Guida a Fleet Hub per la gestione dei AWS IoT dispositivi

# Fleet Hub per la gestione dei AWS IoT dispositivi

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

# Fleet Hub per la gestione dei AWS IoT dispositivi: Guida a Fleet Hub per la gestione dei AWS IoT dispositivi

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

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

# Table of Contents

# Cos'è Fleet Hub per AWS IoT Device Management?

Con Fleet Hub per AWS IoT Device Management (Fleet Hub), è possibile creare applicazioni Web autonome per monitorare lo stato dei parchi istanze dei tuoi dispositivi. È possibile rendere disponibili queste applicazioni agli utenti dell'organizzazione, anche se non dispongono di account AWS. Utilizza Fleet Hub per gestire le attività comuni a tutto il parco istanze, ad esempio indagare e risolvere i problemi operativi e di sicurezza.

Fleet Hub offre le funzionalità seguenti.

- Monitoraggio dei parchi istanze praticamente in tempo reale.
- Imposta avvisi per informare i tecnici in merito a comportamenti insoliti.
- Esecuzione di processi.

> **Note**
>
> Affinché Fleet Hub possa indicizzare i dati sullo stato di connettività, gli oggetti devono connettersi a AWS IoT Core con ID client uguale al nome dell'oggetto.

## Come funziona Fleet Hub per AWS IoT Device Management

Gli amministratori possono utilizzare Fleet Hub per AWS IoT Device Management per creare applicazioni Web sicure in pochi minuti senza provisioning di risorse o scrittura di codice. Le applicazioni Web create usando Fleet Hub si integrano con i sistemi di identità esistenti, come Active Directory. In questo modo, gli amministratori possono applicare i propri modelli di autenticazione e autorizzazione.

Le applicazioni Web Fleet Hub integrano con AWS IoT Core l'indicizzazione del parco istanze e il monitoraggio dei dispositivi. Queste integrazioni offrono la possibilità di monitorare i dati sullo stato dei dispositivi e creare allarmi quando i dispositivi del parco istanze raggiungono uno stato specifico.

Le applicazioni Fleet Hub utilizzano la policy gestita da `AWSIoTFleetHubFederationAccess`. Per ulteriori informazioni, consulta ???.

Casi d'uso di esempio:

- Visualizzazione dei problemi di connettività dei dispositivi: è possibile visualizzare il numero di dispositivi disconnessi nel parco istanze, lo stato dell'ultimo collegamento di un dispositivo e il motivo o i motivi per cui i dispositivi si sono disconnessi.
- Impostazione di allarmi: puoi impostare soglie che attivano allarmi quando un determinato numero di dispositivi si disconnette. Gli allarmi possono anche avvisarti quando uno o più dispositivi si disconnettono per un motivo specifico. Puoi quindi esaminare i dati dettagliati sui dispositivi per indagare sul problema e risolverlo.
- Esegui processi - È possibile eseguire operazioni remote (come gli aggiornamenti del firmware) su uno o più dispositivi.

## Come funziona l'indicizzazione dei dati Fleet Hub

Puoi usare la console Fleet Hub per attivare l'indicizzazione del parco istanze per il parco istanze del tuo dispositivo. Quando attivi l'indicizzazione della parco istanze in Fleet Hub, la attivi per l'intero parco istanze e la rendi disponibile per tutte le applicazioni di Fleet Hub.

Quando è abilitata, l'indicizzazione del parco istanze indicizza tutti i campi gestiti da AWS IoT Core automaticamente. È inoltre possibile utilizzare l'indicizzazione del parco istanze per aggiungere dati personalizzati che è possibile utilizzare per eseguire query e aggregare i dati nelle applicazioni Fleet Hub.

## Funzionamento degli allarmi Fleet Hub

Le applicazioni Web Fleet Hub offrono un'interfaccia che permette agli utenti di creare allarmi. I passaggi seguenti mostrano in che modo gli utenti possono creare allarmi in Fleet Hub.

1. Crea una query per aggregare i dati: specifica una query che aggreghi i dispositivi che gli utenti desiderano assegnare utilizzando campi ricercabili.
2. Configurazione della soglia: puoi impostare una soglia che attiva gli allarmi quando viene raggiunta una condizione nei dati indicizzati, ad esempio lo stato di connettività in un intervallo specificato.
3. Configura notifica: specifica un gruppo di destinatari a cui Fleet Hub notifica quando i dispositivi specificati sono in allarme.

## Come funzionano i processi Fleet Hub

Puoi usare la console Fleet Hub per eseguire operazioni remote sui dispositivi.

Quando sono abilitati i modelli di processo, puoi creare processi specifici dai modelli nelle applicazioni Fleet Hub.

# Fleet Hub per la gestione dei AWS IoT dispositivi per amministratori

Questa sezione contiene linee guida per gli amministratori su come creare e gestire le applicazioni web Fleet Hub for AWS IoT Device Management.

Argomenti



## Nozioni di base

Questa sezione spiega come creare e configurare le applicazioni web Fleet Hub per la gestione dei AWS IoT dispositivi.

Argomenti



### Creazione della prima applicazione Fleet Hub

#### Prerequisiti

L'elenco seguente contiene le risorse necessarie per creare un'applicazione web Fleet Hub.

- Un account AWS.
- AWS IAM Identity Center attivato sull'account. (Se non hai ancora provveduto, la console AWS IoT Core (https://console.aws.amazon.com/iot/) ti chiederà di attivare il servizio.)

#### Creazione della prima applicazione Web Fleet Hub

I passaggi seguenti descrivono come creare applicazioni web Fleet Hub per la gestione dei AWS IoT dispositivi.

1. Vai alla AWS IoT Core console (https://console.aws.amazon.com/iot/) e, nel pannello di sinistra, scegli Fleet Hub, quindi Applicazioni.
2. Nella pagina Applicazioni, scegli Create application (Crea applicazione).
3. Nella pagina Configura IAM Identity Center, se non l'hai attivato AWS IAM Identity Center (IAM Identity Center), segui i passaggi per attivarlo. AWS Organizations ti invia un'e-mail. Fai clic sul collegamento contenuto nell'e-mail per completare l'attivazione di IAM Identity Center.

   > **Note**
   >
   > È possibile collegare a IAM Identity Center il proprio provider di identità. Per ulteriori informazioni, consulta Cos'è AWS IAM Identity Center? e Connect al tuo provider di identità esterno.
   > Quando crei un'applicazione Fleet Hub, devi creare un'istanza organizzativa di IAM Identity Center se non ne hai già una. L'applicazione Fleet Hub che crei deve inoltre trovarsi nella stessa Regione AWS istanza organizzativa di IAM Identity Center. Per ulteriori informazioni, consulta Abilitazione delle istanze di IAM Identity Center e Organization of IAM Identity Center.

   La pagina indica se IAM Identity Center è già attivato.

   Seleziona Successivo.
4. Nella pagina  AWS IoT dei dati dell'indice, consulta le informazioni nella sezione Come funziona il flusso di dati da AWS IoT a Fleet Hub. Questa pagina ti collega alle pagine della AWS IoT Core console in cui puoi attivare e gestire l'indicizzazione del AWS IoT Core parco veicoli. Puoi usare questo servizio per indicizzare, ricercare e aggregare i dati di registro, i dati shadow, i dati di connettività del dispositivo (eventi del ciclo di vita del dispositivo) e i dati di violazione del dispositivo. Puoi anche creare campi personalizzati oltre ai campi gestiti che per impostazione predefinita vengono indicizzati dagli indici di indicizzazione del AWS IoT Core parco veicoli.

   - Se hai attivato l'indicizzazione del parco istanze, questa pagina visualizza le impostazioni di indicizzazione del parco istanze e i campi personalizzati.

   - Per utilizzare Fleet Hub è necessario abilitare l'indicizzazione e la connettività degli oggetti.

Al termine della gestione e della revisione delle impostazioni di indicizzazione del parco istanze, scegli Next (Successivo).

Per ulteriori informazioni su come attivare l'indicizzazione del parco istanze per le applicazioni Fleet Hub, consulta Gestione dell'indicizzazione del parco istanze per le applicazioni Fleet Hub.

5. Nella pagina Configure application (Configura l'applicazione), nella sezione Application role (Ruolo dell'applicazione), crea un nuovo ruolo di servizio o seleziona un ruolo di servizio esistente. L'applicazione web Fleet Hub assume questo ruolo quando utilizza le risorse di Fleet Hub. Gli utenti federati dispongono delle stesse autorizzazioni del ruolo quando utilizzano l'applicazione web.

   - Se si crea un nuovo ruolo, il nome del ruolo deve iniziare con la stringa seguente: `AWSIotFleetHub_`*`random_string`*.

   - Se selezioni un ruolo esistente, assicurati che disponga delle autorizzazioni presenti nel documento di policy. Per visualizzare le autorizzazioni necessarie all'applicazione web Fleet Hub, scegli View role details (Visualizza i dettagli del ruolo). Si apre una finestra che mostra il documento di policy che il servizio applica a qualsiasi nuovo ruolo creato da questa pagina.

6. Nella pagina Configure application (Configura l'applicazione), nella sezione Application properties (Proprietà dell'applicazione), inserisci un nome per la tua applicazione. In maniera facoltativa, è anche possibile inserire una descrizione dell'applicazione.

   Scegli Crea applicazione.

7. Nella pagina Applications (Applicazioni), seleziona l'applicazione creata e quindi scegli View details (Visualizza dettagli). Rivedi i dettagli dell'applicazione.

> **Note**
>
> Per ulteriori informazioni su eventuali soluzioni utili a risolvere i problemi in qualità di amministratore di Fleet Hub, consulta la sezione Risoluzione dei problemi.

# Gestione dell'indicizzazione del parco istanze per le applicazioni Fleet Hub

Puoi utilizzare la AWS IoT Core console o attivare l' AWS CLI indicizzazione del parco veicoli e configurare le seguenti fonti di dati da indicizzare: dati di AWS IoT registro, dati AWS IoT Device Shadow, dati di AWS IoT connettività e dati AWS IoT Device Defender sulle violazioni. I passaggi seguenti descrivono come attivare l'indicizzazione del parco veicoli per le applicazioni Fleet Hub for AWS IoT Device Management nella console. AWS IoT Core Per visualizzare i passaggi di utilizzo AWS CLI, vedi Gestione dell'indicizzazione degli oggetti.

> **Important**
>
> Il 20 luglio 2022 è disponibile la versione General Availability dell'integrazione di AWS IoT Device Management fleet indexing con AWS IoT Core named shadows e rilevamento delle violazioni. AWS IoT Device Defender Con questo rilascio pubblico, potrai indicizzare copie shadow denominate specificando i nomi delle copie shadow. Se hai aggiunto le tue copie shadow nominate per l'indicizzazione durante il periodo di anteprima pubblica di questa funzione, ovvero dal 30 novembre 2021 al 19 luglio 2022, ti invitiamo a riconfigurare le impostazioni di indicizzazione del parco istanze e scegliere nomi di copie shadow specifici per ridurre i costi di indicizzazione e ottimizzare le prestazioni. Per ulteriori informazioni su come riconfigurare le impostazioni di indicizzazione del parco istanze, consulta Gestione dell'indicizzazione del parco istanze.

1. Vai alla AWS IoT Core console (https://console.aws.amazon.com/iot/) e, nel pannello a sinistra, scegli Impostazioni.
2. Nella pagina Settings (Impostazioni), scorri fino alla sezione Fleet indexing (Indicizzazione del parco istanze), quindi scegli Manage indexing (Gestisci indicizzazione).
3. Nella pagina Gestisci l'indicizzazione del parco veicoli, nella sezione Configurazione, scegli Indicizzazione degli oggetti e le fonti di dati che desideri indicizzare. AWS IoT Per utilizzare Fleet Hub, è necessario abilitare l'indicizzazione e la connettività degli oggetti.
4. (Facoltativo) Nella pagina Manage fleet indexing (Gestisci indicizzazione del parco istanze), nella sezione Custom search fields-optional (Campi di ricerca personalizzati - facoltativo), crea campi personalizzati in aggiunta ai campi gestiti che vengono indicizzati di default.

   Al termine della gestione e della revisione delle impostazioni di indicizzazione del parco istanze, scegli Next (Successivo).

L'indicizzazione del parco istanze può richiedere un po' di tempo per aggiornare le impostazioni. Per ulteriori informazioni sull'indicizzazione del parco istanze, consulta Managing fleet indexing (Gestione indicizzazione del parco istanze).

## Aggiunta di utenti alle applicazioni Fleet Hub

La tua applicazione web Fleet Hub for AWS IoT Device Management non contiene utenti quando è stata appena creata. È necessario aggiungere utenti prima che tu e i membri dell'organizzazione possiate utilizzare l'applicazione. I passaggi in questo argomento descrivono come aggiungere utenti alla tua applicazione.

Aggiungi utenti dal tuo sistema di identità esistente configurando AWS IAM Identity Center (IAM Identity Center) per il tuo account. È possibile collegare a IAM Identity Center il proprio provider di identità. Per ulteriori informazioni, consulta Cos'è IAM Identity Center?.

1. Sulla pagina Applications (Applicazioni), scegli l'applicazione Web dall'elenco Fleet Hub applications (Applicazioni Fleet Hub). Seleziona Visualizza dettagli.
2. Nella pagina dei dettagli dell'applicazione, scegli Add user (Aggiungi utente).
3. Nella finestra Add Fleet Hub users (Aggiungi utenti Fleet Hub), seleziona gli utenti dell'organizzazione che desideri abbiano accesso all'applicazione. Scegli Add selected users (Aggiungi gli utenti selezionati).
4. Nella pagina dei dettagli dell'applicazione, verifica che siano visualizzati gli utenti selezionati nell'elenco Fleet Hub users (Utenti Fleet Hub).

# I servizi AWS e AWS IoT Core che interagiscono con Fleet Hub for AWS IoT Device Management

In questo argomento viene illustrato come le funzionalità di Fleet Hub per la gestione dei dispositivi AWS IoT interagiscono con altri servizi AWS per fornire le funzionalità nelle applicazioni web Fleet Hub.

La seguente tabella indica i servizi utilizzati da AWS Fleet Hub per la gestione dei dispositivi AWS IoT per implementare ciascuna funzionalità.

| Funzionalità | Servizio AWS | Descrizione |
| --- | --- | --- |
| Integra i sistemi di identità esistenti, come Active Directory. | AWS IAM Identity Center (IAM Identity Center) | È possibile aggiungere utenti dal sistema di identità esistente impostando AWS IAM Identity Center (IAM Identity Center) per il proprio account. È possibile collegare a IAM Identity Center il proprio provider di identità.<br><br>Per ulteriori informazioni, consulta Cos'è AWS IAM Identity Center? e Identità della forza lavoro. |
| Crea query utilizzando campi gestiti da AWS, campi personalizzati e qualsiasi attributo nelle origini dati indicizzate. | Indicizzazione del parco istanze AWS IoT | Utilizza il servizio di indicizza zione del parco istanze per indicizzare, ricercare e aggregare i dati di registro, i dati shadow e i dati di connettività del dispositivo (eventi del ciclo di vita del dispositivo). Inoltre, puoi creare campi personalizzati per l'aggregazione oltre ai campi gestiti che l'indiciz zazione del parco istanze AWS IoT indicizza per impostazione predefinita.<br><br>Per ulteriori informazioni sull’indicizzazione del parco istanze, consulta Fleet indexing (Indicizzazione del parco istanze). |

| Funzionalità | Servizio AWS | Descrizione |
| --- | --- | --- |
| Creazione di allarmi per un set di dispositivi specificati da una query. | Amazon CloudWatch (CloudWatch) | I pannelli di controllo di Fleet Hub espongono i parametri CloudWatch che puoi usare in combinazione con campi ricercabili per creare soglie allarmanti. Ad esempio, puoi creare allarmi CloudWatch che generano una notifica Amazon Simple Notification Service (Amazon SNS) ogni volta che il numero di dispositi vi collegati scende al di sotto di una quantità specificata.<br><br>Per ulteriori informazioni su CloudWatch, consulta Che cos'è Amazon CloudWatch? Per ulteriori informazioni su come funziona AWS IoT Core con CloudWatch per creare parametri e allarmi, consulta Monitora allarmi e parametri AWS IoT con CloudWatch. |

# Risoluzione dei problemi

Questa sezione fornisce informazioni sulla risoluzione dei problemi e su possibili soluzioni per aiutare a risolvere i problemi in qualità di amministratore di Fleet Hub.

| Caratteristiche | Soluzione |
| --- | --- |
| Il collegamento dell'applicazione web non funziona. | Potrebbero essere necessarie alcune ore dopo la creazione dell'applicazione affinché il collegamento funzioni. |

| Caratteristiche | Soluzione |
| --- | --- |
| Non riesco ad accedere alla mia applicazione Web. | Assicurati di avere aggiunto almeno un utente all'applicazione.<br><br>Assicurati che il tuo ruolo abbia una relazione di trust appropriata come la seguente:<br><br>`{"Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "iotfleethub.amazonaws.com" }, "Action": "sts:AssumeRole" } ] }`<br><br>Per ulteriori informazioni su come modificare la relazione di attendibilità IAM, consulta Modifica della relazione di trust per un ruolo esistente. |
| Non riesco a creare un'applicazione web. | Assicurati di non aver raggiunto il limite del numero totale di applicazioni web. |
| Non vedo il campo personalizzato che mi aspettavo. | Verifica di aver configurato correttamente l'indicizzazione del parco istanze.<br><br>Per ulteriori informazioni sull'indicizzazione del parco istanze, consulta Fleet indexing (Indicizzazione del parco istanze). |

# Fleet Hub per gli utenti di AWS IoT Device Management

Questa sezione contiene informazioni per gli utenti di Fleet Hub per le applicazioni web AWS IoT Device Management. Per informazioni sulla creazione di applicazioni Fleet Hub e sull'aggiunta di utenti, consulta Fleet Hub per la gestione dei AWS IoT dispositivi per amministratori.

Argomenti



## Nozioni di base

Questa sezione contiene informazioni su come iniziare a utilizzare le funzionalità di Fleet Hub per le applicazioni web AWS IoT Device Management.

Argomenti



### Creazione della prima query

Questo argomento descrive le diverse fasi per creare un semplice Fleet Hub per query AWS IoT Device Management. Le query vengono specificate tramite una sintassi di query.

#### Prerequisiti

- Un'applicazione Fleet Hub associata a un account AWS IoT Core che contiene dispositivi (oggetti).
- Un account dell'organizzazione che dispone delle autorizzazioni per utilizzare l'applicazione Fleet Hub.

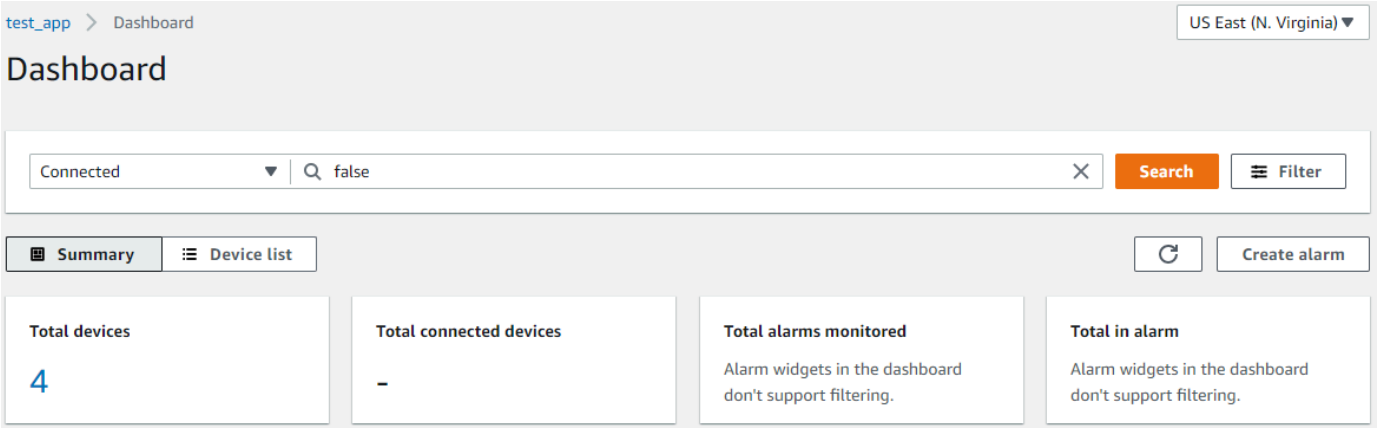
## Crea la prima query di Fleet Hub

Crea la prima query di Fleet Hub

1. Passa all'applicazione Fleet Hub.

   La modalità di visualizzazione di default del pannello di controllo mostra un elenco di tutti i dispositivi che contengono gli attributi gestiti e personalizzati. Gli attributi che contengono il prefisso attributi sono attributi personalizzati.

2. Nel menu nella parte superiore della pagina, scegli Connected (Connesso) da All fields (Tutti i campi). Inserisci **`false`** nella casella di testo accanto al menu a discesa.




3. Per eseguire la ricerca, scegli Cerca. Viene visualizzato un elenco di tutti i dispositivi non connessi a AWS IoT Core.

Per ulteriori informazioni sulla sintassi delle query e sulle query di esempio, consulta Sintassi delle query, Esempio di query per oggetti e Esempio di query per gruppi di oggetti.

# Creazione del primo allarme

Questo argomento descrive le diverse fasi per creare un semplice allarme di Fleet Hub per AWS IoT Device Management.

## Prerequisiti

- Un'applicazione Fleet Hub associata a un account AWS IoT Core che contiene dispositivi (oggetti).
- Un account dell'organizzazione che dispone delle autorizzazioni per utilizzare l'applicazione Fleet Hub.

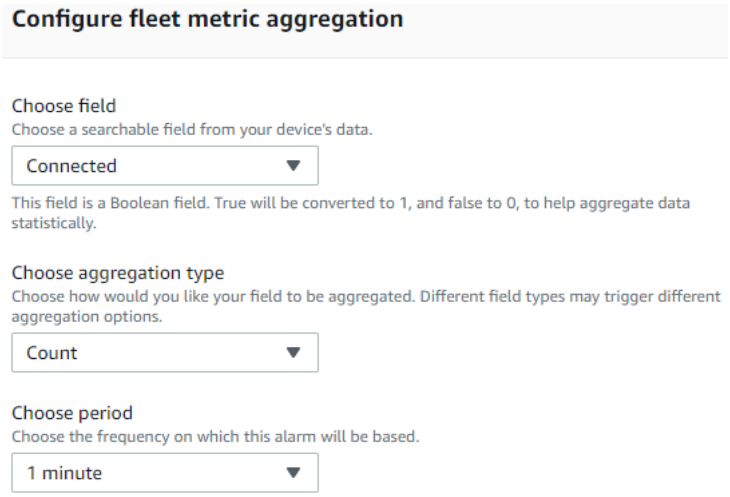
# Creazione del primo allarme

Crea il primo allarme di Fleet Hub

1. Passa all'applicazione Fleet Hub.
2. Se desideri assegnare un determinato set di dispositivi, crea una query. Per istruzioni su come creare una query semplice, consulta the section called “Creazione della prima query”. Se non crei una query, l'allarme verrà applicato a tutti i dispositivi del tuo parco istanze.
3. Nella pagina predefinita del dashboard, scegli Create alarm (Creazione di allarme).
4. Sulla pagina Build aggregation metric (Creazione di parametri di aggregazione), verifica che la query venga visualizzata in Target query (Query di destinazione). Nella sezione Configure fleet metric aggregation (Configurazione dell'aggregazione di parametri del parco istanze), nel menu Choose field (Scegli campo), scegli Connected (Connesso). Questo campo gestito da AWS indica se un dispositivo è connesso ad AWS IoT Core. Il menu Choose field (Scegli campo) contiene i campi gestiti da AWS e i campi personalizzati creati dall'amministratore nell'indicizzazione del parco istanze AWS IoT.
5. Per Choose aggregation type (Scegli il tipo di aggregazione), scegli una delle seguenti opzioni.

   - Massimo – Configura una soglia massima.
   - Conteggio – Configura un conteggio specifico come soglia.
   - Somma – Configura una somma come soglia.
   - Minimo – Configura una soglia minima.
   - Media – Configura una soglia media.
6. Per Choose period (Scegliere il periodo), scegli la durata della condizione specificata nei menu precedenti che attiverà l'allarme.

   Un'impostazione di esempio per Configure fleet metric aggregation (Configura l'aggregazione dei parametri del parco istanze) può avere un aspetto simile al seguente:



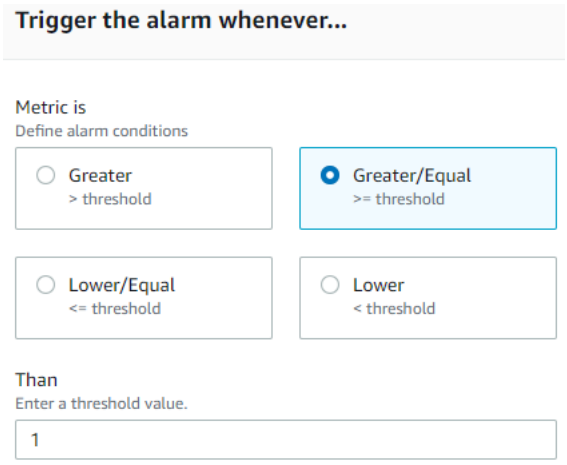

Seleziona Successivo.

7. Sulla pagina Set threshold (Imposta soglia), nella sezione Trigger the alarm whenever... (Attiva l'allarme ogni volta che...), scegli una delle seguenti opzioni.

   - Maggiore – Allarmi quando il parametro e il tipo di aggregazione superano il valore specificato.
   - Maggiore/Uguale – Allarmi quando il parametro di aggregazione e il tipo sono uguali o superiori al valore specificato.
   - Minore – Allarmi quando il parametro e il tipo di aggregazione sono inferiori al valore specificato.
   - Minore/Uguale – Allarmi quando il parametro di aggregazione e il tipo sono uguali o inferiori al valore specificato.

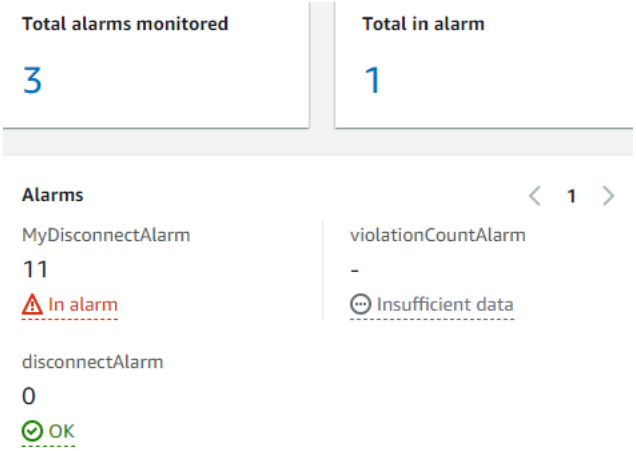
8. Nella casella di ricerca Than, specifica il valore da utilizzare come soglia per l'allarme.

   Un'impostazione di esempio per Set threshold (Imposta soglia) può avere un aspetto simile al seguente:

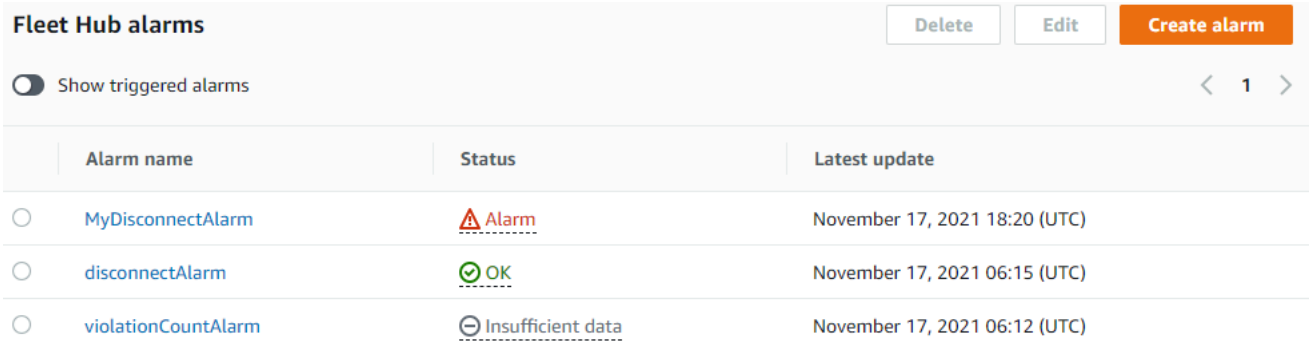


Seleziona Successivo.

9. Sulla pagina Notify user (Notifica all'utente), nella sezione Notify — optional (Notifica – facoltativo), immetti un nome per l'elenco di posta elettronica contenente gli utenti dell'organizzazione che ricevono notifiche quando l'allarme è attivo. Immetti un elenco separato da virgole di indirizzi email per popolare questo elenco.
10. Nella sezione Alarm details (Dettagli allarme), immetti un nome per il tuo allarme e, facoltativamente, inserisci una descrizione per il tuo allarme. Seleziona Successivo.
11. Nella pagina Review (Revisione) esamina le informazioni immesse o selezionate nelle pagine precedenti. Scegli Submit (Invia). Torna al dashboard predefinito.
12. Nel pannello di controllo di default, i widget degli allarmi mostrano le informazioni su tutti gli allarmi creati.




Per visualizzare i dettagli degli allarmi creati, nel pannello di navigazione a sinistra, scegli Fleet Hub alarms (Allarmi di Fleet Hub).



# Visualizzazione dei dettagli del dispositivo

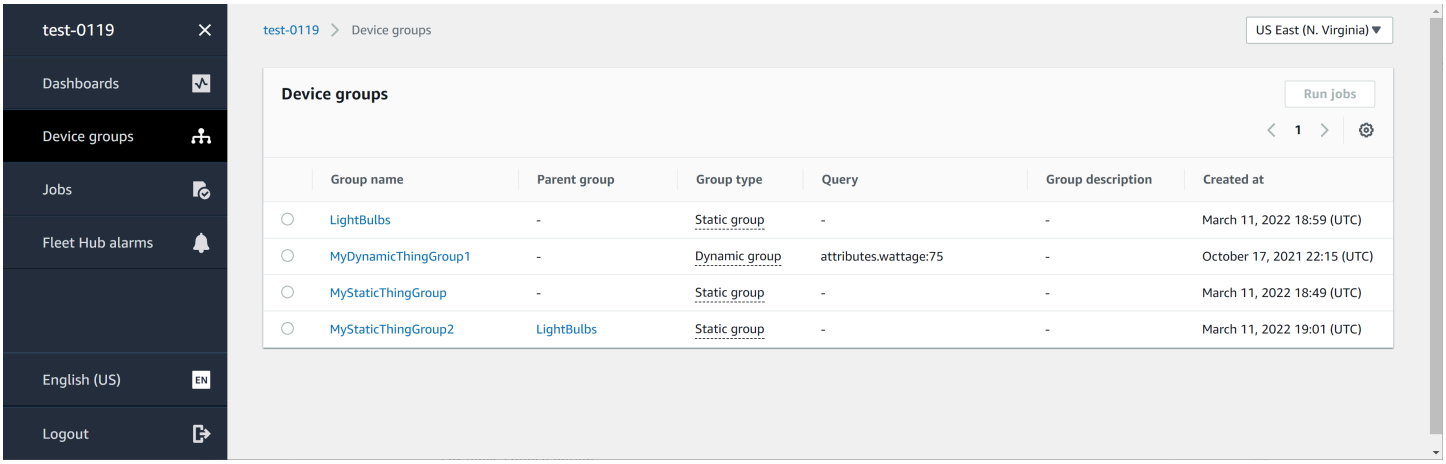
Questo argomento descrive le diverse fasi per visualizzare i dettagli dei gruppi di dispositivi e dei dispositivi.

## Prerequisiti

- Un'applicazione Fleet Hub associata a un account AWS IoT Core che contiene dispositivi (oggetti).
- Un account dell'organizzazione che dispone delle autorizzazioni per utilizzare l'applicazione Fleet Hub.

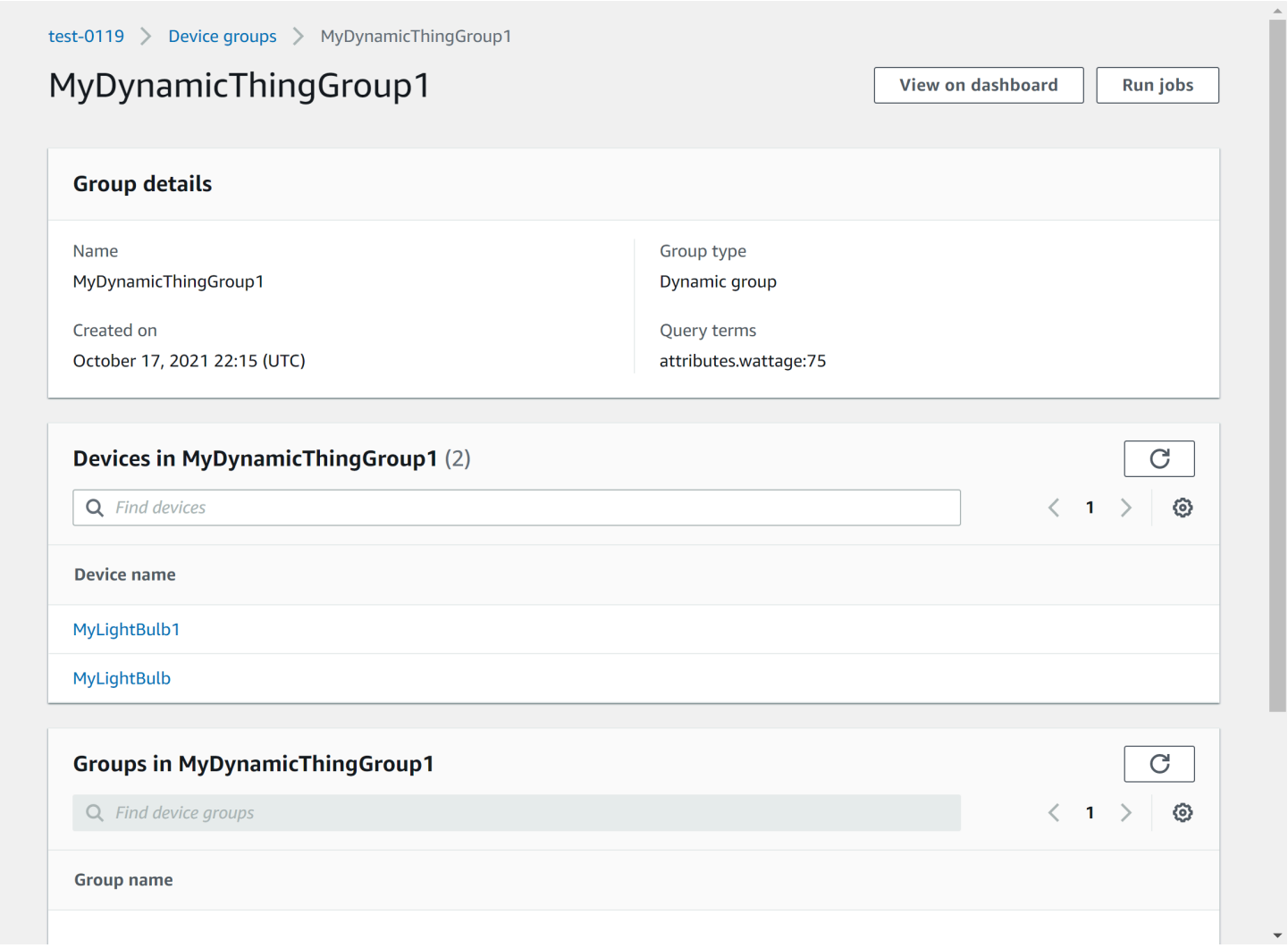
## Gruppi di dispositivi

Quando accedi alla tua applicazione Web Fleet Hub, vengono visualizzati Device groups (Gruppi di dispositivi) sul pannello di navigazione a sinistra. La pagina Device groups (Gruppi di dispositivi) elenca tutti i gruppi di dispositivi dell'applicazione Web Fleet Hub. Per visualizzare i dettagli di un gruppo di dispositivi, scegli un gruppo di dispositivi specifico dalla colonna Group name (Nome gruppo).




## Dettagli del gruppo di dispositivi

La pagina Device group details (Dettagli del gruppo di dispositivi) contiene le informazioni sul gruppo di dispositivi selezionato. Per visualizzare i dettagli di un dispositivo, scegli un dispositivo specifico dalla colonna Device name (Nome dispositivo) della sezione Devices in ***XXX*** (Dispositivi in XXX).




## Dettagli del dispositivo

La pagina Device details (Dettagli del dispositivo) contiene informazioni sul dispositivo selezionato.

> **Note**
>
> Se il tuo client utilizza un ID client diverso da quello di Thing Name durante la connessione a AWS IoT, lo stato della connettività del tuo "oggetto" non verrà indicizzato da Fleet Indexing.

### Informazioni

La sezione Details (Dettagli) contiene le seguenti informazioni sul dispositivo:

- Device name (Nome dispositivo): il nome della risorsa oggetto che rappresenta il dispositivo. Per ulteriori informazioni, consulta Come gestire gli oggetti con il registro.

- Thing type (Tipo di oggetto): il tipo di oggetto associato al tuo dispositivo. Puoi utilizzare il tipo di oggetto per archiviare le informazioni comuni a tutti gli oggetti dello stesso tipo. Per ulteriori informazioni, consulta Tipi di oggetti.

- Last connection timestamp (Timestamp dell'ultima connessione): il timestamp dell'ultima connessione del dispositivo a AWS IoT.

- Shareable device link (Collegamento condivisibile del dispositivo): il collegamento condivisibile che punta alla pagina Device details (Dettagli del dispositivo) del dispositivo selezionato.

- Last connection status (Stato dell'ultima connessione): lo stato della connessione del dispositivo a AWS IoT. Se il dispositivo è connesso, il valore è `true`. Se non è connesso, il valore è `false`.

- Disconnect reason (Motivo di disconnessione): il motivo per cui il dispositivo è stato disconnesso.

Dati segnalati

La sezione Reported data (Dati segnalati) contiene informazioni sui dati del registro di sistema del dispositivo, sui dati Device Shadow e sui gruppi di oggetti.

- Device fields (Campi del dispositivo): i campi del tuo dispositivo indicizzati nell'indicizzazione del parco istanze AWS IoT. Per ulteriori informazioni, consulta Servizio Managing fleet indexing (Gestione dell'indicizzazione del parco istanze).

- Device shadows (Device Shadow): le Device Shadow associate al tuo dispositivo. Le Device Shadow possono includere sia le classiche copie shadow senza nome che quelle con nome. Per ulteriori informazioni, consulta AWS IoT Servizio Device Shadow.

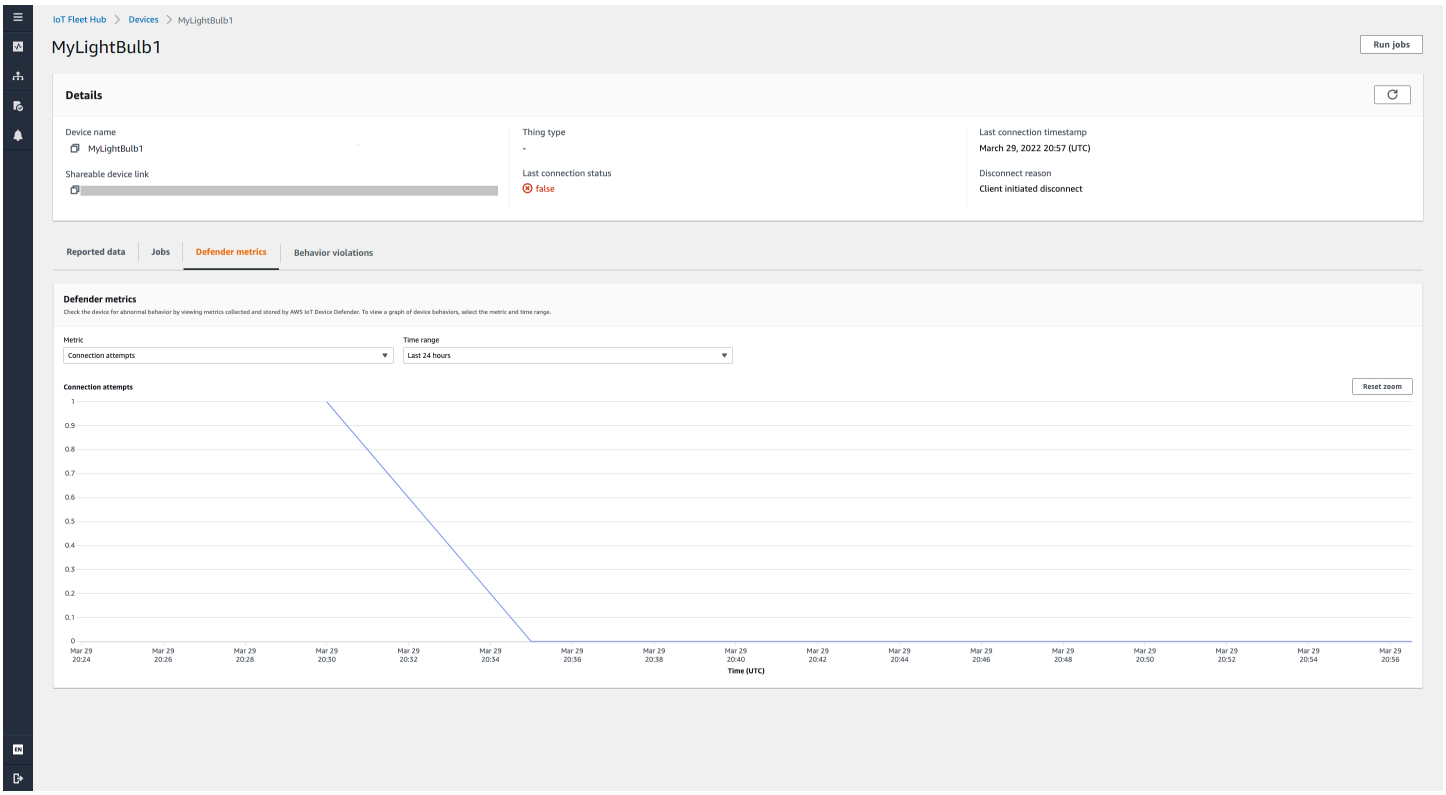
- Device groups (Gruppi di dispositivi): i gruppi di dispositivi associati al tuo dispositivo. I gruppi di dispositivi possono includere gruppi di oggetti statici e dinamici. Per ulteriori informazioni, consulta Gruppi di oggetti statici e Gruppi di oggetti dinamici.

### Processi

La sezione Jobs (Processi) mostra tutti i processi in esecuzione sul dispositivo. Ogni processo dispone di una pagina dei dettagli che visualizza informazioni di riepilogo sul processo, incluse le informazioni sulla destinazione e sul runtime. Per ulteriori informazioni, consulta Utilizzo di processi e modelli di processi in Fleet Hub per AWS IoT Device Management e Processi.

### Parametri di Defender

La sezione Defender metrics (Parametri di Defender) visualizza i parametri di AWS IoT Device Defender associati al dispositivo attualmente selezionato. Puoi utilizzare i dati dei parametri visualizzati per osservare il funzionamento del dispositivo in un intervallo di tempo scelto. Per visualizzare i dati dei parametri di Defender dall'applicazione Fleet Hub, l'amministratore di Fleet Hub deve prima configurare i parametri AWS IoT Device Defender associati al dispositivo selezionato. Per ulteriori informazioni su come creare e configurare i parametri AWS IoT Device Defenderper i tuoi dispositivi, consulta Parametri personalizzati, Parametri sul lato dispositivo e Parametri sul lato cloud.




### Violazioni di comportamento

La sezione Behavior violations (Violazioni di comportamento) visualizza i dati delle violazioni rilevati AWS IoT Device Defender indicizzati associati al dispositivo attualmente selezionato. I dati delle violazioni di comportamento possono includere il conteggio delle violazioni, l'ora dell'ultima

violazione e il valore del parametro dell'ultima violazione. Per visualizzare i dati delle violazioni di comportamento dall'applicazione Fleet Hub, l'amministratore di Fleet Hub deve configurare le violazioni di comportamento AWS IoT Device Defender in un profilo di sicurezza e configurare le violazioni AWS IoT Device Defender nell'indicizzazione del parco istanze. Per ulteriori informazioni su come configurare le violazioni di comportamento in un profilo di sicurezza AWS IoT Device Defender, consulta Rilevamento AWS IoT Device Defender. Per ulteriori informazioni su come configurare le violazioni AWS IoT Device Defender, consulta Gestione dell'indicizzazione del parco istanze per le applicazioni Fleet Hub e Gestione dell'indicizzazione degli oggetti.

# Query e filtri

È possibile utilizzare Fleet Hub per le query di AWS IoT Device Management per creare e visualizzare elenchi di oggetti nel parco istanze del dispositivo. Tutti i campi gestiti da AWS, i campi personalizzati e gli eventuali attributi nelle origini dati indicizzate sono disponibili come filtri di query. Inoltre, puoi creare campi personalizzati per attivare l'aggregazione per the section called “Allarmi” utilizzando il servizio di indicizzazione del parco istanze di AWS IoT. Per ulteriori informazioni sull'indicizzazione del parco istanze, consulta Fleet indexing (Indicizzazione del parco istanze).

Argomenti

- Visualizzazione del pannello di controllo
- Creazione di query con filtri

## Visualizzazione del pannello di controllo

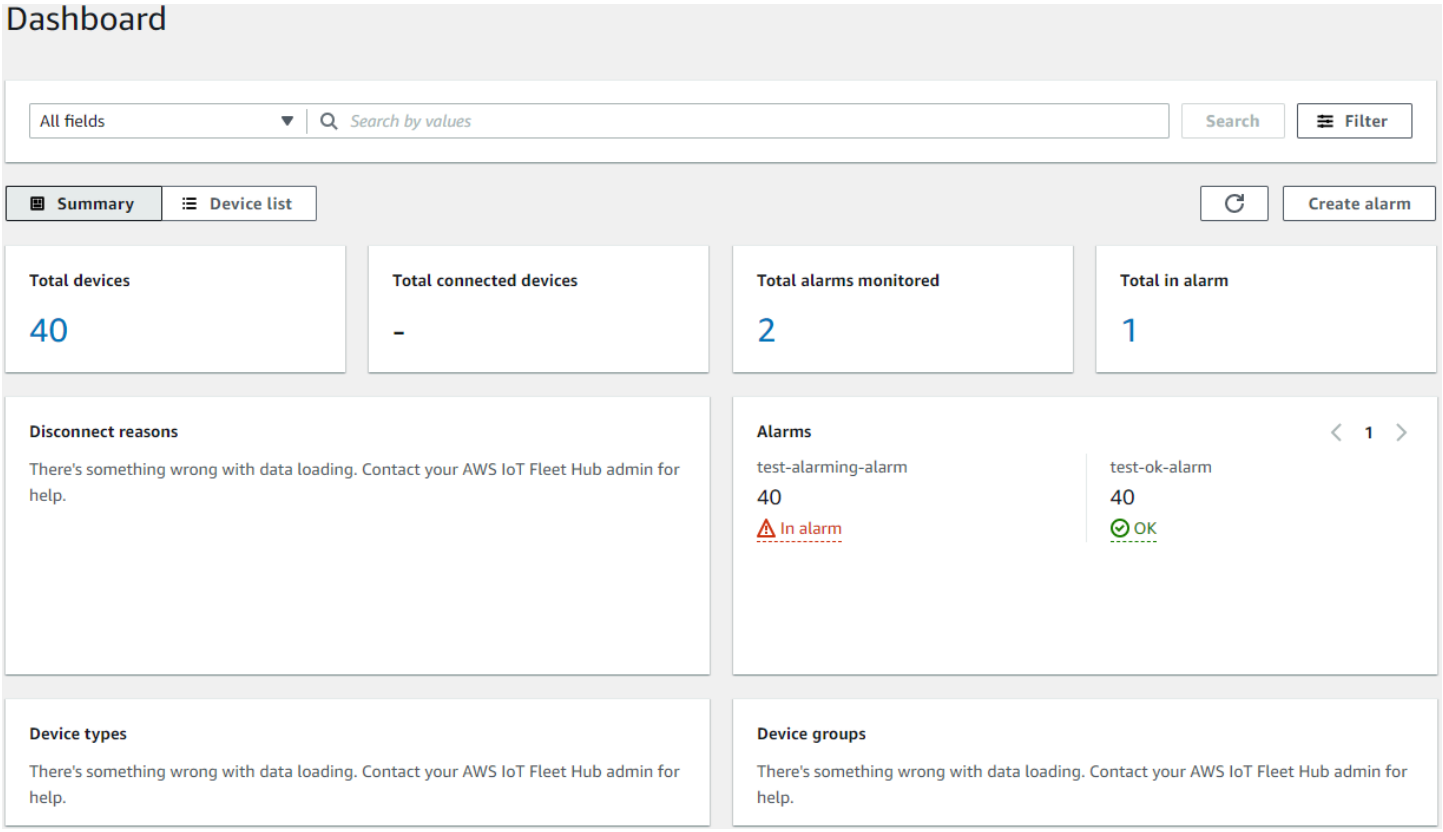
Quando accedi al tuo Fleet Hub per le applicazioni web di AWS IoT Device Management, viene visualizzato un dashboard che presenta due visualizzazioni dei dati sui dispositivi del parco istanze.

### Riepilogo

La modalità di visualizzazione summary (riepilogo) mostra una visualizzazione aggregata dei dati relativi a tutti i dispositivi del parco istanze. Il file fornisce le informazioni seguenti.

- Numero totale dei dispositivi
- Numero di dispositivi connessi
- Un elenco dei motivi per cui i dispositivi si sono disconnessi

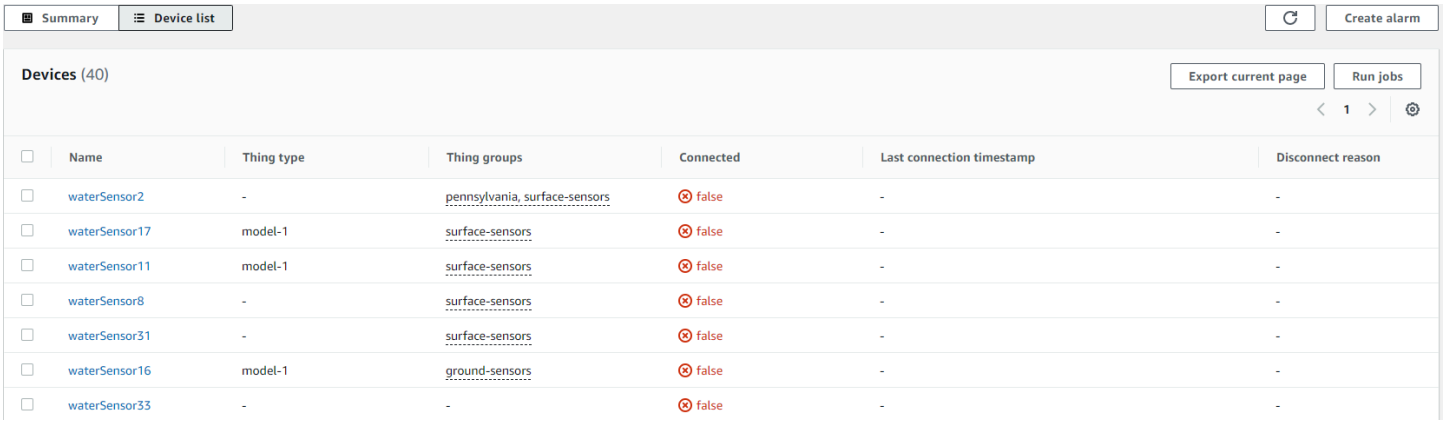
- I tipi di oggetto che hai creato per il tuo parco istanze e il numero di dispositivi per ogni tipo
- I gruppi di oggetti che hai creato per il tuo parco istanze e il numero di dispositivi in ogni gruppo




## Un elenco dispositivi

La modalità di visualizzazione Device list (Elenco dispositivi) mostra una tabella che elenca i dispositivi del parco istanze. La tabella fornisce le seguenti informazioni per ogni dispositivo dell'elenco.

- Il nome del dispositivo
- Stato di connessione del dispositivo
- Il timestamp per l'ultima connessione del dispositivo
- Per un dispositivo non connesso, il motivo per cui è stato disconnesso
- Il tipo di oggetto del dispositivo
- Il gruppo di oggetto del dispositivo
- I campi personalizzati creati nel servizio di indicizzazione del parco istanze




Per scaricare un file CSV contenente i dispositivi visualizzati nella pagina, nell'elenco dei dispositivi, scegli Esporta pagina corrente. Nota che, se l'elenco è impaginato, vengono scaricati solo i dati visualizzati nella pagina corrente, non nelle pagine successive.

È possibile utilizzare query e filtri per limitare il numero di dispositivi che generano i dati di riepilogo nella prima modalità di visualizzazione e che vengono mostrati nell'elenco dei dispositivi. Per ulteriori informazioni sull'utilizzo di query e filtri per ottenere informazioni più specifiche sui dispositivi del parco istanze, consulta the section called “Creazione di query”.

## Creazione di query con filtri

In questo argomento viene illustrato come funziona Fleet Hub per le query di AWS IoT Device Management e vengono descritte le operazioni necessarie per creare una query con filtri.

È possibile controllare il numero e i tipi di dispositivi visualizzati nelle visualizzazioni di riepilogo e l’elenco delle visualizzazioni utilizzando le query. Per filtrare le query, utilizza campi gestiti da AWS, campi personalizzati e qualsiasi attributo delle origini dati indicizzate del servizio di indicizzazione del parco istanze di AWS IoT. Per ulteriori informazioni sull’indicizzazione del parco istanze, consulta Fleet indexing (Indicizzazione del parco istanze).

Puoi anche aggiungere parole chiave alle query. Le parole chiave si applicano a tutti i campi ricercabili. Costituiscono uno svantaggio in virtù del limite di tre filtri che è possibile applicare in una singola query.

Nella sezione seguente vengono descritti i passaggi necessari per creare una query tipica.

### Creazione di query

La procedura che segue descrive come creare una query tipica.

### Prerequisiti

- Un'applicazione Fleet Hub legata a un account AWS IoT Core che contiene diversi dispositivi (oggetti)
- Un account che dispone delle autorizzazioni per utilizzare l'applicazione Fleet Hub

### Crea la tua prima query Fleet Hub con un filtro nella console

1. Passa all'applicazione Fleet Hub.
2. Nel dashboard predefinito, verifica che sia possibile visualizzare la scheda Device list (Elenco dispositivi) e il numero totale di dispositivi (oggetti) nell'account AWS IoT Core associato.

   Il pannello di controllo di default contiene le schede di navigazione, inclusa una contenente l'elenco dei dispositivi. Esso visualizza il numero totale di dispositivi nell’account AWS IoT Core associato e il numero totale di dispositivi connessi.
3. Nel pannello di controllo predefinito, scegli la scheda Device list (Elenco dispositivi). Verifica di visualizzare un elenco di tutti i dispositivi che contengono gli attributi gestiti e personalizzati. Gli attributi personalizzati contengono il prefisso degli attributi.

   Per impostazione predefinita, nel dashboard dell'elenco dei dispositivi vengono visualizzati gli attributi personalizzati e gestiti per tutti i dispositivi nell’account AWS IoT Core associato.
4. Sulla parte superiore della pagina, immetti una parola chiave che desideri includere nella query. Le query per parole chiave si applicano a tutti i campi.
5. Nella parte superiore della pagina, scegli Filter (Filtro).
6. Nel modale Filter (Filtro), in Field (Campo), scegli il campo che desideri utilizzare come filtro. In Operator (Operatore), scegli un'opzione. Infine, per Value (Valore), scegli il valore del campo da utilizzare nel filtro.

   È possibile aggiungere fino a un massimo di tre filtri. Una query parola chiave viene conteggiata in base a questo numero.
7. Per eseguire la query, scegli Apply filters (Applica filtri). I risultati mostrano tutti i dispositivi che corrispondono alla tua query.

# Utilizzo di processi e modelli di processi in Fleet Hub per AWS IoT Device Management

> **Note**
>
> La caratteristica modelli di processo è in anteprima ed è soggetta a modifica.

Un processo è un'operazione remota che viene inviata a uno o più dispositivi connessi ad AWS IoT ed eseguita su di essi. Puoi ad esempio definire un processo che indichi a un set di dispositivi di scaricare e installare aggiornamenti per le applicazioni o il firmware, eseguire il riavvio, ruotare i certificati o eseguire operazioni di risoluzione dei problemi in remoto. È possibile eseguire processi preconfigurati da Fleet Hub per le applicazioni web di AWS IoT Device Management. Gli amministratori dell'organizzazione creano modelli di processo nella console AWS IoT e collegano policy che rendono i modelli disponibili agli utenti di Fleet Hub. Nell'applicazione Fleet Hub, specifica i dispositivi o un gruppo di dispositivi su cui viene eseguito il processo.

Gli amministratori creano inoltre gruppi di dispositivi che è possibile visualizzare nell'applicazione. Per visualizzare questi gruppi, scegli Device groups (Gruppi di dispositivi) nel riquadro di navigazione. Quando si specifica un gruppo di dispositivi come destinazione, è possibile specificare uno dei due seguenti tipi di opzioni per l'esecuzione del processo.

- snapshot: il processo viene eseguito una volta.
- continuous: dopo l'esecuzione iniziale, il processo viene eseguito su qualsiasi dispositivo aggiunto al gruppo.

Per ulteriori informazioni sulla creazione e la gestione di modelli di processo, consulta Modelli di processo. Per ulteriori informazioni sul funzionamento del processo, consulta Processi.

## Esecuzione di processi

Sebbene in un'applicazione Fleet Hub sia possibile eseguire un processo da diverse posizioni, i passaggi che seguono vanno sempre eseguiti.

1. Seleziona un gruppo o uno o più dispositivi come destinazione.
2. Scegliere Run job (Esegui processo).
3. In Job target selection (Selezione destinazione del processo), scegli continuous o snapshot.

4. Seleziona un modello di processo. Verifica che il testo in Job summary (Riepilogo del processo) descriva il tipo di processo da eseguire.
5. Facoltativamente, inserisci un nome per il processo.
6. Scegli Run (Esegui).

Puoi selezionare le destinazioni e seguire questi passaggi dalle seguenti posizioni nell'applicazione Fleet Hub.

- La scheda dell'elenco dei dispositivi sul pannello di controllo.
- La pagina dei dettagli di un dispositivo specifico.
- La pagina dei gruppi di dispositivi.
- La pagina dei dettagli di un gruppo di dispositivi specifico.

## La visualizzazione e gestione dei processi

Puoi visualizzare i lavori in esecuzione nel tuo parco istanze nelle seguenti posizioni.

- Pagina elenco processi: in questa pagina vengono visualizzati tutti i processi in esecuzione nel parco istanze. Per visualizzare questa pagina, scegli Jobs (Processi) nel riquadro di navigazione.
- La pagina dei dettagli di un dispositivo specifico -- questa pagina mostra tutti i processi in esecuzione sul dispositivo.

Ogni processo dispone di una pagina dei dettagli che visualizza informazioni di riepilogo sul processo, incluse le informazioni sulla destinazione e sul runtime. Questa pagina mostra lo stato del tempo di esecuzione del processo su ciascun dispositivo. Mostra inoltre i seguenti totali.

- Numero di esecuzioni.
- Numero di esecuzioni annullate.
- Numero di esecuzioni riuscite.
- Numero di esecuzioni non riuscite.
- Numero di esecuzioni rifiutate.
- Numero di esecuzioni in coda.
- Numero di esecuzioni in corso.

- Numero di esecuzioni rimosse.
- Numero di esecuzioni scadute.

Per annullare un processo, seleziona il processo e scegli Cancel (Annulla).

# Allarmi

Questa sezione spiega come funziona Fleet Hub per gli allarmi di AWS IoT Device Management e guida le fasi necessarie per creare un allarme.

Quando crei un allarme Fleet Hub, questo si applica a tutti i dispositivi attualmente visualizzati nel pannello di controllo. Se non applichi alcuna query, l'allarme si applica a tutti i dispositivi del tuo parco istanze. Per informazioni sull'utilizzo del dashboard e sulla creazione di query, consulta the section called “Query e filtri”.

Gli allarmi utilizzano i parametri di Amazon CloudWatch (CloudWatch) in combinazione con i campi ricercabili dal servizio di indicizzazione del parco istanze AWS IoT per creare allarmi CloudWatch. Ad esempio, puoi creare un allarme che genera un messaggio Amazon Simple Notification Service (Amazon SNS) ogni volta che il livello medio della batteria dei dispositivi del tuo parco istanze scende al di sotto del 50%.

Gli allarmi Fleet Hub utilizzano GetStatistics e GetPercentiles del servizio di indicizzazione del parco istanze per eseguire le query sui dati aggregati. Ad esempio, quando si crea un allarme che tiene traccia di un campo numerico personalizzato, è possibile creare soglie allarmanti applicabili ai seguenti valori dell'attributo specificato.

- Massimo
- Conteggio
- Somma
- Minimo
- Media
- Valori nel 10°, 50°, 90°, 95° o 99° percentuale

Per ulteriori informazioni sull'esecuzione di query sui dati aggregati nel servizio Fleet Indexing, consulta Interrogazione di dati aggregati.

Nella tabella seguente vengono elencati alcuni esempi dei tipi di aggregazione disponibili per AWS campi gestiti e personalizzati.

| Campo | Tipo di aggregazione |
| --- | --- |
| Tipo di oggetti (campo stringa gestito da AWS) | Conteggio |
| Gruppo di oggetti (campo stringa gestito da AWS) | Conteggio |
| Connesso (campo booleano gestito da AWS)<br><br>Il valore di `true` è 1. Il valore di `false` è 0. | • Massimo<br>• Conteggio<br>• Somma<br>• Minimo<br>• Media |
| shadow.reported.batterylevel (campo di aggregazione numerica creato nel servizio di indicizzazione del parco istanze) | • Massimo<br>• Conteggio<br>• Somma<br>• Minimo<br>• Media<br>• p10 (10° percentuale)<br>• p50 (50° percentuale)<br>• p90 (90° percentuale)<br>• p95 (95° percentuale)<br>• p99 (99° percentuale) |

Oltre a specificare i campi e i tipi di aggregazione, si specificano anche i seguenti valori.

- La durata di tempo (1 minuto o 5 minuti) necessaria alla soglia di allarme specificata per attivare l'allarme.
- Uno dei seguenti operatori di confronto da applicare al campo e al tipo di aggregazione specificati.
  - Maggiore
  - Maggiore/Uguale

  - Minore
  - Minore/Uguale
- Il valore da utilizzare con l'operatore di confronto specificato.
- Un elenco di indirizzi e-mail delle persone della tua organizzazione che ricevono messaggi Amazon SNS ogni volta che viene attivato l'allarme.
- Un nome dell'allarme.

Per creare un allarme Fleet Hub, consulta the section called “Creazione di allarmi”.

## Creazione di allarmi

In questo argomento vengono illustrati i passaggi necessari per creare un Fleet Hub per gli allarmi di AWS IoT Device Management. Si presuppone che l'amministratore abbia creato un campo di aggregazione da un campo shadow del dispositivo denominato shadow.reported.batterylevel. Questo campo personalizzato indica il livello della batteria di un dispositivo. È necessario chiedere all'amministratore di creare campi personalizzati ricercabili nel servizio Fleet Indexing AWS IoT.

L'allarme creato invia un messaggio Amazon Simple Notification Service (Amazon SNS) a un elenco di persone della tua organizzazione ogni volta che il livello medio della batteria dei dispositivi nel tuo parco istanze scende al di sotto del 50% per un periodo di 1 minuto.

Creazione di una query Fleet Hub

1. Passa all'applicazione Fleet Hub.
2. Se desideri assegnare un determinato set di dispositivi, crea una query. Per istruzioni su come creare una query semplice, consulta the section called “Creazione di query con filtri”. Se non crei una query, l'allarme verrà applicato a tutti i dispositivi del tuo parco istanze.
3. Nella pagina predefinita del dashboard, scegli Crea allarme.
4. Sulla pagina Crea un parametro di aggregazione verifica che la query venga visualizzata in Query di destinazione. Nella sezione Configurare l'aggregazione dei parametri, per Scegli campo, scegli shadow.reported.batterylevel. Questo menu contiene i campi gestiti e personalizzati AWS creati dall'amministratore nel Servizio Fleet Indexing AWS IoT.
5. Per Scegli il tipo di aggregazione, scegli Media. Questa scelta basa l'allarme sul valore medio del livello della batteria nel parco istanze.
6. Alla voce Scegli periodo, scegli 1 minuto. Questo attiva l'allarme quando il parco istanze rimane nello stato di allarme specificato per un minuto.

Seleziona Successivo.

7. Sulla pagina Imposta soglia, nella sezione Attiva l'allarme ogni volta che..., scegli Inferiore/Uguale. Questo attiva l'allarme quando il valore medio della batteria scende al di sotto di un valore specificato.
8. Nella casella di testo Than, immetti 50.

   Seleziona Successivo.
9. Sulla pagina Notify user (Notifica all'utente), nella sezione Notify — optional (Notifica – facoltativo), immetti un nome per l'elenco di posta elettronica contenente gli utenti dell'organizzazione che ricevono notifiche quando l'allarme è attivo. Immetti un elenco separato da virgole di indirizzi email per popolare questo elenco.
10. Nella sezione Alarm details (Dettagli allarme), immetti un nome per il tuo allarme e, facoltativamente, inserisci una descrizione per il tuo allarme. Seleziona Successivo.
11. Nella pagina Review (Revisione) esamina le informazioni immesse o selezionate nelle pagine precedenti. Scegli Submit (Invia). Torna al dashboard predefinito.
12. Nel pannello di navigazione predefinito, nel riquadro di navigazione sinistro, seleziona Fleet Hub alarms (Allarmi Fleet Hub). Verifica di visualizzare l'allarme creato.

# Risoluzione dei problemi

Questa sezione fornisce informazioni sulla risoluzione dei problemi e su possibili soluzioni per aiutare a risolvere i problemi con Fleet Hub.

| Sintomo | Soluzione |
| --- | --- |
| Non riesco ad aggiungere altri filtri o termini alla mia query. | Assicurati di non aver raggiunto il limite di termini e filtri per la query, fissato a quattro. |
| Non riesco a trovare un parametro personali zzato. | Chiedere all'amministratore di creare la metrica nel servizio di indicizzazione del parco istanze. |
| Il mio allarme non mostra alcun dato. | Il caricamento dei dati di allarme può richiedere alcuni minuti. |

| Sintomo | Soluzione |
| --- | --- |
| Devo cambiare i dispositivi per cui ho impostato gli allarmi. | Vai al pannello di controllo e modifica la query. |
| Visualizzo un errore quando modifico la regione nel dashboard. | Chiedi all'amministratore di verificare che l’indicizzazione del parco istanze sia attivata nella regione selezionata. |
| Lo stato di connettività del mio "oggetto" non è indicizzato da Fleeting Indexing. | Assicurati che il tuo client utilizzi lo stesso ID client di Thing Name durante la connessione a AWS IoT. Se il tuo client utilizza un ID diverso da Thing Name durante la connessione aAWS IoT, lo stato della connettività del tuo "oggetto" non verrà indicizzato da Fleet Indexing. |

# Monitoriaggio di Fleet Hub per la gestione dei dispositivi AWS IoT

Il monitoraggio è importante per mantenere l'affidabilità, la disponibilità e le prestazioni di Fleet Hub e delle altre soluzioni di AWS. AWS fornisce i seguenti strumenti di monitoraggio per controllare Fleet Hub, segnalare eventuali problemi ed eseguire operazioni automatiche quando appropriato.

- AWS CloudTrail acquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo account AWS e fornisce i file di log a un bucket Amazon S3 specificato. Puoi identificare quali utenti e account hanno richiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute. Per ulteriori informazioni, consultare la Guida per l'utente AWS CloudTrail.

Argomenti



## Registrazione di Fleet Hub per le chiamate API della gestione dispositivi AWS IoT con AWS CloudTrail

Fleet Hub per la gestione dei dispositivi AWS IoT è integrato con AWS CloudTrail. CloudTrail è un servizio che fornisce un record delle operazioni eseguite da un utente, un ruolo o un servizio AWS in Fleet Hub. CloudTrail acquisisce tutte le chiamate API per Fleet Hub come eventi. Le chiamate acquisite includono le chiamate dalla console Fleet Hub e le chiamate di codice alle operazioni API Fleet Hub.

Se viene creato un trail, è possibile abilitare la distribuzione continua di eventi CloudTrail in un bucket Amazon S3, inclusi gli eventi per Fleet Hub. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella console di CloudTrail in Cronologia eventi.

Le informazioni raccolte da CloudTrail consentono di determinare la richiesta effettuata a Fleet Hub, l'indirizzo IP da cui è partita la richiesta, l'autore della richiesta, il momento in cui è stata eseguita e altri dettagli.

Per ulteriori informazioni su CloudTrail, consultare la AWS CloudTrailGuida per l'utente di .

# Informazioni Fleet Hub su CloudTrail

AWS CloudTrail è abilitato sull'account AWS al momento della sua creazione. Quando si verifica un'attività in Fleet Hub, questa viene registrata in un evento CloudTrail insieme ad altri eventi di servizio AWS nella Cronologia degli eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account AWS. Per ulteriori informazioni, consulta Visualizzazione di eventi mediante la cronologia eventi di CloudTrail.

Per una registrazione continua degli eventi nell'account AWS, inclusi gli eventi relativi a Fleet Hub, crea un trail. Un trail consente a CloudTrail di distribuire i file di log in un bucket Amazon Simple Storage Service (Amazon S3). Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le regioni AWS. Il trail registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato.

Puoi anche configurare altri servizi AWS per analizzare con maggiore dettaglio e agire sui dati dell'evento raccolti nei log CloudTrail. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- Servizi e integrazioni CloudTrail supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di log CloudTrail da più regioni
- Ricezione di file di log CloudTrail da più account

CloudTrail registra tutte le operazioni Fleet Hub. Sono documentate nella Documentazione di riferimento API AWS IoT. Ad esempio, le chiamate a `CreateApplication` e le operazioni `UpdateApplication` generano voci nei file di log di CloudTrail.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali utente AWS Identity and Access Management o root.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro servizio AWS.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

# Informazioni su Fleet Hub per le voci del file di log della gestione dei dispositivi AWS IoT

Un percorso è una configurazione che consente la distribuzione di eventi come i file di log in un bucket Amazon S3 specificato.

I file di log di CloudTrail possono contenere una o più voci di log. Un evento rappresenta una singola richiesta da un'origine e include informazioni sull'operazione richiesta, sulla data e sull'ora dell'operazione, sui parametri richiesti e così via.

I file di log CloudTrail non sono una traccia di pila ordinata delle chiamate API pubbliche e di conseguenza non devono apparire in base a un ordine specifico.

Example

La seguente voce di log CloudTrail mostra informazioni sull'operazione `CreateApplication`.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "principal-id",
        "arn": "arn:aws:sts::123456789012:assumed-role/Admin/test-user-name",
        "accountId": "123456789012",
        "accessKeyId": "access-key",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "principal-id",
                "arn": "arn:aws:iam::123456789012:role/Admin",
                "accountId": "123456789012",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-12-04T19:59:53Z"
            }
        }
    },
    "eventTime": "2020-12-04T20:02:38Z",
```

```
        "eventSource": "iotfleethub.amazonaws.com",
        "eventName": "CreateApplication",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "72.22.186.61",
        "userAgent": "console.amazonaws.com",
        "requestParameters": {
            "applicationDescription": "Test application description",
            "applicationName": "Test application name",
            "clientToken": "c9bc7f45-3737-4ee9-9b0f-5de1aab169b2"
        },
        "responseElements": {
            "applicationUrl": "https://application-id.app.iotfleethub.aws",
            "applicationArn": "arn:aws:iotfleethub:us-
east-1:123456789012:application/application-id",
            "applicationId": "application-id"
        },
        "requestID": "5456304e-31c5-4336-9bbe-a375e3728eee",
        "eventID": "9ffb5d72-9267-4f4e-88e6-d26051133c8c",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "recipientAccountId": "123456789012"
    }
```

# Sicurezza in Fleet Hub per la AWS IoT gestione dei dispositivi

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per ulteriori informazioni sui programmi di conformità che si applicano a Fleet Hub, consulta AWS Servizi rientranti nell'ambito del programma di conformitàAWS .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e le leggi e le normative applicabili.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi Fleet Hub per la gestione dei AWS IoT dispositivi. I seguenti argomenti illustrano come configurare Fleet Hub per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse di Fleet Hub.

Argomenti

# Protezione dei dati in Fleet Hub

Il modello di responsabilità AWS condivisa modello si applica alla protezione dei dati in Fleet Hub for AWS IoT Device Management. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or 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.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno 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 hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite 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. Ciò include quando lavori con Fleet Hub o altro Servizi AWS utilizzando la console, l'API o gli SDK. AWS CLI AWS 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 inattivi

Fleet Hub protegge i dati inattivi tramite la crittografia lato server. Per ulteriori informazioni, consulta Crittografia dei dati su AWS IoT nella Guida per gli sviluppatori AWS IoT .

## Crittografia in transito

Nelle distribuzioni cloud dei flussi, Fleet Hub protegge i dati in transito utilizzando il protocollo Transport Layer Security (TLS). Per ulteriori informazioni, consulta Sicurezza del trasporto su AWS IoT nella Guida per gli sviluppatori AWS IoT .

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

AWS Identity and Access Management (IAM) è uno strumento Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi è autenticato (accesso effettuato) e autorizzato (dispone di autorizzazioni) a utilizzare risorse Fleet Hub. IAM è un software Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti



## Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Fleet Hub.

Utente del servizio – Se utilizzi il servizio Fleet Hub per eseguire il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. All'aumentare del numero di funzionalità Fleet Hub 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 Fleet Hub, consulta Risoluzione dei problemi Fleet Hub for AWS IoT Device Management di identità e accesso.

Amministratore del servizio – Se sei il responsabile delle risorse Fleet Hub presso la tua azienda, probabilmente disponi dell'accesso completo a Fleet Hub. Il tuo compito è determinare le caratteristiche e le risorse Fleet Hub 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 Fleet Hub, consulta Come Fleet Hub for AWS IoT Device Management funziona con IAM.

Amministratore IAM – Se sei un amministratore IAM, potresti essere interessato a ottenere informazioni su come scrivere policy per gestire l'accesso a Fleet Hub. Per visualizzare esempi di policy basate su identità di Fleet Hub che puoi utilizzare in IAM, consulta Esempi di policy basate sull'identità per Fleet Hub for AWS IoT Device Management.

## Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue 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. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Signing AWS API request nella IAM User Guide.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo 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.

### Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso 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.

### Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni sul Centro identità IAM, consulta Cos'è Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center .

### Utenti e gruppi IAM

Un utente IAM è un'identità interna 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

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o 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 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, con alcuni Servizi AWS, è possibile allegare 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 a più servizi: alcuni Servizi AWS utilizzano le funzionalità di 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.
  - Sessioni di accesso diretto (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato 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 chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. 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 che un servizio assume per eseguire azioni 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.
  - 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 al servizio vengono visualizzati nel tuo 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: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di 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

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come 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 AWS JSON per specificare chi ha accesso a cosa. 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'azione, 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 dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

### 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 ruoli 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 integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS.

Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. 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 collegare 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 collegata 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 puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle 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 su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF 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 tipi di policy aggiuntivi e 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.

- Politiche di controllo dei servizi (SCP): le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS 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. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. 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 scoprire come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

## Come Fleet Hub for AWS IoT Device Management funziona con IAM

Prima di utilizzare IAM per gestire l'accesso a Fleet Hub, scopri quali funzionalità IAM sono disponibili all'uso con Fleet Hub.

Funzionalità IAM che puoi utilizzare con Fleet Hub for AWS IoT Device Management

| Funzionalità IAM | Supporto Fleet Hub |
|---|---|
| Policy basate su identità | Sì |
| Policy basate su risorse | No |
| Azioni di policy | Sì |

| Funzionalità IAM | Supporto Fleet Hub |
| --- | --- |
| 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 | Sì |
| Ruoli collegati al servizio | No |

Per avere una visione di alto livello di come Fleet Hub e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

## Policy basate su identità per Fleet Hub

| | |
| --- | --- |
| 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 utilizzati in una policy JSON, consulta Riferimento degli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Esempi di policy basate su identità per Fleet Hub

Per visualizzare esempi di policy basate su identità Fleet Hub, consulta Esempi di policy basate sull'identità per Fleet Hub for AWS IoT Device Management.

## Policy basate su risorse all'interno di Fleet Hub

| | |
|---|---|
| Supporta le policy basate su risorse | No |

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare 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 collegata 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 il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad 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 IAM.

## Azioni di policy per Fleet Hub

> **Note**
>
> Le applicazioni Fleet Hub utilizzano la policy gestita da `AWSIoTFleetHubFederationAccess`. Per ulteriori informazioni, consulta ???.

| | |
|---|---|
| Supporta le azioni di policy | Sì |

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. 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 un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. 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.

Per visualizzare un elenco di operazioni Fleet Hub, consulta Operazioni definite da Fleet Hub for AWS IoT Device Management in Riferimento per l'autorizzazione del servizio.

Le operazioni delle policy su Fleet Hub utilizzano il seguente prefisso prima dell'operazione:

```
iotfleethub
```

Per specificare più operazioni in una sola istruzione, separale con la virgola.

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

Per visualizzare esempi di policy basate su identità Fleet Hub, consulta Esempi di policy basate sull'identità per Fleet Hub for AWS IoT Device Management.

## Risorse delle policy per Fleet Hub

| | |
|---|---|
| Supporta le risorse di policy | Sì |

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. 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": "*"
```

Per visualizzare un elenco di tipi di risorse Fleet Hub e dei relativi ARN, consulta Risorse definite da Fleet Hub for AWS IoT Device Management in Riferimento per l'autorizzazione del servizio. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta la sezione Operazioni definite da Fleet Hub for AWS IoT Device Management.

Per visualizzare esempi di policy basate su identità Fleet Hub, consulta Esempi di policy basate sull'identità per Fleet Hub for AWS IoT Device Management.

## Chiavi di condizione della policy per Fleet Hub

| | |
|---|---|
| Supporta le chiavi di condizione delle policy specifiche del servizio | Sì |

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni 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 si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` 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 del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per visualizzare un elenco di chiavi di condizione Fleet Hub, consulta Chiavi di condizione per Fleet Hub for AWS IoT Device Management in Riferimento per l'autorizzazione del servizio. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, consulta Actions defined by Fleet Hub for AWS IoT Device Management.

Per visualizzare esempi di policy basate su identità Fleet Hub, consulta Esempi di policy basate sull'identità per Fleet Hub for AWS IoT Device Management.

## Liste di controllo accessi di rete (ACL) su Fleet Hub

| | |
|---|---|
| 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.

## Controllo dell'accesso basato su attributi (ABAC) con Fleet Hub

| | |
|---|---|
| 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, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. 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 Uso del controllo dell'accesso basato su attributi (ABAC) nella Guida per l'utente di IAM.

## Utilizzo di credenziali temporanee con Fleet Hub

| | |
|---|---|
| Supporta le credenziali temporanee | Sì |

Alcuni Servizi AWS non funzionano quando accedi utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedete AWS utilizzando il link Single Sign-On (SSO) della vostra azienda, tale processo crea automaticamente 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 l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

## Autorizzazioni principali tra servizi per Fleet Hub

| | |
|---|---|
| Supporta l'inoltro delle sessioni di accesso (FAS) | Sì |

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato 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 chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.

## Ruoli dei servizi per Fleet Hub

| | |
|---|---|
| Supporta i ruoli di servizio | Sì |

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.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere la funzionalità di Fleet Hub. Modifica i ruoli di servizio solo quando Fleet Hub fornisce indicazioni per farlo.

## Ruolo collegato al servizio per Fleet Hub

| | |
|---|---|
| Supporta i ruoli collegati ai servizi | No |

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 al servizio vengono visualizzati nel tuo 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.

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta Servizi AWS supportati da IAM. Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked

role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

# Esempi di policy basate sull'identità per Fleet Hub for AWS IoT Device Management

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse Fleet Hub. Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o l'API. AWS Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Per informazioni dettagliate sulle operazioni e sui tipi di risorse definiti da Fleet Hub, incluso il formato degli ARN per ogni tipo di risorsa, consulta Operazioni, risorse e chiavi di condizione per Fleet Hub for AWS IoT Device Management in Service Authorization Reference (Guida di riferimento per l'autorizzazione del servizio).

Argomenti

- Best practice per le policy
- Utilizzo della console Fleet Hub
- Consentire agli utenti di visualizzare le loro autorizzazioni

## Best practice per le policy

Le policy basate su identità determinano se qualcuno può creare, accedere o eliminare le risorse Fleet Hub nell'account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy AWS gestite che concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzionalità dei processi nella Guida per l'utente di 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 ad azioni 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 anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio 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.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'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 Fleet Hub

Per accedere alla Fleet Hub for AWS IoT Device Management console, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse di Fleet Hub presenti nel tuo. Account AWS Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che gli utenti e i ruoli possano ancora utilizzare la console Fleet Hub, collega anche il Fleet Hub `ConsoleAccess` o la politica `ReadOnly` AWS gestita alle entità. Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente IAM.

## 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 cpllegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando programmaticamente l' AWS CLI API o. AWS

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

```
}
```

# Risoluzione dei problemi Fleet Hub for AWS IoT Device Management di identità e accesso

Utilizza le informazioni seguenti per diagnosticare e risolvere i problemi comuni che possono verificarsi durante l'utilizzo di Fleet Hub e IAM.

Argomenti



## Non sono autorizzato a eseguire un'operazione su Fleet Hub

Se ti AWS Management Console dice che non sei autorizzato a eseguire un'azione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è colui che ti ha fornito le credenziali di accesso.

> **Note**
>
> Le applicazioni Fleet Hub utilizzano la policy gestita da `AWSIoTFleetHubFederationAccess`. Per ulteriori informazioni, consulta ???.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` cerca di utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `iotfleethub:`*`GetWidget`* fittizie.

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

In questo caso, Mateo richiede al suo amministratore di aggiornare le policy per poter accedere alla risorsa *`my-example-widget`* utilizzando l'azione `iotfleethub:`*`GetWidget`*.

## Non sono autorizzato a eseguire iam: PassRole

Se ricevi un errore che indica che non sei autorizzato a eseguire l'operazione `iam:PassRole`, le tue policy devono essere aggiornate per poter passare un ruolo a Fleet Hub.

Alcuni Servizi AWS consentono di passare un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` cerca di utilizzare la console per eseguire un'operazione su Fleet Hub. Tuttavia, l'operazione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

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

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

## Voglio consentire a persone esterne al mio AWS account di accedere alle mie risorse Fleet Hub

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 Fleet Hub supporta queste funzionalità, consulta Come Fleet Hub for AWS IoT Device Management funziona con IAM.
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti 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, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente IAM.

# Convalida della conformità per Fleet Hub for AWS IoT Device Management

I revisori di terze parti valutano la sicurezza e la conformità di Fleet Hub nell'ambito di più programmi di AWS conformità. Questi includono SOC, PCI, FedRAMP, HIPAA e altri.

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono i passaggi per l'implementazione di ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

> **Note**
>
> Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Evaluating Resources with Rules nella AWS Config Developer Guide: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente AWS l'utilizzo per semplificare la gestione dei rischi e la conformità alle normative e agli standard di settore.

# Resilienza in Fleet Hub per la gestione dei AWS IoT dispositivi

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. AWS Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover 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 AWS regioni e zone di disponibilità, consulta Global Infrastructure.AWS

# AWS politiche gestite per Fleet Hub for AWS IoT Device Management

Per aggiungere autorizzazioni a utenti, gruppi e ruoli, è più facile utilizzare le politiche AWS gestite che scrivere le politiche da soli. Creare policy gestite dal cliente IAM per fornire al tuo team solo

le autorizzazioni di cui ha bisogno richiede tempo e competenza. Per iniziare rapidamente, puoi utilizzare le nostre politiche AWS gestite. Queste politiche coprono casi d'uso comuni e sono disponibili nel tuo AWS account. Per ulteriori informazioni sulle policy AWS gestite, consulta le policy AWS gestite nella IAM User Guide.

AWS i servizi mantengono e aggiornano le politiche AWS gestite. Non è possibile modificare le autorizzazioni nelle politiche AWS gestite. 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 AWS gestita, quindi gli aggiornamenti delle policy non comprometteranno le autorizzazioni esistenti.

Inoltre, AWS supporta politiche gestite per le funzioni lavorative che si estendono su più servizi. Ad esempio, la policy ReadOnlyAccess AWS gestita fornisce l'accesso in sola lettura a tutti i AWS servizi e le risorse. Quando un servizio lancia 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.

## AWS politica gestita: AWSIoTFleetHubFederationAccess

È possibile allegare la policy `AWSIoTFleetHubFederationAccess`alle identità IAM.

Questa politica concede agli utenti federati di Fleet Hub for AWS IoT Device Management le autorizzazioni necessarie per intraprendere azioni nelle applicazioni web di Fleet Hub AWS IoT e in altri AWS servizi.

Per ulteriori informazioni sull'aggiunta di utenti alle applicazioni web Fleet Hub, consulta ???.

È possibile visualizzare la policy nella console AWS.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `iot`- Recupera i dati AWS IoT del dispositivo ed esegui azioni a livello di flotta.
- `iotfleethub` - Recupero dei metadati dell'app Fleet Hub.
- `cloudwatch`- Recupera i dati di CloudWatch allarme e metrici. Consente inoltre di creare ed eliminare operazioni relative agli allarmi Fleet Hub.
- `sns` - Eseguire, creare, leggere, eliminare, sottoscrivere e annullare le operazioni. Queste operazioni sono limitate agli argomenti SNS di Fleet Hub.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:DescribeIndex",
                "iot:DescribeThingGroup",
                "iot:GetBucketsAggregation",
                "iot:GetCardinality",
                "iot:GetIndexingConfiguration",
                "iot:GetPercentiles",
                "iot:GetStatistics",
                "iot:SearchIndex",
                "iot:CreateFleetMetric",
                "iot:ListFleetMetrics",
                "iot:DeleteFleetMetric",
                "iot:DescribeFleetMetric",
                "iot:UpdateFleetMetric",
                "iot:DescribeCustomMetric",
                "iot:ListCustomMetrics",
                "iot:ListDimensions",
                "iot:ListMetricValues",
                "iot:ListThingGroups",
                "iot:ListThingsInThingGroup",
                "iot:ListJobTemplates",
                "iot:DescribeJobTemplate",
                "iot:ListJobs",
                "iot:CreateJob",
                "iot:CancelJob",
                "iot:DescribeJob",
                "iot:ListJobExecutionsForJob",
```

```
                "iot:ListJobExecutionsForThing",
                "iot:DescribeJobExecution",
                "iot:ListSecurityProfiles",
                "iot:DescribeSecurityProfile",
                "iot:ListActiveViolations",
                "iot:GetThingShadow",
                "iot:ListNamedShadowsForThing",
                "iot:CancelJobExecution",
                "iot:DescribeEndpoint",
                "iotfleethub:DescribeApplication",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:GetMetricData",
                "cloudwatch:ListMetrics",
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:ListSubscriptionsByTopic",
                "sns:Subscribe",
                "sns:Unsubscribe"
            ],
            "Resource": "arn:aws:sns:*:*:iotfleethub*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricAlarm",
                "cloudwatch:DeleteAlarms",
                "cloudwatch:DescribeAlarmHistory"
            ],
            "Resource": "arn:aws:cloudwatch:*:*:iotfleethub*"
        }
    ]
}
```

# Fleet Hub: aggiornamenti alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per Fleet Hub da quando questo servizio ha iniziato a tracciare queste modifiche. Per ulteriori informazioni, consulta la pagina Documentation history (Cronologia della documentazione) di Fleet Hub.

| Modifica | Descrizione | Data |
| --- | --- | --- |
| AWSIoTFleetHubFederationAccess: aggiornamento a una policy esistente | Fleet Hub ha aggiunto nuove autorizzazioni per permettere agli utenti delle app di recuperare i dati dei parametri AWS IoT Device Defender nelle app Fleet Hub. | 4 aprile 2022 |
| AWSIoTFleetHubFederationAccess: aggiornamento a una policy esistente | Fleet Hub ha aggiunto nuove autorizzazioni per permettere agli utenti delle app di recuperare origini dati aggiuntive per l'indiciz zazione. Viene inoltre aggiunta un'autorizzazione per consentire agli utenti dell'app di annullare l'esecuzione di un AWS IoT lavoro all'interno dell'app. | 15 novembre 2021 |
| AWSIoTFleetHubFederationAccess: aggiornamento a una policy esistente | Fleet Hub ha aggiunto nuove autorizzazioni per gli utenti dell'app per recuperare i dati di Thing Group ed eseguire operazioni CRUD sui lavori. AWS IoT | 24 maggio 2021 |
| AWSIoTFleetHubFederationAccess: aggiornamento a una policy esistente | Fleet Hub ha rimosso le autorizzazioni per le API non supportate del pannello di controllo di Fleet Hub. | 12 Aprile 2021 |

| Modifica | Descrizione | Data |
| --- | --- | --- |
| AWSIoTFleetHubFederationAccess: nuova policy | Fleet Hub ha aggiunto una nuova politica che concede le autorizzazioni necessarie agli utenti dell'applicazione Fleet Hub per recuperare i dati del dispositivo ed eseguire azioni. AWS IoT | 12 Aprile 2021 |
| Fleet Hub ha iniziato a monitorare le modifiche | Fleet Hub ha iniziato a tracciare le modifiche alle sue AWS politiche gestite. | 12 Aprile 2021 |

# Sicurezza dell'infrastruttura in Fleet Hub per la gestione dei AWS IoT dispositivi

In quanto servizio gestito, Fleet Hub for AWS IoT Device Management è protetto dalle procedure di sicurezza di rete AWS globali descritte nel white paper Amazon Web Services: Overview of Security Processes.

Utilizzi chiamate API AWS pubblicate per accedere a Fleet Hub attraverso la rete. I client devono supportare Transport Layer Security (TLS) 1.2 o versioni successive. È consigliabile utilizzare TLS 1.3. I client devono, inoltre, supportare le suite di crittografia 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 utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. O puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

# Prevenzione del problema "confused deputy" tra servizi

Con "confused deputy" si intende un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire una certa operazione può costringere un'entità con più privilegi a eseguire tale operazione. Nel AWS, l'impersonificazione tra servizi può portare al confuso problema

del vice. La rappresentazione tra servizi può verificarsi quando un servizio (il servizio chiamante) effettua una chiamata a un altro servizio (il servizio chiamato). Il servizio chiamante può essere manipolato per utilizzare le proprie autorizzazioni e agire sulle risorse di un altro cliente, a cui normalmente non avrebbe accesso. Per evitare ciò, AWS fornisce alcuni strumenti che consentono di proteggere i dati per tutti i servizi che dispongono di principali del servizio a cui è stato consentito l'accesso alle risorse del tuo account.

Si consiglia di utilizzare le chiavi di contesto delle condizioni globali `aws:SourceArn` e `aws:SourceAccount` nelle policy delle risorse per limitare le autorizzazioni alle risorse che Fleet Hub fornisce ad altri servizi. Se si utilizzano entrambe le chiavi di contesto delle condizioni globali, il valore `aws:SourceAccount` e l'account nel valore `aws:SourceArn` devono utilizzare lo stesso ID account nella stessa istruzione di policy.

Il modo più efficace per proteggersi dal problema "confused deputy" è quello di usare la chiave di contesto della condizione globale `aws:SourceArn` con l'Amazon Resource Name (ARN) completo della risorsa. Per Fleet Hub, il tuo `aws:SourceArn` deve soddisfare il formato `arn:aws:iot:`*`region`*`:`*`account-id`*`:*`. Assicurarsi che la *`regione`* corrisponda alla tua regione Fleet Hub e che il tuo *`id account`* corrisponda all'ID dell'account cliente.

L'esempio seguente mostra come prevenire il problema del "confused deputy" le chiavi di contesto delle condizioni globali `aws:SourceArn` e `aws:SourceAccount` nella policy di attendibilità dei ruoli Fleet Hub. Per trovare l'ARN del tuo ruolo Fleet Hub, vai alla sezione Fleet Hub nella AWS IoT console e seleziona la tua applicazione Fleet Hub per visualizzare la pagina dei dettagli dell'applicazione.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "iotfleethub.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:iot:us-east-1:123456789012:*"
```

```
          }
        }
      }
    ]
}
```

# Cronologia della documentazione

La tabella seguente descrive gli aggiornamenti alla documentazione per Fleet Hub. Per le modifiche in policy gestite da AWS per Fleet Hub, vedi policy gestite da AWS per Fleet Hub per AWS IoT Device Management.

| Modifica | Descrizione | Data |
| --- | --- | --- |
| Rilascio di disponibilità generale di Fleet Hub per AWS IoT Device Management | Aggiornamenti dei contenuti per riflettere i miglioramenti apportati a Fleet Hub per AWS IoT Device Management durante il periodo di anteprima . | 25 maggio 2021. |
| Versione di anteprima di Fleet Hub per AWS IoT Device Management | Pubblicata la versione di anteprima della Guida per l'utente di Fleet Hub per AWS IoT Device Management. | 16 dicembre 2020. |

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.