruppi CloudWatch Log

Nella Console CloudWatch, i log CloudWatch vengono visualizzati in un gruppo di log chiamato /aws/iotwireless. Per ulteriori informazioni su CloudWatch Logs, consulta la CloudWatch Log.

Per visualizzare i log AWS IoT, apri la console CloudWatch

Passa alla Console CloudWatch e scegli Log groups (Gruppi di log) nel pannello di navigazione.

1. Nella casella di testo Filter (Filtro), immetti **`/aws/iotwireless`** e seleziona la casella di controllo `/aws/iotwireless` Gruppo di log.

2. Per un elenco completo dei registri AWS IoT Core per LoRaWAN generati per il tuo account, scegli Cerca tutto. Scegli l'icona di espansione per esaminare un singolo flusso di log.
3. Per filtrare i gruppi di log, è possibile anche immettere una query nella casella di testo Filter events (Filtra eventi). Di seguito sono illustrate alcune query da provare:

   - `{ $.logLevel = "ERROR" }`

     Usa questo filtro per trovare tutti i log con livello `ERROR`. Puoi espandere i singoli flussi di errore per leggere i messaggi di errore, che ti aiuteranno a risolverli.
   - `{ $.resource = "WirelessGateway" }`

     Trova tutti i log per la risorsa `WirelessGateway`, indipendentemente dal livello di log.
   - `{ $.event = "CUPS_Request" && $.logLevel = "ERROR" }`

     Trova tutti i log con un tipo di evento `CUPS_Request` e un livello di log `ERROR`.

Eventi e tipi di risorse

Nella tabella seguente vengono illustrati i diversi tipi di eventi per i quali verranno visualizzate le voci di log. I tipi di eventi dipendono anche dal fatto che il tipo di risorsa sia un dispositivo wireless o un gateway wireless. È possibile utilizzare il livello di log predefinito per le risorse e i tipi di evento oppure sovrascrivere il livello di log predefinito specificando un livello di log per ciascuno di essi.

Tipi di eventi basati sulle risorse utilizzate

Risorsa	Tipo di risorsa	Tipo di evento	
Gateway wireless	LoRaWAN	• CUPS_request • Certificato	
Dispositivo wireless	LoRaWAN	• Join • Rejoin • Uplink_Data • Downlink_Data	
Dispositivo wireless	Sidewalk	• Registration (Registrazione) • Uplink_Data	

Risorsa	Tipo di risorsa	Tipo di evento	
		• Downlink_Data	

L'argomento seguente contiene ulteriori informazioni su questi tipi di eventi e sulle voci di log per gateway wireless e dispositivi wireless.

Argomenti

- Voci di registro per gateway wireless e risorse di dispositivi wireless

Voci di registro per gateway wireless e risorse di dispositivi wireless

Dopo aver abilitato la registrazione, è possibile visualizzare le voci di log per i gateway wireless e i dispositivi wireless. Nella sezione seguente vengono descritti i vari tipi di voci di log in base ai tipi di risorsa e di evento.

Voci di registro del gateway wireless

In questa sezione vengono illustrate alcune voci di log di esempio per le risorse del gateway wireless visualizzate nella sezione CloudWatch console (Console CloudWatch). Questi messaggi di registro possono avere tipo di evento come `CUPS_Request` o `Certificate` che può essere configurato per visualizzare un livello di log di `INFO`, `ERROR`, oppure `DISABLED` a livello di risorsa o a livello di evento. Se desideri visualizzare solo le informazioni di errore, imposta il livello di log su `ERROR`. Il messaggio `ERROR` nella voce di log conterrà informazioni sul motivo per cui non è riuscito.

Le voci di log per la risorsa del gateway wireless possono essere classificate in base ai seguenti tipi di evento:

- CUPS_request

  LoRa Basics Station in esecuzione sul gateway invia periodicamente una richiesta al server di configurazione e aggiornamento (CUPS) per gli aggiornamenti. Per questo tipo di evento, se imposti il livello di log su `INFO` durante la configurazione dell'interfaccia della riga di comando per la risorsa del gateway wireless, quindi nei log:

  - Se l'evento viene completato correttamente, vengono visualizzati i messaggi di log con un `logLevel` di `INFO`. I messaggi includeranno dettagli sulla risposta CUPS inviata al gateway e i dettagli del gateway. Nell'esempio seguente viene mostrata una voce di log. Per ulteriori

informazioni su `logLevel` e altri campi nella voce di log, consulta Risorse AWS IoT Wireless e livelli di registro.

```
{
    "timestamp": "2021-05-13T16:56:08.853Z",
    "resource": "WirelessGateway",
    "wirelessGatewayId": "5da85cc8-3361-4c79-8be3-3360fb87abda",
    "wirelessGatewayType": "LoRaWAN",
    "gatewayEui": "fefffff00000000e2",
    "event": "CUPS_Request",
    "logLevel": "INFO",
    "message": "Sending CUPS response of total length 3213 to GatewayEui:
 fefffff00000000e2 with  TC Credentials,"
}
```

- Se si verifica un errore, verranno visualizzate le voci di log con un `logLevel` di `ERROR` e i messaggi includeranno dettagli sull'errore. Gli esempi di quando si può verificare un errore per l'evento `CUPS_Request` includono: CUPS CRC mancante, mancata corrispondenza nel TC Uri del gateway con AWS IoT Core per LoRaWAN, `IoTWirelessGatewayCertManagerRole` mancante o non in grado di ottenere il registro del gateway wireless. Nell'esempio seguente viene mostrata una voce di log CRC mancante. Per risolvere l'errore, controlla la configurazione del gateway per verificare di aver inserito il CRC CUPS corretto.

```
{
    "timestamp": "2021-05-13T16:56:08.853Z",
    "resource": "WirelessGateway",
    "wirelessGatewayId": "5da85cc8-3361-4c79-8be3-3360fb87abda",
    "wirelessGatewayType": "LoRaWAN",
    "gatewayEui": "fefffff00000000e2",
    "event": "CUPS_Request",
    "logLevel": "ERROR",
    "message": "The CUPS CRC is missing from the request. Check your gateway setup
 and enter the CUPS CRC,"
}
```

- Certificato

  Queste voci di log consentono di verificare se il gateway wireless ha presentato il certificato corretto per l'autenticazione della connessione a AWS IoT. Per questo tipo di evento, se imposti il livello di log su `INFO` durante la configurazione dell'interfaccia della riga di comando per la risorsa del gateway wireless, nei log:

- Se l'evento viene completato correttamente, vengono visualizzati i messaggi di log con un `logLevel` di `INFO`. I messaggi includeranno dettagli sull'ID certificato e sull'identificatore del gateway wireless. Nell'esempio seguente viene mostrata una voce di log. Per ulteriori informazioni su `logLevel` e altri campi nella voce di log, consulta Risorse AWS IoT Wireless e livelli di registro.

```
{
    "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)"
}
```

- Se si verifica un errore, verranno visualizzate le voci di log con un `logLevel` di `ERROR` e i messaggi includeranno dettagli sull'errore. Esempi di quando si può imbattere in un errore `Certificate` per l'evento includono un ID certificato non valido, un identificatore del gateway wireless o una mancata corrispondenza tra l'identificatore del gateway wireless e l'ID del certificato. L'esempio a seguire mostra un `ERROR` dovuto a un identificatore di gateway wireless non valido. Per risolvere il problema, controlla gli identificatori del 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)"
}
```

Voci di registro dei dispositivi wireless

Questa sezione mostra alcune delle voci di log di esempio per le risorse del dispositivo wireless che vedrai nella sezione CloudWatch console (Console CloudWatch). Il tipo di evento per questi messaggi di registro dipende dal fatto che si stia utilizzando un dispositivo LoRaWAN o un dispositivo Sidewalk. Ogni risorsa o tipo di evento del dispositivo wireless può essere configurato per visualizzare un livello di log di `INFO`, `ERROR` oppure `DISABLED`.

> **Note**
>
> La tua richiesta non deve contenere contemporaneamente metadati wireless LoRaWAN e Sidewalk. Per evitare una voce di log `ERROR` per questo scenario, specifica i dati wireless LoRaWAN o Sidewalk.

Voci di registro del dispositivo LoRaWAN

Le voci di log per il dispositivo wireless LoRaWAN possono essere classificate in base ai seguenti tipi di eventi:

- **`Join`** e **`Rejoin`**

  Quando aggiungi un dispositivo LoRaWAN e lo connetti ad AWS IoT Core per LoRaWAN, prima che il dispositivo possa inviare dati uplink, è necessario completare un processo chiamato `activation` o `join procedure`. Per ulteriori informazioni, consultare Aggiungi il dispositivo wireless ad AWS IoT Core per LoRaWAN.

  Per questo tipo di evento, se imposti il livello di log su `INFO` durante la configurazione dell'interfaccia della riga di comando per la risorsa del gateway wireless, nei log:

  - Se l'evento viene completato correttamente, vengono visualizzati i messaggi di log con un `logLevel` di `INFO`. I messaggi includeranno dettagli sullo stato della tua richiesta di join o rejoin. Di seguito viene mostrata una voce di log. Per ulteriori informazioni su `logLevel` e altri campi nella voce di log, consulta Risorse AWS IoT Wireless e livelli di registro.

    ```
    {
        "timestamp": "2021-05-13T16:56:08.853Z",
        "resource": "WirelessDevice",
        "wirelessDeviceType": "LoRaWAN",
        "WirelessDeviceId": "5da85cc8-3361-4c79-8be3-3360fb87abda",
    ```

```
    "devEui": "fefffff00000000e2",
    "event": "Rejoin",
    "logLevel": "INFO",
    "message": "Rejoin succeeded"
}
```

- Se si verifica un errore, verranno visualizzate le voci di log con un `logLevel` di `ERROR` e i messaggi includeranno dettagli sull'errore. Esempi di quando si può imbattere in un errore per `Join` e `Rejoin` includono l'impostazione della regione LoRaWAN non valida o il controllo MIC (Message Integrity Code) non valido. L'esempio seguente mostra un errore di join a causa del controllo MIC. Per risolvere l'errore, verifica se sono state immesse le chiavi root corrette.

```
{
    "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

  Il tipo di evento `Uplink_Data` viene utilizzato per i messaggi generati da AWS IoT Wireless quando il carico utile viene inviato dal dispositivo LoRaWAN o Sidewalk ad AWS IoT. Il tipo di evento `Downlink_Data` viene utilizzato per i messaggi correlati ai messaggi downlink inviati da AWS IoT al dispositivo wireless.

  Per questo tipo di evento, se imposti il livello di log su `INFO` durante la configurazione dell'interfaccia della riga di comando per i dispositivi wireless, nei registri verrà visualizzato:

  - Se l'evento viene completato correttamente, vengono visualizzati i messaggi di log con un `logLevel` di `INFO`. I messaggi includeranno dettagli sullo stato del messaggio di uplink o downlink inviato e sull'identificatore del dispositivo wireless. Di seguito viene illustrato un esempio di questa voce di log per un dispositivo Sidewalk. Per ulteriori informazioni su `logLevel` e altri campi nella voce di log, consulta Risorse AWS IoT Wireless e livelli di registro.

```
{
    "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\"}"
}
```

- Se si verifica un errore, verranno visualizzate le voci di log con un `logLevel` di `ERROR` e i messaggi includeranno dettagli sull'errore, che ti aiuteranno a risolverlo. Esempi di quando si può imbattere in un errore `Registration` per l'evento includono: problemi di autenticazione, richieste non valide o troppe, impossibile crittografare o decrittare il payload o impossibile trovare il dispositivo wireless utilizzando l'ID specificato. L'esempio seguente mostra un errore di autorizzazione riscontrato durante l'elaborazione di un messaggio.

```
{
    "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"
}
```

Voci dei log di dispositivo Sidewalk

Le voci di log per il dispositivo Sidewalk possono essere classificate in base ai seguenti tipi di eventi:

- **`Registration`**

  Queste voci di registro ti aiuteranno a monitorare lo stato di tutti i dispositivi Sidewalk che stai registrando con AWS IoT Wireless. Per questo tipo di evento, se si imposta il livello di log su `INFO` durante la configurazione dell'interfaccia della riga di comando per la risorsa del dispositivo wireless, nei log verranno visualizzati i messaggi di log con un `logLevel` di `INFO` e `ERROR`.

I messaggi includeranno dettagli sullo stato di avanzamento della registrazione dall'inizio al completamento. I messaggi di log `ERROR` conterranno informazioni su come risolvere i problemi relativi alla registrazione del dispositivo.

Di seguito viene illustrato un esempio per un messaggio di log con livello di log di `INFO`. Per ulteriori informazioni su `logLevel` e altri campi nella voce di log, consulta Risorse AWS IoT Wireless e livelli di registro.

```
{
    "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

  I tipi di eventi `Uplink_Data` e `Downlink_Data` per i dispositivi Sidewalk sono simili ai tipi di eventi corrispondenti per i dispositivi LoRaWAN. Per ulteriori informazioni, consulta la sezione Uplink_Data e Downlink_Data descritta in precedenza per le voci di log dei dispositivi LoRaWAN.

Passaggi successivi

Hai appreso come visualizzare le voci di registro per le risorse e le diverse voci di registro che è possibile visualizzare nella console CloudWatch dopo aver abilitato la registrazione per AWS IoT Wireless. Anche se è possibile creare flussi di filtro utilizzando Gruppi di log, ti consigliamo di utilizzare CloudWatch Insights per creare e utilizzare flussi di filtri. Per ulteriori informazioni, consultare Usa CloudWatch Insights per filtrare i log per AWS IoT Wireless.

Usa CloudWatch Insights per filtrare i log per AWS IoT Wireless

Sebbene sia possibile utilizzare CloudWatch Logs per creare espressioni di filtro, si consiglia di utilizzare CloudWatch Insights per creare e utilizzare in modo più efficace le espressioni di filtro a seconda dell'applicazione.

Ti consigliamo di utilizzare prima CloudWatch Gruppi di log per informazioni sui diversi tipi di risorse, sui relativi tipi di eventi e sui livelli di log che è possibile utilizzare per visualizzare le voci di log nella

console. Poi puoi utilizzare gli esempi di espressioni filtro in questa pagina come riferimento per creare filtri personalizzati per le risorse AWS IoT Wireless.

Visualizzazione di log AWS IoT nella console CloudWatch Logs insights

Nella Console CloudWatch, i log CloudWatch vengono visualizzati in un gruppo di log chiamato /aws/iotwireless. Per ulteriori informazioni su CloudWatch Logs, consulta la CloudWatch Log.

Per visualizzare i log AWS IoT nella console CloudWatch

Passa alla Console CloudWatch e scegli Logs Insights (Informazioni dettagliate sui log) nel pannello di navigazione.

1. Nella casella di testo Filter (Filtra), immetti **`/aws/iotwireless`** e seleziona `/aws/iotwireless` Logs Insights.
2. Per visualizzare un elenco completo dei gruppi di log, scegli Select log group(s) (Seleziona gruppo/i di log). Per esaminare i gruppi di registro per AWS IoT Wireless, scegli `/aws/iotwireless`.

Ora è possibile iniziare a inserire query per filtrare i gruppi di registro. Le sezioni seguenti contengono alcune utili query che ti aiuteranno a ottenere informazioni dettagliate sui parametri delle risorse.

Creare query utili per filtrare e ottenere informazioni dettagliate per AWS IoT Wireless

È possibile utilizzare le espressioni di filtro per mostrare ulteriori utili informazioni di registro con CloudWatch Insights. Di seguito vengono illustrate alcune query di esempio:

Mostra solo i log per tipi di risorse specifici

È possibile creare una query che consente di visualizzare i log solo per tipi di risorse specifici, ad esempio un gateway LoRaWAN o un dispositivo Sidewalk. Ad esempio, per filtrare i log in modo da visualizzare solo i messaggi per i dispositivi Sidewalk, puoi immettere la seguente query e scegliere Run query (Esecuzione di query). Per salvare questa query, scegli Save (Salva).

```
fields @message
| filter @message like /Sidewalk/
```

Dopo l'esecuzione della query, i risultati verranno visualizzati nella scheda Log, che mostra i timestamp per i log relativi ai dispositivi Sidewalk nel tuo account. Verrà inoltre visualizzato un grafico

a barre, che mostrerà l'ora in cui si sono verificati gli eventi, se si sono verificati in precedenza, correlati al dispositivo Sidewalk. Di seguito viene illustrato un esempio di cosa accade se si espande uno dei risultati nella scheda Log. In alternativa, se desideri risolvere gli errori relativi ai dispositivi Sidewalk, puoi aggiungere un altro filtro che imposta il livello di log su ERR0R e mostra solo le informazioni di errore.

```
Field           Value
@ingestionTime      1623894967640
@log              954314929104:/aws/iotwireless
@logStream    WirelessDevice-
Downlink_Data-715adccfb34170214ec2f6667ddfa13cb5af2c3ddfc52fbeee0e554a2e780bed
@message      {
                    "resource": "WirelessDevice",
                    "wirelessDeviceId": "3b058d05-4e84-4e1a-b026-4932bddf978d",
                    "wirelessDeviceType": "Sidewalk",
                    "devEui": "fefffff000000011a",
                    "event": "Downlink_Data",
                    "logLevel": "INFO",
                    "messageId": "7e752a10-28f5-45a5-923f-6fa7133fedda",
                    "message": "Successfully sent downlink message. Amazon SidewalkId =
 2000000006, Sequence number = 0"
                    }
@timestamp          1623894967640
devEui            fefffff000000011a
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
```

Mostra messaggi o eventi specifici

È possibile creare una query che ti aiuterà a mostrare messaggi specifici e ad osservare quando si sono verificati gli eventi. Ad esempio, se vuoi vedere quando il tuo messaggio downlink è stato inviato dal tuo dispositivo wireless LoRaWAN, puoi inserire la seguente query e scegliere Run query (Esecuzione di query). Per salvare questa query, scegli Save (Salva).

```
filter @message like /Downlink message sent/
```

Dopo l'esecuzione della query, i risultati verranno visualizzati nella scheda Log, che mostra i timestamp quando il messaggio downlink è stato inviato correttamente al dispositivo wireless. Verrà inoltre visualizzato un grafico a barre, che mostrerà l'ora in cui è stato inviato un messaggio downlink, se sono stati precedentemente inviati messaggi downlink al dispositivo wireless. Di seguito viene illustrato un esempio di cosa accade se si espande uno dei risultati nella scheda Log. In alternativa, se non è stato inviato un messaggio downlink, è possibile modificare la query per visualizzare solo i risultati per quando il messaggio non è stato inviato in modo da poter eseguire il debug del problema.

```
Field           Value
@ingestionTime      1623884043676
@log              954314929104:/aws/iotwireless
@logStream    WirelessDevice-
Downlink_Data-42d0e6d09ba4d7015f4e9756fcdc616d401cd85fe3ac19854d9fbd866153c872
@message      {
                    "timestamp": "2021-06-16T22:54:00.770493863Z",
                    "resource": "WirelessDevice",
                    "wirelessDeviceId": "3b058d05-4e84-4e1a-b026-4932bddf978d",
                    "wirelessDeviceType": "LoRaWAN",
                    "devEui": "fefffff000000011a",
                    "event": "Downlink_Data",
                    "logLevel": "INFO",
                    "messageId": "7e752a10-28f5-45a5-923f-6fa7133fedda",
                    "message": "Downlink message sent. MessageId:
 7e752a10-28f5-45a5-923f-6fa7133fedda"
                    }
@timestamp          1623884040858
devEui            fefffff000000011a
event         Downlink_Data
logLevel            INFO
message           Downlink message sent. MessageId:
 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
```

Passaggi successivi

Hai appreso come utilizzare CloudWatch Insights per ottenere informazioni più utili creando query per filtrare i messaggi di log. È possibile combinare alcuni filtri descritti in precedenza e progettare i

filtri personalizzati in base alla risorsa che stai monitorando. Per ulteriori informazioni su CloudWatch Insights, consulta Analisi dei dati di log con CloudWatch Insights.

Dopo aver creato le query con CloudWatch Insights, se sono state salvate, è possibile caricare ed eseguire le query salvate in base alle esigenze. In alternativa, se fai clic sul pulsante History (Cronologia) nella console CloudWatch Logs Insights (Informazioni dettagliate sui log), puoi visualizzare le query eseguite in precedenza e rieseguirle in base alle esigenze oppure modificarle ulteriormente creando query aggiuntive.

Notifiche di eventi per AWS IoT Wireless

AWS IoT Wireless può pubblicare messaggi per segnalarti eventi per i dispositivi LoRaWAN e Sidewalk per cui hai eseguito l'onboarding in AWS IoT Core. Ad esempio, puoi ricevere una notifica di eventi quando i dispositivi Sidewalk nel tuo account sono stati sottoposti a provisioning o sono stati registrati.

In che modo le tue risorse possono essere informate sugli eventi

Le notifiche degli eventi vengono pubblicate quando si verificano determinati eventi. Ad esempio, gli eventi vengono generati quando viene eseguito il provisioning del dispositivo Sidewalk. Ogni evento comporta l'invio di una notifica di evento univoca. Le notifiche di evento vengono pubblicate su MQTT con un payload JSON. Il contenuto del payload dipende dal tipo di evento.

> **Note**
>
> Le notifiche degli eventi vengono pubblicate almeno una volta. È anche possibile che vengano pubblicate più di una volta. L'ordine delle notifiche di evento non è garantito.

Eventi e tipi di risorse

Nella tabella seguente vengono illustrati i diversi tipi di eventi per i quali si ricevono le notifiche. I tipi di evento variano a seconda che il tipo di risorsa sia un dispositivo wireless, un gateway wireless o un account Sidewalk. Puoi anche abilitare gli eventi a livello di risorsa, che si applica a tutte le risorse di un determinato tipo, oppure per risorse selezionate, come descritto nella sezione seguente. Per ulteriori informazioni sui diversi tipi di eventi, consulta Notifiche di eventi per le risorse LoRaWAN e Notifiche di eventi per le risorse Sidewalk.

Tipi di evento basati sulle risorse

Risorsa	Tipo di risorsa	Tipo di evento	
Dispositivo wireless	LoRaWAN	Join	
	Sidewalk	• Stato di registrazione del dispositivo	

Risorsa	Tipo di risorsa	Tipo di evento
		• Prossimità
Gateway wireless	LoRaWAN	Stato della connessione
Account Sidewalk	Sidewalk	• Stato di registrazione del dispositivo • Prossimità

Policy per la ricezione delle notifiche degli eventi wireless

Per ricevere notifiche di evento, il dispositivo deve usare una policy appropriata che gli permetta di connettersi al gateway dei dispositivi AWS IoT e di sottoscrivere argomenti di evento MQTT. Devi anche sottoscrivere i filtri di argomenti appropriati.

Di seguito viene mostrato un esempio della policy necessaria per la ricezione delle notifiche per i vari eventi wireless.

```
{
    "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 degli argomenti MQTT per eventi wireless

Per inviarti notifiche di eventi per le tue risorse wireless, AWS IoT utilizza argomenti riservati MQTT che iniziano con il simbolo del dollaro ($). Effettua la sottoscrizione e pubblica gli argomenti riservati. Tuttavia, non è possibile creare nuovi argomenti che inizino con un simbolo del dollaro.

> **Note**
>
> Gli argomenti MQTT sono specifici per il tuo Account AWS e utilizzano il formato `arn:aws:iotwireless:aws-region:AWS-account-ID:topic/Topic`. Per ulteriori informazioni, consultare Argomenti MQTT nella Guida per gli sviluppatori di AWS IoT.

Gli argomenti MQTT riservati per i dispositivi wireless utilizzano il seguente formato:

- Argomenti a livello di risorsa

  Questi argomenti si applicano a tutte le risorse di un determinato tipo nel tuo Account AWS sottoposto a onboarding in AWS IoT Wireless.

  ```
  $aws/iotwireless/events/{eventName}/{eventType}/{resourceType}/resources
  ```

- Argomenti a livello di identificatore

  Questi argomenti si applicano a risorse selezionate di un determinato tipo nel tuo Account AWS sottoposto a onboarding in AWS IoT Wireless, specificato dall'identificatore della risorsa.

  ```
  $aws/iotwireless/events/{eventName}/{eventType}/{resourceType}/
  {resourceIdentifierType}/{resourceID}/{id}
  ```

Per ulteriori informazioni sugli argomenti a livello di risorsa e identificatore, consulta Configurazioni degli eventi.

La tabella seguente mostra esempi di argomenti MQTT per i vari eventi:

Eventi e argomenti MQTT

Evento	Argomento MQTT	Note

Stato di registrazione del dispositivo Sidewalk	• Argomento a livello di risorsa
	`$aws/iotwireless/events/device_registration_state/{eventType}/sidewalk/wireless_devices`
	• Argomento a livello di identificatore
	`$aws/iotwireless/events/device_registration_state/{eventType}/sidewalk/{resourceType}/{resourceID}/{id}`
		• `{eventType}` può essere `registered` o `provisioned`
		• `{resourceType}` può essere `sidewalk_accounts` o `wireless_devices`
		• `{resourceID}` è l'`amazon_id` per `sidewalk_accounts` e l'`wireless_device_id` per `wireless_devices`

Prossimità Sidewalk	• Argomento a livello di risorsa `$aws/iotwireless/events/proximity/{eventType}/sidewalk/wireless_devices` • Argomento a livello di identificatore	• `{eventType}` può essere `beacon_discovered` o `beacon_lost` • `{resourceType}` può essere `sidewalk_accounts` o `wireless_devices` • `{resourceID}` è l'`amazon_id` per `sidewalk_accounts` e l'`wireless_device_id` per `wireless_devices`

Evento	Argomento MQTT	Note
	`$aws/iotwireless/events/proximity/{eventType}/sidewalk/{resourceType}/{resourceID}/{id}`	

Join LoRaWAN	• Argomento a livello di risorsa
	`$aws/iotwireless/events/join/{eventType}/lorawan/wireless_devices`
	• Argomento a livello di identificatore
	`$aws/iotwireless/events/join/{eventType}/lorawan/wireless_devices/{resourceID}/{id}`
		• `{eventType}` può essere `join_req_0_received` o `join_req_2_received` o `join_accepted`
		• `{resourceID}` può essere `wireless_device_id` o `dev_eui`

Evento	Argomento MQTT	Note

Stato della connessione del gateway LoRaWAN	• Argomento a livello di risorsa
	`$aws/iotwireless/events/join/{eventType}/lorawan/wireless_gateways`
	• Argomento a livello di identificatore
	`$aws/iotwireless/events/join/{eventType}/lorawan/wireless_gateways/{resourceID}/{id}`
		• `{eventType}` può essere `connected` o `disconnected`
		• `{resourceID}` può essere `wireless_gateway_id` o `gateway_eui`

Per ulteriori informazioni sui diversi eventi, consulta Notifiche di eventi per le risorse LoRaWAN e Notifiche di eventi per le risorse Sidewalk.

Se hai sottoscritto questi argomenti, riceverai una notifica quando viene pubblicato un messaggio su uno degli argomenti di notifica dell'evento. Per ulteriori informazioni, consultare Argomenti riservati MQTT nella Guida per gli sviluppatori di AWS IoT.

Prezzi degli eventi wireless

Per informazioni sui prezzi per la sottoscrizione di eventi e per la ricezione di notifiche, consulta Prezzi di AWS IoT Core.

Abilitazione degli eventi per le risorse wireless

Prima che i sottoscrittori agli argomenti riservati possano ricevere messaggi, è necessario abilitare le notifiche degli eventi. Per fare ciò, è possibile utilizzare la AWS Management Console, l'API AWS IoT Wireless o AWS CLI.

Configurazioni degli eventi

Puoi configurare gli eventi per inviare notifiche a tutte le risorse appartenenti a un determinato tipo o per singole risorse wireless. Il tipo di risorsa può essere un gateway wireless, un account partner Sidewalk o un dispositivo wireless, che può essere un dispositivo LoRaWAN o Sidewalk. Per informazioni sul tipo di eventi che è possibile abilitare per i dispositivi wireless, consulta Tipi di evento per le risorse LoRaWAN e Tipi di evento per le risorse Sidewalk.

Tutte le risorse

Puoi abilitare gli eventi in modo che tutte le risorse presenti nel tuo Account AWS che appartengono a un determinato tipo di risorse ricevano le notifiche. Ad esempio, è possibile abilitare un evento che notifichi le modifiche dello stato della connessione per tutti i gateway LoRaWAN che hai sottoposto all'onboarding con AWS IoT Core per LoRaWAN. Il monitoraggio di questi eventi ti aiuterà a ricevere le notifiche nei casi in cui i gateway LoRaWAN del tuo parco istanze di risorse vengano disconnessi o un beacon venga perso per un certo numero di dispositivi Sidewalk nel tuo Account AWS.

Risorse individuali

È anche possibile aggiungere singole risorse LoRaWAN e Sidewalk alla configurazione dell'evento e abilitare le notifiche per queste risorse. In tal modo puoi monitorare le singole risorse di un determinato tipo. Ad esempio, puoi aggiungere determinati dispositivi LoRaWAN e Sidewalk alla configurazione e ricevere le notifiche per gli eventi di join o stato di registrazione del dispositivo per queste risorse.

Prerequisiti

La risorsa LoRaWAN o Sidewalk deve disporre di una policy appropriata che consenta di ricevere le notifiche degli eventi. Per ulteriori informazioni, consultare Policy per la ricezione delle notifiche degli eventi wireless.

Abilitazione delle notifiche tramite AWS Management Console

Per abilitare i messaggi di evento dalla console, accedi alla scheda Settings (Impostazioni) della console AWS IoT e vai nella sezione LoRaWAN and Sidewalk event notification (Notifica evento LoRaWAN e Sidewalk).

Puoi abilitare le notifiche per tutte le risorse del tuo Account AWS che appartengono a un determinato tipo di risorsa e monitorarle.

Per abilitare le notifiche per tutte le risorse

1. Nella sezione LoRaWAN and Sidewalk event notification (Notifica eventi LoRaWAN e Sidewalk), vai nella scheda All resources (Tutte le risorse), seleziona Action (Operazione) e quindi scegli Manage events (Gestione eventi).
2. Abilita gli eventi da monitorare e scegli Update events (Aggiorna eventi). Se non vuoi più monitorare determinati eventi, scegli Action (Operazione), seleziona Manage events (Gestione eventi) e quindi disabilita gli eventi.

Puoi anche abilitare le notifiche per le singole risorse nel tuo Account AWS che appartengono a un determinato tipo di risorsa e monitorarle.

Per abilitare le notifiche per singole risorse

1. Nella sezione LoRaWAN and Sidewalk event notification (Notifica eventi LoRaWAN e Sidewalk), scegli Action (Operazione) e quindi seleziona Add resources (Aggiungi risorse).
2. Seleziona le risorse e gli eventi per i quali desideri ricevere le notifiche:

    a. Scegli se desideri monitorare gli eventi per le LoRaWAN resources (risorse LoRaWAN) o per le Sidewalk resources (risorse Sidewalk).

    b. Puoi scegliere gli eventi da abilitare per le risorse a seconda del tipo di risorsa. Puoi quindi iscriverti a questi eventi e ricevere le notifiche. Se scegli:

    - Le risorse LoRaWAN: puoi abilitare gli eventi di join per i tuoi dispositivi LoRaWAN o gli eventi di stato della connessione per i tuoi gateway LoRaWAN.
    - Le risorse Sidewalk: puoi abilitare gli eventi di stato di registrazione del dispositivo o di prossimità o entrambi per gli account partner Sidewalk e i dispositivi Sidewalk.
3. A seconda del tipo di risorsa e degli eventi scelti, seleziona i dispositivi wireless o i gateway da monitorare. Puoi selezionare fino a 250 risorse per tutte le risorse combinate.

4. Scegli Submit (Invia) per aggiungere le risorse.

Le risorse aggiunte verranno visualizzate con i relativi argomenti MQTT nella scheda per il tipo di risorsa nella sezione LoRaWAN and Sidewalk event notification (Notifica eventi LoRaWAN e Sidewalk) della console.

- Gli eventi di join LoRaWAN e gli eventi per i tuoi dispositivi Sidewalk vengono visualizzati nella sezione Wireless devices (Dispositivi wireless) della console.
- Gli eventi di stato della connessione per i gateway LoRaWAN vengono visualizzati nella sezione Wireless gateways (Gateway wireless).
- Gli eventi di stato di registrazione del dispositivo e di prossimità per gli account Sidewalk vengono visualizzati nella scheda Sidewalk accounts (Account Sidewalk).

Sottoscrizione agli argomenti tramite il client MQTT

A seconda che siano stati abilitati per tutte le risorse o per singoli tipi di risorse, gli eventi vengono visualizzati nella console con i relativi argomenti MQTT nella scheda All resources (Tutte le risorse) o nella scheda per il tipo di risorsa specificato.

- Se scegli un argomento MQTT, puoi accedere al client MQTT per sottoscrivere l'argomento e ricevere messaggi.
- Se hai aggiunto più eventi, puoi sottoscrivere più argomenti dell'evento e ricevere le relative notifiche. Per sottoscrivere più argomenti, scegli gli argomenti e seleziona Action (Operazione) e quindi Subscribe (Sottoscrivi).

Abilitazione delle notifiche tramite AWS CLI

Puoi configurare gli eventi e aggiungere le risorse alla configurazione utilizzando l'API AWS IoT Wireless o AWS CLI.

Abilitazione delle notifiche per tutte le risorse

Puoi abilitare le notifiche per tutte le risorse del tuo Account AWS che appartengono a un determinato tipo di risorsa e monitorarle utilizzando l'API UpdateEventConfigurationByResourceTypes o il comando `update-event-configuration-by-resource-types` dell'interfaccia a riga di comando. Ad esempio:

```
aws iotwireless update-event-configuration-by-resource-types \
   --cli-input-json input.json
```

Contenuto di input.json

```
{
   "DeviceRegistrationState": {
      "Sidewalk": {
         "AmazonIdEventTopic": "Enabled"
      }
   },
   "ConnectionStatus": {
      "LoRaWAN": {
         "WirelessGatewayEventTopic": "Enabled"
      }
   }
}
```

> **Note**
>
> Tutte le virgolette doppie (") sono precedute dal carattere di escape barra rovesciata (\).

Puoi ottenere la configurazione degli eventi corrente chiamando l'API GetEventConfigurationByResourceTypes o utilizzando il comando `get-event-configuration-by-resource-types` dell'interfaccia a riga di comando. Ad esempio:

```
aws iotwireless get-event-configuration-by-resource-types
```

Abilitazione delle notifiche per singole risorse

Per aggiungere singole risorse alla configurazione dell'evento e controllare quali eventi vengono pubblicati utilizzando l'API o l'interfaccia a riga di comando, chiama l'API UpdateResourceEventConfiguration o usa il comando `update-resource-event-configuration` dell'interfaccia a riga di comando. Ad esempio:

```
aws iotwireless update-resource-event-configuration \
   --identifer 1ffd32c8-8130-4194-96df-622f072a315f \
   --identifier-type WirelessDeviceId \
   --cli-input-json input.json
```

Contenuto di input.json

```
{
   "Join": {
      "LoRaWAN": {
         "DevEuiEventTopic": "Disabled"
      },
      "WirelessDeviceIdEventTopic": "Enabled"
   }
}
```

> **Note**
>
> Tutte le virgolette doppie (") sono precedute dal carattere di escape barra rovesciata (\).

Puoi ottenere la configurazione degli eventi corrente chiamando l'API GetResourceEventConfiguration o utilizzando il comando CLI `get-resource-event-configuration`. Ad esempio:

```
aws iotwireless get-resource-event-configuration \
    --identifier-type WirelessDeviceId \
    --identifier 1ffd32c8-8130-4194-96df-622f072a315f
```

Elenco delle configurazioni di eventi

Puoi utilizzare l'API AWS IoT Wireless o AWS CLI per elencare le configurazioni degli eventi in cui è stato abilitato almeno un argomento. Per elencare le configurazioni, utilizza l'operazione API ListEventConfigurations o il comando `list-event-configurations` dell'interfaccia a riga di comando. Ad esempio:

```
aws iotwireless list-event-configurations --resource-type WirelessDevice
```

Notifiche di eventi per le risorse LoRaWAN

Puoi utilizzare le operazioni API AWS Management Console o AWS IoT Wireless per ricevere le notifiche degli eventi per i dispositivi e i gateway LoRaWAN. Per informazioni sulle notifiche di eventi e su come abilitarle, consulta Notifiche di eventi per AWS IoT Wireless e Abilitazione degli eventi per le risorse wireless.

Tipi di evento per le risorse LoRaWAN

Gli eventi che puoi abilitare per le risorse LoRaWAN sono:

- Eventi di join che ti notificano gli eventi di join del tuo dispositivo LoRaWAN. Ricevi le notifiche quando un dispositivo esegue il join con AWS IoT Core per LoRaWAN o quando viene ricevuta una richiesta di rejoin di tipo 0 o di tipo 2.
- Eventi di stato della connessione che ti notificano quando lo stato della connessione del gateway LoRaWAN cambia in connesso o disconnesso.

Le sezioni seguenti contengono ulteriori informazioni sugli eventi per le risorse LoRaWAN:

Argomenti

Eventi di join LoRaWAN

AWS IoT Core per LoRaWAN può pubblicare messaggi per notificarti gli eventi per i dispositivi LoRaWAN di cui hai eseguito l'onboarding in AWS IoT. Gli eventi di join ti notificano quando viene ricevuta una richiesta di join o di rejoin di tipo 0 o di tipo 2 e il dispositivo è stato sottoposto al join con AWS IoT Core per LoRaWAN.

Come funzionano gli eventi di join

Quando esegui l'onboarding dei dispositivi LoRaWAN con AWS IoT Core per LoRaWAN, AWS IoT Core per LoRaWAN esegue una procedura di join per il tuo dispositivo con AWS IoT Core per LoRaWAN. Il dispositivo viene quindi attivato per l'uso e può inviare un messaggio di uplink per indicare che è disponibile. Una volta eseguito il join del dispositivo, i messaggi di uplink e downlink possono essere scambiati tra il dispositivo e AWS IoT Core per LoRaWAN. Per informazioni su come eseguire l'onboarding del dispositivo, consulta Integra i tuoi dispositivi su AWS IoT Core per LoRaWAN.

Puoi abilitare gli eventi per ricevere la notifica di quando viene eseguito il join del tuo dispositivo con AWS IoT Core per LoRaWAN. Ricevi una notifica anche quando l'evento di join non riesce, quando viene ricevuta una richiesta di rejoin di tipo 0 o di tipo 2 e quando viene accettata.

Abilitazione degli eventi di join LoRaWAN

Prima che sottoscrittori agli argomenti riservati di join LoRaWAN possano ricevere messaggi, è necessario abilitare le notifiche degli eventi dalla AWS Management Console o utilizzando l'API o l'interfaccia a riga di comando. Puoi abilitare questi eventi per tutte le risorse LoRaWAN nel tuo Account AWS o per risorse selezionate. Per ulteriori informazioni su come abilitare gli eventi, consulta Abilitazione degli eventi per le risorse wireless.

Formato degli argomenti MQTT per eventi LoRaWAN

Gli argomenti MQTT riservati per i dispositivi LoRaWAN utilizzano il seguente formato. Se hai sottoscritto questi argomenti, tutti i dispositivi LoRaWAN registrati nel tuoAccount AWS possono ricevere la notifica:

- Argomenti a livello di risorsa

  ```
  $aws/iotwireless/events/{eventName}/{eventType}/lorawan/wireless_devices
  ```

- Argomenti identificatore

  ```
  $aws/iotwireless/events/{eventName}/{eventType}/lorawan/wireless_devices/
  {resourceID}/{id}
  ```

Dove:

{eventName}

{eventName} deve essere `join`.

{eventType}

{eventType} può essere:

- `join_req_received`
- `rejoin_req_0_received`
- `rejoin_req_2_received`
- `join_accepted`

{resourceID}

{resourceID} può essere `dev_eui` o `wireless_device_id`.

Ad esempio, puoi sottoscrivere i seguenti argomenti per ricevere una notifica di evento quando AWS IoT Core per LoRaWAN ha accettato una richiesta di join dai tuoi dispositivi.

```
$aws/iotwireless/events/join/join_accepted/lorawan/wireless_devices/
wireless_device_id/{id}
```

È possibile utilizzare anche il carattere jolly + per sottoscrivere più argomenti contemporaneamente. Il carattere jolly + corrisponde a qualsiasi stringa nel livello che contiene il carattere, come il seguente argomento:

```
$aws/iotwireless/events/join/join_req_received/lorawan/wireless_devices/
wireless_device_id/+
```

> **Note**
>
> Non è possibile utilizzare il carattere jolly # per sottoscrivere argomenti riservati.

Per ulteriori informazioni sull'utilizzo del carattere jolly + quando si sottoscrivono gli argomenti, consulta MQTT topic filters nella Guida per gli sviluppatori di AWS IoT.

Payload dei messaggi per l'evento di join LoRaWAN

Di seguito viene illustrato il payload dei messaggi per l'evento di join 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",
```

```
    }
}
```

Il payload contiene gli attributi seguenti:

eventId

ID evento univoco generato da AWS IoT Core per LoRaWAN (stringa).

eventType

Il tipo di evento che si è verificato. Può essere uno dei seguenti valori:

- `join_req_received`: questo campo mostra i parametri EUI `JoinEui` o `AppEui`
- `rejoin_req_0_received`
- `rejoin_req_2_received`
- `join_accepted`: questo campo mostra `NetId` e `DevAddr`.

wirelessDeviceId

ID del dispositivo LoRaWAN.

timestamp

Timestamp Unix del momento in cui si è verificato l'evento.

DevEui

Identificatore univoco del dispositivo trovato sull'etichetta del dispositivo o sulla documentazione del dispositivo.

DevAddr e EUI (facoltativo)

Questi campi rappresentano l'indirizzo del dispositivo facoltativo e i parametri EUI `JoinEUI` o `AppEUI`.

Eventi di stato della connessione

AWS IoT Core per LoRaWAN può pubblicare messaggi per segnalarti eventi di stato della connessione per i gateway LoRaWAN per cui hai eseguito l'onboarding in AWS IoT. Gli eventi di stato della connessione segnalano quando lo stato della connessione di un gateway LoRaWAN cambia in connesso o disconnesso.

Come funzionano gli eventi di stato della connessione

Dopo aver eseguito l'onboarding del gateway in AWS IoT Core per LoRaWAN, puoi connettere il gateway a AWS IoT Core per LoRaWAN e verificare lo stato della connessione. Questo evento ti avvisa quando lo stato della connessione del gateway cambia in connesso o disconnesso. Per ulteriori informazioni su come eseguire l'onboarding e sulla connessione del gateway a AWS IoT Core per LoRaWAN, consulta Integrare i gateway per AWS IoT Core per LoRaWAN e Connetti il tuo gateway LoRaWAN e verifica lo stato della connessione.

Formato degli argomenti MQTT per gateway LoRaWAN

Gli argomenti MQTT riservati per i gateway LoRaWAN utilizzano il seguente formato. Se hai sottoscritto questi argomenti, tutti i gateway LoRaWAN registrati nel tuo Account AWS possono ricevere la notifica:

- Per argomenti a livello di risorsa:

  ```
  $aws/iotwireless/events/{eventName}/{eventType}/lorawan/wireless_gateways
  ```

- Per argomenti identificatore:

  ```
  $aws/iotwireless/events/{eventName}/{eventType}/lorawan/
  wireless_gateways/{resourceID}/{id}
  ```

Dove:

{eventName}

{eventName} deve essere `connection_status`.

{eventType}

{eventType} può essere `connected` o `disconnected`.

{resourceID}

{resourceID} può essere `gateway_eui` o `wireless_gateway_id`.

Ad esempio, puoi sottoscrivere i seguenti argomenti per ricevere una notifica di evento quando tutti i gateway si sono connessi a AWS IoT Core per LoRaWAN:

```
$aws/iotwireless/events/connection_status/connected/lorawan/
wireless_gateways/wireless_gateway_id/{id}
```

È possibile utilizzare anche il carattere jolly + per sottoscrivere più argomenti contemporaneamente. Il carattere jolly + corrisponde a qualsiasi stringa nel livello che contiene il carattere, come il seguente argomento:

```
$aws/iotwireless/events/connection_status/connected/lorawan/
wireless_gateways/wireless_gateway_id/+
```

> **Note**
>
> Non è possibile utilizzare il carattere jolly # per sottoscrivere argomenti riservati.

Per ulteriori informazioni sull'utilizzo del carattere jolly + quando si sottoscrivono gli argomenti, consulta MQTT topic filters nella Guida per gli sviluppatori di AWS IoT.

Payload dei messaggi per eventi di stato della connessione

Di seguito viene illustrato il payload dei messaggi per l'evento di stato della connessione.

```
{
 // General fields
    "eventId": "string",
    "eventType": "connected|disconnected",
    "WirelessGatewayId": "string",
    "timestamp": "timestamp",

 // Event-specific fields
    "LoRaWAN": {
        "GatewayEui": "string"
    }
}
```

Il payload contiene gli attributi seguenti:

eventId

ID evento univoco generato da AWS IoT Core per LoRaWAN (stringa).

eventType

Il tipo di evento che si è verificato. Può essere `connected` o `disconnected`.

wirelessGatewayId

L'ID del gateway LoRaWAN.

timestamp

Timestamp Unix del momento in cui si è verificato l'evento.

GatewayEui

Identificatore univoco del gateway trovato sull'etichetta del gateway o nella documentazione del gateway.

Notifiche di eventi per le risorse Sidewalk

Puoi utilizzare le operazioni API AWS Management Console o AWS IoT Wireless per ricevere le notifiche degli eventi per i dispositivi Sidewalk e gli account partner. Per informazioni sulle notifiche di eventi e su come abilitarle, consulta Notifiche di eventi per AWS IoT Wireless e Abilitazione degli eventi per le risorse wireless.

Tipi di evento per le risorse Sidewalk

Gli eventi che puoi abilitare per le risorse Sidewalk sono:

- Eventi del dispositivo che segnalano modifiche allo stato del dispositivo Sidewalk, ad esempio quando il dispositivo è stato registrato ed è pronto per l'uso.
- Eventi di prossimità quando AWS IoT Wireless riceve una notifica da Amazon Sidewalk per segnalare che un beacon è stato individuato o perso.

Le sezioni seguenti contengono ulteriori informazioni sugli eventi per le risorse Sidewalk:

Argomenti

- Eventi sullo stato di registrazione del dispositivo
- Eventi di prossimità

Eventi sullo stato di registrazione del dispositivo

Gli eventi dello stato di registrazione del dispositivo pubblicano le notifiche degli eventi in caso di modifica dello stato di registrazione del dispositivo, (ad esempio, in caso di provisioning o registrazione di un dispositivo Sidewalk). Gli eventi forniscono informazioni sui diversi stati del dispositivo dal momento in cui viene eseguito il provisioning al momento della registrazione.

Come funzionano gli eventi sullo stato di registrazione del dispositivo

Quando esegui l'onboarding del dispositivo Sidewalk con Amazon Sidewalk e AWS IoT Wireless, AWS IoT Wireless esegue un'operazione `create` e aggiunge il dispositivo Sidewalk al tuo Account AWS. Il dispositivo entra quindi nello stato di provisioning e `eventType` diventa `provisioned`. Per informazioni su come eseguire l'onboarding del dispositivo, consulta Nozioni di base sull'utilizzo di AWS IoT Core per Amazon Sidewalk.

Una volta che lo stato del dispositivo è `provisioned`, Amazon Sidewalk esegue un'operazione `register` per registrare il dispositivo Sidewalk con AWS IoT Wireless. Il processo di registrazione inizia dove vengono configurate le chiavi di crittografia e di sessione con AWS IoT. Quando il dispositivo è registrato, `eventType` diventa `registered`, e il dispositivo è pronto per l'uso.

Una volta che lo stato del dispositivo è `registered`, Sidewalk può inviare una richiesta per `deregister` il dispositivo. AWS IoT Wireless quindi soddisfa la richiesta e modifica lo stato del dispositivo in `provisioned`. Per ulteriori informazioni sullo stato del dispositivo, consulta DeviceState (Stato Dispositivo).

Abilita le notifiche per gli eventi di stato della registrazione del dispositivo

Prima che i sottoscrittori dello stato di registrazione del dispositivo, possano ricevere messaggi, è necessario abilitare per loro le notifiche degli eventi, dalla AWS Management Console o utilizzando l'API o la CLI. Puoi abilitare questi eventi per tutte le risorse Sidewalk nel tuo Account AWS o per risorse selezionate. Per ulteriori informazioni su come abilitare gli eventi, consulta Abilitazione degli eventi per le risorse wireless.

Formato degli argomenti MQTT per eventi di stato di registrazione del dispositivo

Per ricevere avvisi sugli eventi di stato di registrazione del dispositivo, puoi sottoscrivere gli argomenti riservati MQTT che iniziano con un simbolo del dollaro ($). Per ulteriori informazioni, consultare Argomenti MQTT nella Guida per gli sviluppatori di AWS IoT.

Gli argomenti MQTT riservati per gli eventi di stato di registrazione del dispositivo Sidewalk utilizzano il seguente formato:

- Per argomenti a livello di risorsa:

  ```
  $aws/iotwireless/events/{eventName}/{eventType}/sidewalk/wireless_devices
  ```

- Per argomenti identificatore:

  ```
  $aws/iotwireless/events/{eventName}/{eventType}/sidewalk/{resourceType}/
  {resourceID}/{id}
  ```

Dove:

{eventName}

{eventName} deve essere `device_registation_state`.

{eventType}

{eventType} può essere `provisioned` o `registered`.

{resourceType}

{resourceType} può essere `sidewalk_accounts` o `wireless_devices`.

{resourceID}

{resourceID} è `amazon_id` per {resourceType} di `sidewalk_accounts` e `wireless_device_id` per {resourceType} di`wireless_devices`.

È possibile utilizzare anche il carattere jolly + per sottoscrivere più argomenti contemporaneamente. Il carattere jolly + corrisponde a qualsiasi stringa nel livello che contiene il carattere. Ad esempio, se vuoi ricevere notifiche su tutti i tipi di evento possibili (`provisioned` e `registered`) e per tutti i dispositivi registrati su un particolare ID Amazon, puoi utilizzare il filtro di argomenti che segue:

```
$aws/iotwireless/events/device_registration_state/+/sidewalk/
sidewalk_accounts/amazon_id/+
```

> **Note**
>
> Non è possibile utilizzare il carattere jolly # per sottoscrivere argomenti riservati. Per ulteriori informazioni sui filtri per argomento, consulta MQTT topic filters nella Guida per gli sviluppatori di AWS IoT.

Payload dei messaggi per eventi di stato di registrazione del dispositivo

Dopo aver abilitato notifiche per eventi di stato di registrazione del dispositivo, le notifiche degli eventi vengono pubblicate su MQTT con un payload JSON. Questi eventi contengono il payload di esempio seguente:

```
{
    "eventId": "string",
    "eventType": "provisioned|registered",
    "WirelessDeviceId": "string",
    "timestamp": "timestamp",

    // Event-specific fields
    "operation": "create|deregister|register",
    "Sidewalk": {
        "AmazonId": "string",
        "SidewalkManufacturingSn": "string"
    }
}
```

Il payload contiene gli attributi seguenti:

eventId

ID evento univoco (stringa).

eventType

Il tipo di evento che si è verificato. Può essere `provisioned` o `registered`.

wirelessDeviceId

Identificatore del dispositivo wireless.

timestamp

Timestamp Unix del momento in cui si è verificato l'evento.

operazione

Operazione che ha attivato l'evento. I valori validi sono `create`, `register` e `deregister`.

sidewalk

L'ID Amazon Sidewalk o `SidewalkManufacturingSn` per cui vuoi ricevere le notifiche di evento.

Eventi di prossimità

Gli eventi di prossimità pubblicano notifiche degli eventi quando AWS IoT riceve un beacon dal dispositivo Sidewalk. Quando il dispositivo Sidewalk si avvicina ad Amazon Sidewalk, i beacon inviati dal dispositivo vengono filtrati da Amazon Sidewalk a intervalli regolari e ricevuti da AWS IoT Wireless. AWS IoT Wireless quindi ti notifica questi eventi quando viene ricevuto un beacon.

Come funzionano gli eventi di prossimità

Gli eventi di prossimità ti segnalano quando AWS IoT riceve un beacon, i dispositivi Sidewalk possono emettere beacon in qualsiasi momento. Quando il tuo dispositivo è vicino ad Amazon Sidewalk, Sidewalk riceve i beacon e li inoltra a AWS IoT Wireless a intervalli di tempo regolari. Amazon Sidewalk ha impostato questo intervallo di tempo a 10 minuti. Quando AWS IoT Wireless riceve il beacon da Sidewalk, riceverai una notifica dell'evento.

Gli eventi di prossimità ti avviseranno quando un beacon viene scoperto o perso. È possibile configurare gli intervalli con cui viene notificato l'evento di prossimità.

Abilita le notifiche per eventi di prossimità

Prima che i sottoscrittori degli argomenti riservati di prossimità Sidewalk possano ricevere i messaggi, è necessario abilitare le notifiche di eventi, dalla AWS Management Console o utilizzando l'API o l'interfaccia a riga di comando. Puoi abilitare questi eventi per tutte le risorse Sidewalk nel tuo Account AWS o per risorse selezionate. Per ulteriori informazioni su come abilitare gli eventi, consulta Abilitazione degli eventi per le risorse wireless.

Formato degli argomenti MQTT per eventi di prossimità

Per ricevere avvisi sugli eventi di prossimità, puoi sottoscrivere gli argomenti riservati MQTT che iniziano con un simbolo del dollaro ($). Per ulteriori informazioni, consultare Argomenti MQTT nella Guida per gli sviluppatori di AWS IoT.

Gli argomenti MQTT riservati per gli eventi di prossimità Sidewalk utilizzano il formato:

- Per argomenti a livello di risorsa:

  `$aws/iotwireless/events/{eventName}/{eventType}/sidewalk/wireless_devices`
- Per argomenti identificatore:

  `$aws/iotwireless/events/{eventName}/{eventType}/sidewalk/{resourceType}/{resourceID}/{id}`

Dove:

{eventName}

{eventName} deve essere `proximity`.

{eventType}

{eventType} può essere `beacon_discovered` o `beacon_lost`.

{resourceType}

{resourceType} può essere `sidewalk_accounts` o `wireless_devices`.

{resourceID}

{resourceID} è `amazon_id` per {resourceType} di `sidewalk_accounts` e `wireless_device_id` per {resourceType} di`wireless_devices`.

È possibile utilizzare anche il carattere jolly + per sottoscrivere più argomenti contemporaneamente. Il carattere jolly + corrisponde a qualsiasi stringa nel livello che contiene il carattere. Ad esempio, se vuoi ricevere notifiche su tutti i tipi di evento possibili (`beacon_discovered` e `beacon_lost`) e per tutti i dispositivi registrati su un particolare ID Amazon, puoi utilizzare il filtro di argomenti che segue:

`$aws/iotwireless/events/proximity/+/sidewalk/sidewalk_accounts/amazon_id/+`

> **Note**
>
> Non è possibile utilizzare il carattere jolly # per sottoscrivere argomenti riservati. Per ulteriori informazioni sui filtri per argomento, consulta MQTT topic filters nella Guida per gli sviluppatori di AWS IoT.

Payload dei messaggi per eventi di prossimità

Dopo aver abilitato le notifiche per eventi di prossimità, i messaggi di evento vengono pubblicati su MQTT con un payload JSON. Questi eventi contengono il payload di esempio seguente:

```
{
    "eventId": "string",
    "eventType": "beacon_discovered|beacon_lost",
    "WirelessDeviceId": "string",
    "timestamp": "1234567890123",

    // Event-specific fields
    "Sidewalk": {
        "AmazonId": "string",
        "SidewalkManufacturingSn": "string"
    }
}
```

Il payload contiene gli attributi seguenti:

eventId

Un ID evento univoco, rappresentato da una stringa.

eventType

Il tipo di evento che si è verificato. Può essere `beacon_discovered` o `beacon_lost`.

WirelessDeviceId

Identificatore del dispositivo wireless.

timestamp

Timestamp Unix del momento in cui si è verificato l'evento.

sidewalk

L'ID Amazon Sidewalk o `SidewalkManufacturingSn` per cui vuoi ricevere le notifiche di evento.

Operazioni API AWS IoT Wireless

È possibile eseguire le seguenti operazioni API aggiuntive durante l'onboarding dei dispositivi finali LoRaWAN o Sidewalk oppure durante la creazione di un'attività di importazione per il provisioning di dispositivi finali Sidewalk in blocco.

Le sezioni seguenti contengono informazioni aggiuntive su queste operazioni API.

Argomenti

Operazioni API AWS IoT Wireless per profili dei dispositivi

È possibile eseguire le seguenti operazioni API per i profili dei dispositivi LoRaWAN o Sidewalk:

- API `CreateDeviceProfile` o interfaccia a riga di comando `create-device-profile`
- API `GetDeviceProfile` o interfaccia a riga di comando `get-device-profile`
- API `ListDeviceProfiles` o interfaccia a riga di comando `list-device-profiles`
- API `DeleteDeviceProfile` o interfaccia a riga di comando `delete-device-profile`

Nelle sezioni seguenti viene illustrato come elencare ed eliminare i profili. Per informazioni sulla creazione e il recupero di profili di dispositivi, consulta:

- Aggiungi profili di dispositivo
- Fase 1: Creazione di un profilo del dispositivo

Elencare profili di dispositivi in Account AWS

È possibile utilizzare l'operazione API `ListDeviceProfiles` per elencare i profili di dispositivi in Account AWS che sono stati aggiunti ad AWS IoT Wireless. È possibile utilizzare queste informazioni per identificare i dispositivi a cui si desidera associare questo profilo.

Per filtrare l'elenco per visualizzare solo i profili dei dispositivi Sidewalk, imposta il `Type` durante l'esecuzione dell'API. Di seguito viene illustrato un esempio del comando dell'interfaccia a riga di comando:

```
aws iotwireless list-device-profiles --wireless-device-type "Sidewalk"
```

L'esecuzione di questo comando restituisce un elenco di profili dei dispositivi aggiunti, inclusi l'identificatore del profilo e il nome della risorsa Amazon (ARN). Per recuperare dettagli aggiuntivi su un profilo specifico, utilizza l'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"
        }
    ]
}
```

Eliminazione dei profili di dispositivi da Account AWS

È possibile eliminare profili di dispositivi utilizzando l'operazione API `DeleteDeviceProfile`. Di seguito viene illustrato un esempio del comando dell'interfaccia a riga di comando:

> **Warning**
>
> Le operazioni di eliminazione non possono essere annullate. Il profilo del dispositivo verrà rimosso definitivamente da Account AWS.

```
aws iotwireless delete-device-profile --name "SidewalkProfile"
```

Il comando non produce output. È possibile utilizzare l'API `GetDeviceProfile` o l'operazione API `ListDeviceProfiles` per verificare che il profilo sia stato rimosso dall'account.

Operazioni API AWS IoT Wireless per dispositivi LoRaWAN e Sidewalk

È possibile eseguire le seguenti operazioni API per i dispositivi LoRaWAN e Sidewalk:

- API `CreateWirelessDevice` o interfaccia a riga di comando `create-wireless-device`
- API `GetWirelessDevice` o interfaccia a riga di comando `get-wireless-device`
- API `ListWirelessDevices` o interfaccia a riga di comando `list-wireless-devices`
- API `DeleteWirelessDevice` o interfaccia a riga di comando `delete-wireless-device`
- API `UpdateWirelessDevice` o interfaccia a riga di comando `update-wireless-device`
- API `AssociateWirelessDeviceWithThing` o interfaccia a riga di comando `associate-wireless-device-with-thing`
- API `DisassociateWirelessDeviceFromThing` o interfaccia a riga di comando `disassociate-wireless-device-from-thing`

Nelle sezioni seguenti viene illustrato come elencare ed eliminare i dispositivi. Per informazioni sulla creazione di dispositivi finali wireless e sul recupero delle informazioni dispositivo, consulta:

- Aggiungi il dispositivo wireless ad AWS IoT Core per LoRaWAN
- Fase 2: Aggiunta del dispositivo Sidewalk

Associazione di dispositivi wireless dell'Account AWS a un oggetto IoT

Per associare i dispositivi LoRaWAN e Sidewalk a un oggetto AWS IoT, utilizza l'operazione API `AssociateWirelessDeviceWithThing`.

Gli oggetti in AWS IoT semplificano la ricerca e la gestione dei dispositivi. L'associazione di un oggetto al dispositivo consente al dispositivo di accedere ad altre funzionalità di AWS IoT Core. Per ulteriori informazioni sull'utilizzo dell'API, consulta `AssociateWirelessDeviceWithThing`.

Di seguito viene illustrato un esempio di esecuzione di questo comando. L'esecuzione di questo comando non produce output.

```
aws iotwireless associate-wireless-device-with-thing \
    --id "12345678-a1b2-3c45-67d8-e90fa1b2c34d" \
    --thing-arn "arn:aws:iot:us-east-1:123456789012:thing/MySidewalkThing"
```

Per dissociare il dispositivo wireless da un oggetto AWS IoT, utilizza l'operazione API DisassociateWirelessDeviceFromThing, come illustrato nell'esempio seguente.

```
aws iotwireless disassociate-wireless-device-from-thing \
    --id "12345678-a1b2-3c45-67d8-e90fa1b2c34d"
```

Elencazione dei dispositivi wireless presenti nell'Account AWS

Per elencare i dispositivi Sidewalk dell'Account AWS aggiunti ad AWS IoT Wireless, utilizza l'operazione API ListWirelessDevices. Per filtrare l'elenco in modo da restituire solo i dispositivi Sidewalk, imposta `WirelessDeviceType`.

Di seguito viene illustrato un esempio di esecuzione di questo comando:

```
aws iotwireless list-wireless-devices --wireless-device-type Sidewalk
```

L'esecuzione di questo comando restituisce un elenco di dispositivi aggiunti, inclusi l'identificatore del profilo e il nome della risorsa Amazon (ARN). Per recuperare dettagli aggiuntivi su un dispositivo specifico, utilizza l'operazione API GetWirelessDevice.

```
{
    "WirelessDeviceList": [
        {
            "Name": "mySidewalkDevice",
            "DestinationName": "SidewalkDestination",
            "Id": "1ffd32c8-8130-4194-96df-622f072a315f",
            "Type": "Sidewalk",
            "Sidewalk": {
                "SidewalkId": "1234567890123456"
            },
            "Arn": "arn:aws:iotwireless:us-
east-1:123456789012:WirelessDevice/1ffd32c8-8130-4194-96df-622f072a315f"
        }
    ]
}
```

Eliminazione di dispositivi wireless da Account AWS

Per eliminare i dispositivi wireless, passa il `WirelessDeviceID` dei dispositivi da eliminare all'operazione API `DeleteWirelessDevice`.

Di seguito viene illustrato un esempio del comando:

```
aws iotwireless delete-wireless-device --id "23456789-abcd-0123-bcde-fabc012345678"
```

Il comando non produce output. È possibile utilizzare l'API `GetWirelessDevice` o l'operazione API `ListWirelessDevices` per verificare che il dispositivo sia stato rimosso dall'account.

Operazioni API AWS IoT Wireless per destinazioni per dispositivi wireless

È possibile eseguire le seguenti operazioni API per destinazioni per i dispositivi finali LoRaWAN e Sidewalk:

- API `CreateDestination` o interfaccia a riga di comando `create-destination`
- API `GetDestination` o interfaccia a riga di comando `get-destination`
- API `UpdateDestination` o interfaccia a riga di comando `update-destination`
- API `ListDestinations` o interfaccia a riga di comando `list-destinations`
- API `DeleteDestination` o interfaccia a riga di comando `delete-destination`

Nelle sezioni seguenti viene illustrato come ottenere, elencare, aggiornare ed eliminare le destinazioni. Per informazioni sulla creazione di destinazioni, consultare Aggiunta di una destinazione per il dispositivo finale Sidewalk.

Ottenere informazioni sulla destinazione

È possibile utilizzare l'operazione API `GetDestination` per ottenere informazioni sulla destinazione aggiunta all'account per AWS IoT Wireless. Fornisci il nome della destinazione come input all'API. L'API restituirà le informazioni sulla destinazione che corrispondono all'identificatore specificato.

Di seguito viene illustrato un esempio del comando dell'interfaccia a riga di comando:

```
aws iotwireless get-destination --name SidewalkDestination
```

L'esecuzione di questo comando restituisce i parametri della destinazione.

```
{
    "Arn": "arn:aws:iotwireless:us-east-1:123456789012:Destination/
IoTWirelessDestination",
    "Name": "SidewalkDestination",
    "Expression": "IoTWirelessRule",
    "ExpressionType": "RuleName",
    "RoleArn": "arn:aws:iam::123456789012:role/IoTWirelessDestinationRole"
}
```

Aggiornamento delle proprietà della destinazione

Utilizza l'operazione API `UpdateDestination` per aggiornare le proprietà della destinazione aggiunta all'account per AWS IoT Wireless. Di seguito viene illustrato un esempio del comando dell'interfaccia a riga di comando che aggiorna la proprietà descrizione:

```
aws iotwireless update-destination --name SidewalkDestination \
    --description "Destination for messages processed using IoTWirelessRule"
```

Elencare le destinazioni in Account AWS

Utilizza l'operazione API `ListDestinations` per elencare le destinazioni in Account AWS aggiunte ad AWS IoT Wireless. Per filtrare l'elenco in modo da restituire solo le destinazioni per i dispositivi finali LoRaWAN e Sidewalk, utilizza il parametro `WirelessDeviceType`.

Di seguito viene illustrato un esempio del comando dell'interfaccia a riga di comando:

```
aws iotwireless list-destinations --wireless-device-type "Sidewalk"
```

L'esecuzione di questo comando restituisce un elenco di destinazioni aggiunte, incluso il nome della risorsa Amazon (ARN). Per recuperare dettagli aggiuntivi su una destinazione specifica, utilizza l'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"
        }
    ]
}
```

Eliminazione di destinazioni da Account AWS

Per eliminare la destinazione, passa il nome della destinazione da eliminare come input all'operazione API `DeleteDestination`. Di seguito viene illustrato un esempio del comando dell'interfaccia a riga di comando:

> **Warning**
>
> Le operazioni di eliminazione non possono essere annullate. La destinazione verrà rimossa definitivamente da Account AWS.

```
aws iotwireless delete-destination --name "SidewalkDestination"
```

Il comando non produce output. È possibile utilizzare l'API `GetDestination` o l'operazione API `ListDestinations` per verificare che la destinazione sia stata rimossa dall'account.

Operazioni API AWS IoT Core per Amazon Sidewalk per il provisioning in blocco

È possibile eseguire le seguenti operazioni API per il provisioning in blocco dei dispositivi finali Sidewalk:

- API `StartWirelessDeviceImportTask` o interfaccia a riga di comando `start-wireless-device-import-task`

- API StartSingleWirelessDeviceImportTask o interfaccia a riga di comando start-single-wireless-device-import-task
- API ListWirelessDeviceImportTasks o interfaccia a riga di comando list-wireless-device-import-tasks
- API ListDevicesForWirelessDeviceImportTask o interfaccia a riga di comando list-devices-for-wireless-device-import-task
- API GetWirelessDeviceImportTask o interfaccia a riga di comando get-wireless-device-import-task
- API UpdateWirelessDeviceImportTask o interfaccia a riga di comando update-wireless-device-import-task
- API DeleteWirelessDeviceImportTask o interfaccia a riga di comando delete-wireless-device-import-task

Nelle sezioni seguenti viene illustrato come ottenere, elencare, aggiornare ed eliminare le attività di importazione. Per ulteriori informazioni sulla creazione di attività di importazione, consultare Operazioni API AWS IoT Core per Amazon Sidewalk per il provisioning in blocco.

Ottenere informazioni sull'attività di importazione

È possibile utilizzare l'operazione API ListDevicesForWirelessDeviceImportTask per recuperare informazioni su una particolare attività di importazione e sullo stato di onboarding dei dispositivi in tale attività. Come input per l'operazione API, specifica l'ID dell'attività di importazione ottenuto dalle operazioni API `StartWirelessDeviceImportTask` o `StartSingleWirelessDeviceImportTask`. L'API restituirà quindi le informazioni sull'attività di importazione corrispondenti all'identificatore specificato.

Di seguito viene illustrato un esempio del comando dell'interfaccia a riga di comando:

```
aws iotwireless list-devices-for-wireless-device-import-task --id e2a5995e-743b-41f2-a1e4-3ca6a5c5249f
```

L'esecuzione di questo comando restituisce le informazioni sull'attività di importazione e lo stato di onboarding del 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":
 "12345ABCDE6789FABDESBDEF123456789012345FEABC0123679AFEBC01234EF"
         },
      }
   ]
}
```

Ottenere il riepilogo delle attività di importazione dei dispositivi

Per ottenere un conteggio delle informazioni di riepilogo dello stato di onboarding dei dispositivi aggiunti a una particolare attività di importazione, utilizza l'operazione API `GetWirelessDeviceImportTask`. Di seguito viene illustrato un esempio del comando dell'interfaccia a riga di comando.

```
aws iotwireless get-wireless-device-import-task --Id "e2a5995e-743b-41f2-
a1e4-3ca6a5c5249f"
```

Il codice riportato di seguito mostra una risposta di esempio del comando.

```
{
   "NumberOfFailedImportedDevices": 2,
   "NumberOfOnboardedImportedDevices": 4,
   "NumberOfPendingImportedDevices": 1
}
```

Aggiunta di dispositivi all'attività di importazione

Utilizza l'operazione API `UpdateWirelessDeviceImportTask` per aggiungere dispositivi a un'attività di importazione esistente aggiunta. Puoi utilizzare questa operazione API per aggiungere i numeri di serie (SMSN) dei dispositivi che in precedenza non erano inclusi nell'attività creata utilizzando l'operazione API `StartWirelessDeviceImportTask`.

Per aggiungere dispositivi all'attività di importazione, come parte della richiesta API, specifica un nuovo file CSV in un bucket Amazon S3 contenente i numeri di serie dei dispositivi da aggiungere. La richiesta verrà accettata solo se il processo di onboarding non è già stato avviato per i dispositivi attualmente contenuti nell'attività di importazione. Se il processo di onboarding è già stato avviato, la richiesta API `UpdateWirelessDeviceImportTask` non andrà a buon fine.

Se desideri comunque aggiungere dispositivi all'attività di importazione, puoi eseguire l'operazione API `UpdateWirelessDeviceImportTask` una seconda volta. Prima di eseguire questa operazione API, la prima richiesta API `UpdateWirelessDeviceImportTask` deve aver completato l'elaborazione del file CSV nel bucket S3.

> **Note**
>
> Quando esegui una richiesta API `ListImportedWirelessDeviceTasks`, l'URL S3 del nuovo file CSV specificato utilizzando l'operazione API `UpdateWirelessDeviceImportTask` non viene attualmente restituito. L'operazione API restituisce invece l'URL S3 della richiesta inviata originariamente utilizzando la richiesta API `StartWirelessDeviceImportTask`.

Di seguito viene illustrato un esempio del comando dell'interfaccia a riga di comando.

```
aws iotwireless update-wireless-device-import task \
    --Id "e2a5995e-743b-41f2-a1e4-3ca6a5c5249f" \
    --sidewalk '{"FileForCreateDevices": "s3://import_task_bucket/import_file3"}'
```

Elencare le attività di importazione in Account AWS

Utilizza l'API `ListWirelessDeviceImportTasks` o il comando dell'interfaccia a riga di comando `list-imported-wireless-device-tasks` per elencare le attività di importazione in Account AWS. Di seguito viene illustrato un esempio del comando dell'interfaccia a riga di comando.

```
aws iotwireless list-wireless-device-import-tasks
```

L'esecuzione di questo comando restituisce un elenco delle attività di importazione create. L'elenco include i file CSV di Amazon S3 e il ruolo IAM specificato, l'ID dell'attività di importazione e informazioni di riepilogo dello stato di inserimento del 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"
      }
   ]
}
```

Eliminazione delle attività di importazione da Account AWS

Per eliminare un'attività di importazione, passa l'ID dell'attività di importazione all'operazione API `DeleteWirelessDeviceImportTask` o al comando dell'interfaccia a riga di comando `delete-wireless-device-import-task`.

> **Warning**
>
> Le operazioni di eliminazione non possono essere annullate. L'attività di importazione verrà rimossa definitivamente da Account AWS.

Quando esegui la richiesta API `DeleteWirelessDeviceImportTask`, un processo in background avvia l'eliminazione dell'attività di importazione. Quando la richiesta è in corso, i numeri di serie (SMSN) dei dispositivi nelle attività di importazione sono inclusi nel processo di eliminazione. Solo dopo il completamento dell'eliminazione potrai visualizzare queste informazioni utilizzando le operazioni API `ListImportedWirelessDeviceTasks` o `GetImportedWirelessDeviceTasks`.

Se un'attività di importazione contiene ancora dispositivi per i quali non è ancora stato eseguito l'onboarding, la richiesta API `DeleteWirelessDeviceImportTask` verrà elaborata solo dopo che sarà stato eseguito l'onboarding di tutti i dispositivi nell'attività di importazione o l'onboarding non è andato a buon fine. Un'attività di importazione scade dopo 90 giorni e, una volta scaduta, può essere eliminata dall'account. Tuttavia, i dispositivi che per i quali è stato eseguito l'onboarding utilizzando l'attività di importazione non verranno eliminati.

> **Note**
>
> Se tenti di creare un'altra attività di importazione che include il numero di serie di un dispositivo in attesa di eliminazione utilizzando la richiesta API `DeleteWirelessDeviceImportTask`, l'operazione API `StartWirelessDeviceImportTask` restituirà un errore.

Di seguito viene illustrato un esempio del comando dell'interfaccia a riga di comando:

```
aws iotwireless delete-import-task --Id "e2a5995e-743b-41f2-a1e4-3ca6a5c5249f"
```

Il comando non produce output. Dopo che l'attività è stata eliminata, per verificare che l'attività di importazione sia stata rimossa dall'account, puoi utilizzare l'operazione API `GetWirelessDeviceImportTask` o `ListWirelessDeviceImportTasks`.

Creazione di risorse wireless AWS IoT con AWS CloudFormation

Wireless AWS IoT è integrato con AWS CloudFormation, un servizio che ti consente di modellare e configurare le risorse AWS in modo da dedicare meno tempo alla creazione e alla gestione delle risorse e dell'infrastruttura. Puoi creare un modello che descrive tutte le risorse AWS che desideri perché AWS CloudFormation si occupi del provisioning e della configurazione di queste risorse per te.

Quando usi AWS CloudFormation, puoi riutilizzare il modello per configurare le risorse Wireless AWS IoT in modo coerente e continuo. Basta descrivere le risorse una volta sola, dopodiché si può effettuare il provisioning di tali risorse quante volte si vuole in più Account AWS e regioni.

Wireless AWS IoT e modelli AWS CloudFormation

Per eseguire l'assegnazione e la configurazione delle risorse per Wireless AWS IoT e i servizi correlati, devi conoscere i modelli AWS CloudFormation. I modelli sono file di testo formattati in JSON o YAML. Questi modelli descrivono le risorse di cui intendi effettuare il provisioning negli stack AWS CloudFormation. Se non hai familiarità con JSON o YAML, puoi usare AWS CloudFormationDesigner per iniziare a utilizzare i modelli AWS CloudFormation. Per ulteriori informazioni, consulta Che cos'è AWS CloudFormationDesigner? nella Guida per l'utente di AWS CloudFormation.

Wireless AWS IoT supporta la creazione di risorse wireless in AWS CloudFormation. Per ulteriori informazioni, inclusi esempi di modelli JSON e YAML per le risorse AWS IoT Wireless, consulta AWS IoT Wireless resource type reference nella Guida per l'utente AWS CloudFormation.

Ulteriori informazioni su AWS CloudFormation

Per ulteriori informazioni su AWS CloudFormation, consulta le seguenti risorse:

- AWS CloudFormation
- Guida per l'utente di AWS CloudFormation
- Guida per l'utente dell'interfaccia a riga di comando di AWS CloudFormation

Quote per Wireless AWS IoT

Il tuo Account AWS dispone di quote predefinite, precedentemente chiamate limiti, per ogni Servizio AWS. Salvo diversa indicazione, ogni quota si applica a una regione specifica. Se per alcune quote è possibile richiedere aumenti, altre quote non possono essere modificate.

Per visualizzare le quote per Wireless AWS IoT, apri la console Service Quotas. Nel pannello di navigazione, scegli Servizio AWS e seleziona Wireless AWS IoT.

Per richiedere un aumento delle quote, consultare Richiesta di aumento delle quote nella Guida per l'utente di Service Quotas. Se la quota non è ancora disponibile in Service Quotas, utilizza il modulo di incremento dei limiti.

AWS IoT Wireless ha quote per:

- Quote AWS IoT Core per LoRaWAN applicabili ai dati del dispositivo che vengono trasmessi tra i dispositivi
- Operazioni API AWS IoT Wireless applicabili sia ai dispositivi LoRaWAN che ai Sidewalk.

Per ulteriori informazioni, consultare AWS IoT Core per LoRaWAN quotas in Riferimenti generali di AWS.

Tagging delle risorse AWS IoT Wireless

Per aiutarti a gestire e organizzare dispositivi, gateway, destinazioni e profili, è possibile assegnare i metadati a ciascuna di queste risorse sotto forma di tag. Questa sezione descrive i tag e mostra come crearli. AWS IoT Wireless non ha gruppi di fatturazione e utilizza gli stessi gruppi di fatturazione di AWS IoT Core. Per ulteriori informazioni, consultare Gruppi di fatturazione nella Documentazione AWS IoT Core.

Nozioni di base sui tag

In presenza di diverse risorse AWS IoT Wireless dello stesso tipo, è possibile usare i tag per categorizzare le risorse in modi diversi (ad esempio, per finalità, proprietario o ambiente). Ciò consente di identificare velocemente una risorsa in base ai tag a questa assegnati.

Ogni tag è formato da una chiave e da un valore opzionale, entrambi personalizzabili. Ad esempio, è possibile definire un set di tag per un gruppo di dispositivi LoRaWAN per i quali viene aggiornato il firmware del dispositivo. Per gestire più facilmente le risorse, è consigliabile creare un set di chiavi di tag coerente in grado di soddisfare i requisiti di ciascun tipo di risorsa.

Puoi cercare e filtrare le risorse in base ai tag che aggiungi o applichi. Puoi anche utilizzare i tag per controllare l'accesso alle risorse utilizzando le policy IAM e i tag di gruppo di fatturazione per categorizzare e monitorare i costi.

Creazione e gestione di agenti

Puoi creare e gestire i tag utilizzando il Tag Editor nella AWS Management Console, nell'AWS IoT Wireless o nella AWS CLI

Utilizzo della console

Per semplicità di utilizzo, Tag Editor nella AWS Management Console fornisce una soluzione centrale e unificata per creare e gestire i tag. Per ulteriori informazioni, consultare Utilizzo dell'editor di tag in Utilizzo della AWS Management Console.

Utilizzo dell'API o dell'interfaccia a riga di comando

Puoi anche utilizzare l'API o la CLI e associare tag a dispositivi wireless, gateway, profili e destinazioni quando li crei utilizzando il campo `Tags` nei seguenti comandi:

- AssociateAwsAccountWithPartnerAccount
- CreateDestination
- CreateDeviceProfile
- CreateFuotaTask
- CreateMulticastGroup
- CreateServiceProfile
- CreateWirelessGateway
- CreateWirelessGatewayTaskDefinition
- CreateWirelessDevice
- API_StartBulkAssociateWirelessDeviceWithMulticastGroup

Aggiornamento dei tag o elencazione dei tag per le risorse

Puoi aggiungere, modificare o eliminare i tag per le risorse esistenti che supportano il tagging utilizzando i comandi seguenti:

- TagResource
- ListTagsForResource
- UntagResource

Puoi modificare chiavi e valori di tag e rimuovere tag da una risorsa in qualsiasi momento. Puoi impostare il valore di un tag su una stringa vuota, ma non su null. Se aggiungi un tag con la stessa chiave di un tag esistente a una risorsa specifica, il nuovo valore sovrascrive quello precedente. Se elimini una risorsa, verranno eliminati anche tutti i tag associati alla risorsa.

Restrizioni e limitazioni di tag

Ai tag si applicano le seguenti limitazioni di base:

- Numero massimo di tag per risorsa: 50.
- Lunghezza massima della chiave: 127 caratteri Unicode in formato UTF-8.
- Lunghezza massima del valore: 255 caratteri Unicode in formato UTF-8.
- I valori e le chiavi dei tag rispettano la distinzione tra maiuscole e minuscole.

- Non utilizzare il prefisso `aws:` nei nomi dei tag o nei valori. Riservato per l'utilizzo da parte di AWS. Non è possibile modificare né eliminare i nomi o i valori di tag con tale prefisso. I tag con questo prefisso non vengono conteggiati per il limite del numero di tag per risorsa.
- Se lo schema di tagging viene utilizzato in più servizi e risorse, è necessario tenere presente che in altri servizi possono essere presenti limiti sui caratteri consentiti. I caratteri consentiti sono lettere, spazi e numeri rappresentabili in formato UTF-8, più i caratteri speciali + - = . _ : / @.

Utilizzo dei tag con policy IAM

Per specificare le risorse che un utente può creare, modificare o utilizzare, è possibile applicare autorizzazioni a livello di risorsa basate su tag nelle policy IAM utilizzate per le operazioni API AWS IoT Wireless. Puoi utilizzare l'elemento `Condition` (denominato anche blocco `Condition`) con i seguenti valori e chiavi di contesto di condizione in una policy IAM per controllare l'accesso dell'utente (autorizzazioni) in base ai tag della risorsa.

- Utilizza `aws:ResourceTag/`*`tag-key`*`: `*`tag-value`* per concedere o negare agli utenti operazioni su risorse con specifici tag.
- Utilizza `aws:RequestTag/`*`tag-key`*`: `*`tag-value`* per richiedere che un tag specifico venga utilizzato (o non utilizzato) durante la creazione di una richiesta API per creare o modificare una risorsa che abilita i tag.
- Utilizza `aws:TagKeys: [`*`tag-key`*`, ...]` per richiedere che un set di tag specifico venga utilizzato (o non utilizzato) durante la creazione di una richiesta API per creare o modificare una risorsa che abilita i tag.

> **Note**
>
> Le chiavi di contesto della condizione e i valori all'interno di una policy IAM si applicano solo alle operazioni AWS IoT in cui un identificatore per una risorsa in grado di essere taggata è un parametro obbligatorio. Ad esempio, l'uso di DescribeEndpoint non viene consentito o negato sulla base di valori e chiavi di contesto di condizione perché in questa richiesta non si fa riferimento a una risorsa compatibile con l'assegnazione di tag.

Per ulteriori informazioni sull'utilizzo dei tag, consulta Controllo degli accessi tramite tag nella Guida per l'utente di AWS Identity and Access Management. La sezione relativa al riferimento alle policy

JSON IAM della guida ha una sintassi dettagliata, descrizioni ed esempi di elementi, variabili e logica di valutazione delle policy JSON in IAM.

La policy di esempio seguente applica due restrizioni basate su tag. Un utente IAM limitato da questa policy:

- Non può assegnare a una risorsa il tag "env=prod" (nell'esempio, consulta la riga `"aws:RequestTag/env" : "prod"`).
- Non può modificare o accedere a una risorsa con un tag esistente "env=prod" (nell'esempio, consulta la riga `"aws:ResourceTag/env" : "prod"`).

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

È anche possibile specificare più valori di tag per una determinata chiave tag racchiudendoli in un elenco, come segue:

```
"StringEquals" : {
              "aws:ResourceTag/env" : ["dev", "test"]
}
```

> **Note**
>
> Se consenti o neghi a un utente l'accesso a risorse in base ai tag, devi considerare esplicitamente di negare agli utenti la possibilità di aggiungere o rimuovere tali tag dalle stesse risorse. In caso contrario, un utente può eludere le restrizioni e ottenere l'accesso a una risorsa modificandone i tag.

Cronologia dei documenti per la Guida per l'utente di Wireless AWS IoT

La tabella seguente descrive i release di documentazione per Wireless AWS IoT.

Modifica	Descrizione	Data
Versione iniziale	Versione iniziale della Guida per gli utenti di Wireless AWS IoT	31 dicembre 2020