aws

Guida per l'utente

AWS IoT SiteWise

AWS IoT SiteWise: Guida per l'utente

Table of Contents

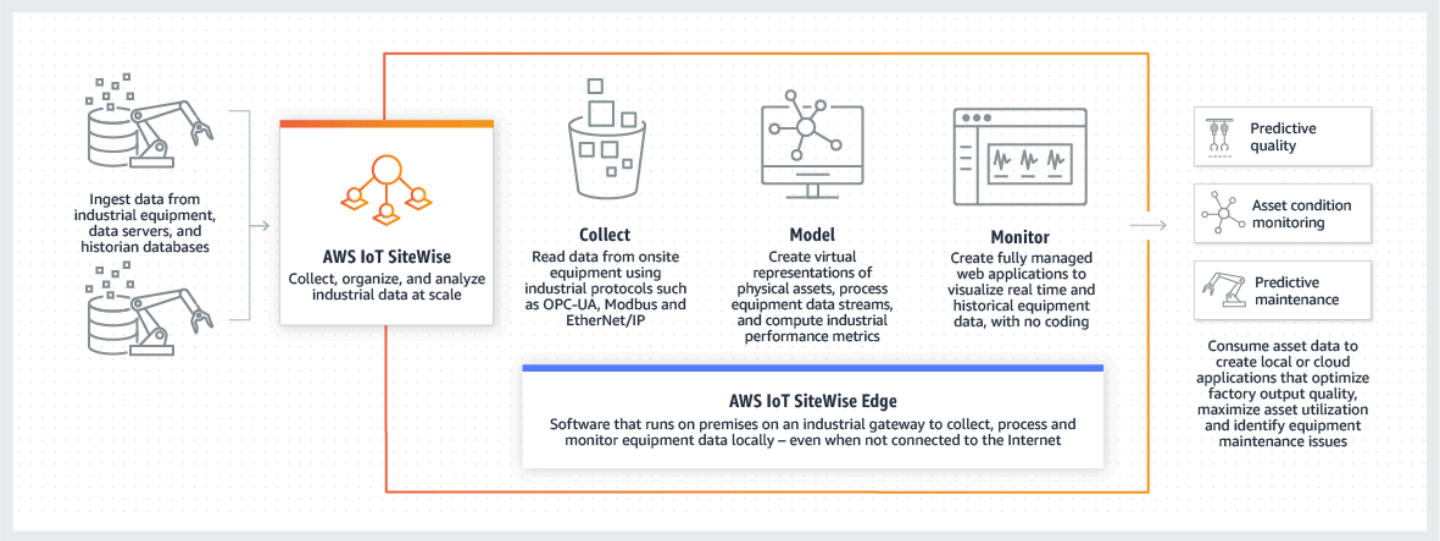
Che cos'è AWS IoT SiteWise?

AWS IoT SiteWise è un servizio gestito che semplifica la raccolta, l'archiviazione, l'organizzazione e il monitoraggio dei dati provenienti dalle apparecchiature industriali su larga scala per aiutarti a prendere decisioni migliori e basate sui dati. È possibile utilizzarlo AWS IoT SiteWise per monitorare le operazioni tra le strutture, calcolare rapidamente metriche di prestazioni industriali comuni e creare applicazioni che analizzano i dati delle apparecchiature industriali per prevenire costosi problemi alle apparecchiature e ridurre le lacune nella produzione.

AWS IoT SiteWise Monitor consente agli utenti operativi di creare rapidamente applicazioni web per visualizzare e analizzare i dati industriali in tempo reale. Per ottenere informazioni dettagliate sulle operazioni industriali, bisogna configurare e monitorare parametri quali il tempo medio tra i guasti e l'efficienza complessiva delle apparecchiature (OEE).

AWS IoT SiteWise Edge è un componente AWS IoT SiteWise che consente la raccolta, l'archiviazione e l'elaborazione di dati su dispositivi locali. Ciò è utile se hai un accesso limitato a Internet o hai bisogno di mantenere privati i tuoi dati.

Il diagramma seguente mostra l'architettura di base di AWS IoT SiteWise:



Argomenti

- Come AWS IoT SiteWise funziona
- AWS IoT SiteWise concetti
- Casi d'uso per AWS IoT SiteWise

Come AWS IoT SiteWise funziona

AWS IoT SiteWise offre un framework di modellazione delle risorse che è possibile utilizzare per creare rappresentazioni di dispositivi, processi e strutture industriali. Le rappresentazioni delle apparecchiature e dei processi sono denominate modelli di asset in. AWS IoT SiteWise Con i modelli di asset, definisci i dati grezzi da consumare e come trasformarli in metriche utili. Crea e visualizza risorse e modelli per le tue operazioni industriali nella AWS IoT SiteWise console. Puoi anche configurare modelli di asset per raccogliere ed elaborare dati sull'edge o nel AWS cloud.

Argomenti

Inserisci dati industriali

Inizia a utilizzare AWS IoT SiteWise ingerendo dati industriali. L'acquisizione dei dati avviene in diversi modi:

- Inserimento diretto dai server in loco: utilizza protocolli come OPC-UA per leggere i dati direttamente dai dispositivi in loco. Implementa il software SiteWise Edge gateway, compatibile con AWS IoT Greengrass V2, su un'ampia gamma di piattaforme come gateway industriali comuni o server virtuali. È possibile connettere fino a 100 server OPC-UA a un singolo gateway. AWS IoT SiteWise Per ulteriori informazioni, consulta SiteWise Requisiti del gateway edge.

  Tieni presente che protocolli come Modbus TCP ed EtherNet/IP (EIP) sono supportati dalla nostra partnership con nel contesto di. Domatica AWS IoT Greengrass V2
- Elaborazione dati edge con pacchetti: migliora il tuo gateway SiteWise Edge aggiungendo pacchetti per abilitare funzionalità edge complete. Con SiteWise Edge, disponibile su AWS IoT Greengrass V2, l'elaborazione dei dati viene eseguita direttamente in loco prima di essere trasmessa in modo sicuro al AWS Cloud tramite un AWS IoT Greengrass flusso. Per ulteriori informazioni, consulta Utilizzo dei pacchetti.

- Inserimento adattivo tramite Amazon S3 con operazioni in blocco: quando lavori con un gran numero di asset o modelli di asset, utilizza operazioni in blocco per importare ed esportare in blocco risorse dai bucket Amazon S3. Per ulteriori informazioni, consulta Operazioni in blocco con risorse e modelli.
- Messaggi MQTT con regole di AWS IoT base: per i dispositivi collegati a AWS IoT Core che inviano messaggi MQTT, utilizzate il motore AWS IoT Core rules per indirizzare tali messaggi a AWS IoT SiteWise.Se avete dispositivi collegati a AWS IoT Core che inviano messaggi MQTT, utilizzate il motore AWS IoT Core rules per indirizzare tali messaggi AWS IoT SiteWise. Per ulteriori informazioni, consulta Acquisizione di dati tramite regole AWS IoT Core.
- Inserimento di dati innescato da eventi: utilizza le azioni AWS IoT Events per configurare l' SiteWise azione IoT per inviare dati AWS IoT Events a quando si verificano gli eventi. AWS IoT SiteWise Per ulteriori informazioni, consulta Acquisizione di dati da AWS IoT Events.
- AWS IoT SiteWise API: le tue applicazioni su Edge o nel cloud possono inviare dati direttamente a. AWS IoT SiteWise Per ulteriori informazioni, consulta Acquisizione di dati tramite l'API AWS IoT SiteWise

Modella le risorse per contestualizzare i dati raccolti

Dopo aver acquisito i dati, puoi utilizzarli per creare rappresentazioni virtuali di risorse, processi e strutture creando modelli delle tue operazioni fisiche. Una risorsa, che rappresenta un dispositivo o un processo, trasmette flussi di dati al Cloud. AWS Le risorse possono anche significare raggruppamenti logici di dispositivi. Le gerarchie vengono create associando risorse per rispecchiare operazioni complesse. Queste gerarchie consentono alle risorse di accedere ai dati delle risorse secondarie associate. Gli asset vengono creati a partire da modelli di asset. I modelli di asset sono strutture dichiarative che standardizzano i formati degli asset. Riutilizza i componenti degli asset per l'organizzazione e la manutenibilità dei tuoi modelli. Per ulteriori informazioni, consulta Modellazione degli asset industriali

Con AWS IoT SiteWise, puoi configurare le tue risorse per trasformare i dati in entrata in metriche e trasformazioni contestuali.

- Trasforma il lavoro quando si ricevono i dati delle apparecchiature.
- Le metriche vengono calcolate a intervalli definiti dall'utente.

Le metriche e le trasformazioni sono applicabili sia alle risorse singole che a più risorse.AWS IoT SiteWise calcola automaticamente gli aggregati statistici di uso comune come media, somma

e conteggio, in vari intervalli di tempo relativi ai dati, alle metriche e alle trasformazioni delle apparecchiature.

Le risorse possono essere sincronizzate utilizzando. AWS IoT TwinMaker Per ulteriori informazioni, consulta

Per integrare AWS IoT SiteWise eAWS IoT TwinMaker, devi disporre di quanto segue:

- AWS IoT SiteWiseruolo collegato al servizio impostato nel tuo account
- AWS IoT TwinMakerruolo collegato al servizio impostato nel tuo account
- AWS IoT TwinMakerspazio di lavoro con ID `IoTSiteWiseDefaultWorkspace` nel tuo account nella regione.

Da integrare utilizzando la console AWS IoT SiteWise

Quando vedi il AWS IoT TwinMaker banner Integrazione con nella console, scegli Concedi l'autorizzazione. I prerequisiti vengono creati nel tuo account.

Da integrare utilizzando il AWS CLI

Per integrarlo AWS IoT SiteWise e AWS IoT TwinMaker utilizzarloAWS CLI, inserisci i seguenti comandi:

1. Chiama `CreateServiceLinkedRole` con un `AWSServiceName` di`iotsitewise.amazonaws.com`.

```
aws iam create-service-linked-role --aws-service-name iotsitewise.amazonaws.com
```

2. Chiama `CreateServiceLinkedRole` con un `AWSServiceName` di `iottwinmaker.amazonaws.com`.

```
aws iam create-service-linked-role --aws-service-name iottwinmaker.amazonaws.com
```

3. Chiama `CreateWorkspace` con un `ID` di`IoTSiteWiseDefaultWorkspace`.

```
 aws iottwinmaker create-workspace --workspace-id IoTSiteWiseDefaultWorkspace
```

.

Analizza utilizzando domande, allarmi e previsioni

Analizza la data raccolta AWS IoT SiteWise eseguendo interrogazioni e impostando allarmi. Puoi anche utilizzare Amazon Lookout per rilevare automaticamente le anomalie all'interno dei parametri e identificarne le cause principali.

- Imposta allarmi specifici per avvisare il team quando apparecchiature o processi si discostano dalle prestazioni ottimali, garantendo una rapida identificazione e risoluzione dei problemi. Per ulteriori informazioni, consulta Monitoraggio dei dati con allarmi.
- Utilizza le operazioni AWS IoT SiteWise API per interrogare i valori correnti, i valori storici e gli aggregati delle proprietà degli asset su intervalli di tempo specifici. Per ulteriori informazioni, consulta Interroga dati da AWS IoT SiteWise.
- Usa il rilevamento delle anomalie con Amazon Lookout for Equipment per identificare e visualizzare i cambiamenti nelle apparecchiature o nelle condizioni operative. Con il rilevamento delle anomalie, puoi determinare misure di manutenzione preventiva per le tue operazioni. Questa integrazione consente ai clienti di sincronizzare i dati tra Amazon Lookout for Equipment AWS IoT SiteWise e Amazon. Per ulteriori informazioni, consulta

  > **Note**
  >
  > Il rilevamento delle anomalie è disponibile solo nelle regioni in cui è disponibile Amazon Lookout for Equipment.

  Puoi integrarti AWS IoT SiteWise con Amazon Lookout for Equipment per ottenere informazioni dettagliate sulle tue apparecchiature industriali attraverso il rilevamento delle anomalie e la manutenzione predittiva delle apparecchiature industriali. Lookout for Equipment è un servizio di machine learning (ML) per il monitoraggio delle apparecchiature industriali che rileva il comportamento anomalo delle apparecchiature e identifica potenziali guasti. Con Lookout for Equipment, è possibile implementare programmi di manutenzione predittiva e identificare i processi delle apparecchiature non ottimali. Per ulteriori informazioni su Lookout for Equipment, consulta Cos'è Amazon Lookout for Equipment? nella Guida per l'utente di Amazon Lookout for Equipment.

  Quando crei una previsione per addestrare un modello ML a rilevare il comportamento anomalo delle apparecchiature, AWS IoT SiteWise invia i valori delle proprietà degli asset a Lookout for Equipment per addestrare un modello ML per rilevare il comportamento anomalo delle

apparecchiature. Per definire una definizione di previsione su un modello di asset, specifichi i ruoli IAM necessari a Lookout for Equipment per accedere ai tuoi dati e alle proprietà da inviare a Lookout for Equipment e inviare i dati elaborati ad Amazon S3. Per ulteriori informazioni, consulta Creazione dei modelli di asset.

Per integrare AWS IoT SiteWise e Lookout for Equipment, dovrai eseguire i seguenti passaggi di alto livello:

- Aggiungi una definizione di previsione su un modello di asset che delinei le proprietà che desideri monitorare. La definizione di previsione è una raccolta riutilizzabile di misurazioni, trasformazioni e metriche utilizzata per creare previsioni sugli asset basati su quel modello di asset.
- Addestra la previsione in base ai dati storici che fornisci.
- Pianifica l'inferenza, che indica la AWS IoT SiteWise frequenza con cui eseguire una previsione specifica.

Una volta pianificata l'inferenza, il modello Lookout for Equipment monitora i dati ricevuti dalle apparecchiature e cerca anomalie nel comportamento delle apparecchiature. È possibile visualizzare e analizzare i risultati in SiteWise Monitor, utilizzando le operazioni dell'API AWS IoT SiteWise GET o la console Lookout for Equipment. Puoi anche creare allarmi utilizzando i rilevatori di allarme del modello Asset per avvisarti del comportamento anomalo delle apparecchiature.

Argomenti

Aggiungere una definizione di previsione (console)

Per iniziare a inviare i dati raccolti da AWS IoT SiteWise a Lookout for Equipment, è necessario aggiungere AWS IoT SiteWise una definizione di previsione a un modello di asset.

Per aggiungere una definizione di previsione a un modello di asset AWS IoT SiteWise

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegliete Modelli e selezionate il modello di asset a cui desiderate aggiungere la definizione di previsione.
3. Scegliete Previsioni.
4. Scegli Aggiungi definizione di previsione.
5. Definisci i dettagli sulla definizione della previsione.
   a. Inserisci un nome e una descrizione univoci per la definizione della previsione. Scegli il nome con attenzione perché dopo aver creato la definizione di previsione, non puoi cambiarne il nome.
   b. Crea o seleziona un ruolo di autorizzazione IAM che AWS IoT SiteWise consenta di condividere i dati delle tue risorse con Amazon Lookout for Equipment. Il ruolo deve avere le seguenti politiche IAM e trust. Per informazioni sulla creazione del ruolo, consulta Creazione di un ruolo utilizzando politiche di fiducia personalizzate (console).

      Policy IAM

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "L4EPermissions",
            "Effect": "Allow",
            "Action": [
                "lookoutequipment:CreateDataset",
                "lookoutequipment:CreateModel",
                "lookoutequipment:CreateInferenceScheduler",
                "lookoutequipment:DescribeDataset",
                "lookoutequipment:DescribeDataIngestionJob",
                "lookoutequipment:DescribeModel",
                "lookoutequipment:DescribeInferenceScheduler",
```

```
                "lookoutequipment:ListInferenceExecutions",
                "lookoutequipment:StartDataIngestionJob",
                "lookoutequipment:StartInferenceScheduler",
                "lookoutequipment:UpdateInferenceScheduler",
                "lookoutequipment:StopInferenceScheduler"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:PutObject",
                "s3:GetObject"
            ],
            "Resource": ["arn:aws:s3:::iotsitewise-*"]
        },
        {
            "Sid": "IAMPermissions",
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam:::role/*"
        }
    ]
}
```

Policy di trust

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

```
                    "aws:SourceAccount": "account_id"
```

```
                },
                "ArnEquals": {
                    "aws:SourceArn":
 "arn:aws:iotsitewise:region:account_id:asset/*"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "lookoutequipment.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "account_id"
                },
                "ArnEquals": {
                    "aws:SourceArn":
 "arn:aws:lookoutequipment:region:account_id:*"
                }
            }
        }
    ]
}
```

c. Seleziona Avanti.

6. Seleziona gli attributi dei dati (misurazioni, trasformazioni e metriche) che desideri inviare a Lookout for Equipment.

a. (Facoltativo) Seleziona le misurazioni.

b. (Facoltativo) Seleziona le trasformazioni.

c. (Facoltativo) Seleziona le metriche.

d. Seleziona Avanti.

7. Rivedi le tue selezioni. Per aggiungere la definizione di previsione al modello di asset, nella pagina di riepilogo, scegli Aggiungi definizione di previsione.

Puoi anche modificare o eliminare una definizione di previsione esistente a cui sono allegate previsioni attive.

Addestramento di una previsione (console)

Dopo aver aggiunto una definizione di previsione a un modello di asset, puoi addestrare le previsioni relative ai tuoi asset.

Per addestrare una previsione in AWS IoT SiteWise

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Risorse e seleziona la risorsa che desideri monitorare.
3. Scegliete Previsioni.
4. Seleziona i pronostici che desideri addestrare.
5. In Azioni, scegli Inizia allenamento ed esegui le seguenti operazioni:
   a. In Dettagli di previsione, seleziona un ruolo di autorizzazione IAM che AWS IoT SiteWise consenta di condividere i dati degli asset con Lookout for Equipment. Se devi creare un nuovo ruolo, scegli Crea un nuovo ruolo.
   b. Per le impostazioni dei dati di allenamento, inserisci un intervallo temporale dei dati di allenamento per selezionare quali dati utilizzare per addestrare la previsione.
   c. (Facoltativo) Per le etichette dati, fornisci un bucket Amazon S3 e un prefisso che contenga i dati di etichettatura. Per ulteriori informazioni sui dati di etichettatura, consulta Etichettatura dei dati nella Amazon Lookout for Equipment User Guide.
   d. Seleziona Avanti.
6. (Facoltativo) Se desideri che la previsione sia attiva non appena ha completato l'allenamento, in Impostazioni avanzate, seleziona Attiva automaticamente la previsione dopo l'allenamento, quindi procedi come segue:
   a. In Dati di input, per Frequenza di caricamento dei dati, definisci la frequenza di caricamento dei dati e per il tempo di ritardo di Offset, definisci la quantità di buffer da utilizzare.
   b. Seleziona Avanti.
7. Controlla i dettagli del pronostico e scegli Salva e inizia.

Avvio o interruzione dell'inferenza su una previsione (console)

> **Note**
>
> I costi di Lookout for Equipment si applicano alle inferenze programmate con i dati trasferiti AWS IoT SiteWise tra e Lookout for Equipment. Per ulteriori informazioni, consulta i prezzi di Amazon Lookout for Equipment.

Se hai aggiunto una previsione ma non hai scelto di attivarla dopo l'allenamento, devi attivarla per iniziare a monitorare le tue risorse.

Per avviare l'inferenza per una previsione

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Risorse e seleziona la risorsa a cui viene aggiunta la previsione.
3. Scegliete Previsioni.
4. Seleziona le previsioni che desideri attivare.
5. In Azioni, scegli Avvia inferenza ed esegui le seguenti operazioni:
   a. In Dati di input, per Frequenza di caricamento dei dati, definisci la frequenza di caricamento dei dati e per il tempo di ritardo di Offset, definisci la quantità di buffer da utilizzare.
   b. Scegli Salva e inizia.

Per interrompere l'inferenza per una previsione

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Risorse e seleziona la risorsa a cui viene aggiunta la previsione.
3. Scegliete Previsioni.
4. Seleziona i pronostici che desideri interrompere.
5. In Azioni, scegli Stop inference.

Aggiungere una definizione di previsione (CLI)

Per definire una definizione di previsione su un modello di asset nuovo o esistente, puoi utilizzare (). AWS Command Line Interface AWS CLI Dopo aver definito la definizione di previsione sul modello di asset, addestrate e pianificate l'inferenza per una previsione su un asset per eseguire il rilevamento delle anomalie con AWS IoT SiteWise Lookout for Equipment.

Prerequisiti

Per completare questi passaggi, è necessario disporre di un modello di asset e creare almeno una risorsa. Per ulteriori informazioni, consultare Creazione di un modello di asset (AWS CLI) e Creare una risorsa (AWS CLI).

Se non lo sapete AWS IoT SiteWise, dovete chiamare l'operazione `CreateBulkImportJob` API per importare i valori delle proprietà dell'asset AWS IoT SiteWise, che verranno utilizzati per addestrare il modello. Per ulteriori informazioni, consulta Crea un processo di importazione in blocco ()AWS CLI.

Per aggiungere una definizione di previsione

1. Crea un file denominato `asset-model-payload.json`. Segui i passaggi descritti in queste altre sezioni per aggiungere i dettagli del tuo modello di asset al file, ma non inviare la richiesta per creare o aggiornare il modello di asset.
   - Per ulteriori informazioni su come creare un modello di asset, consulta Creazione di un modello di asset (AWS CLI)
   - Per ulteriori informazioni su come aggiornare un modello di asset esistente, consulta Aggiornamento di un modello di asset o componente ()AWS CLI
2. Aggiungete un modello composito Lookout for Equipment `assetModelCompositeModels` () al modello di asset aggiungendo il codice seguente.
   - Sostituitelo *`Property`* con l'ID delle proprietà che desiderate includere. Per ottenere quegli ID, chiama `DescribeAssetModel`.
   - Sostituiscilo *`RoleARN`* con l'ARN di un ruolo IAM che consente a Lookout for Equipment di accedere ai tuoi dati. AWS IoT SiteWise

```
{
  ...
  "assetModelCompositeModels": [
    {
      "name": "L4Epredictiondefinition",
      "type": "AWS/L4E_ANOMALY",
      "properties": [
          {
            "name": "AWS/L4E_ANOMALY_RESULT",
            "dataType": "STRUCT",
            "dataTypeSpec": "AWS/L4E_ANOMALY_RESULT",
            "unit": "none",
            "type": {
              "measurement": {}
            }
          },
          {
            "name": "AWS/L4E_ANOMALY_INPUT",
            "dataType": "STRUCT",
            "dataTypeSpec": "AWS/L4E_ANOMALY_INPUT",
            "type": {
               "attribute": {
                 "defaultValue": "{\"properties\": [\"Property1\",
 \"Property2\"]}"
               }
            }
          },
          {
            "name": "AWS/L4E_ANOMALY_PERMISSIONS",
            "dataType": "STRUCT",
            "dataTypeSpec": "AWS/L4E_ANOMALY_PERMISSIONS",
            "type": {
              "attribute": {
                "defaultValue": "{\"roleArn\": \"RoleARN\"}"
              }
            }
          },
          {
            "name": "AWS/L4E_ANOMALY_DATASET",
            "dataType": "STRUCT",
            "dataTypeSpec": "AWS/L4E_ANOMALY_DATASET",
            "type": {
```

```
                "attribute": {}
            }
          },
          {
            "name": "AWS/L4E_ANOMALY_MODEL",
            "dataType": "STRUCT",
            "dataTypeSpec": "AWS/L4E_ANOMALY_MODEL",
            "type": {
              "attribute": {}
            }
          },
          {
            "name": "AWS/L4E_ANOMALY_INFERENCE",
            "dataType": "STRUCT",
            "dataTypeSpec": "AWS/L4E_ANOMALY_INFERENCE",
            "type": {
              "attribute": {}
            }
          },
          {
            "name": "AWS/L4E_ANOMALY_TRAINING_STATUS",
            "dataType": "STRUCT",
            "dataTypeSpec": "AWS/L4E_ANOMALY_TRAINING_STATUS",
            "type": {
              "attribute": {
                "defaultValue": "{}"
              }
            }
          },
          {
            "name": "AWS/L4E_ANOMALY_INFERENCE_STATUS",
            "dataType": "STRUCT",
            "dataTypeSpec": "AWS/L4E_ANOMALY_INFERENCE_STATUS",
            "type": {
              "attribute": {
                "defaultValue": "{}"
              }
            }
          }
    ]
}
```

3. Crea il modello di asset o aggiorna il modello di asset esistente. Esegui una di queste operazioni:

- Per creare il modello di asset, esegui il seguente comando:

```
aws iotsitewise create-asset-model --cli-input-json file://asset-model-
payload.json
```

- Per aggiornare il modello di asset esistente, esegui il comando seguente. Sostituitelo *asset-model-id* con l'ID del modello di asset che desiderate aggiornare.

```
aws iotsitewise update-asset-model \
  --asset-model-id asset-model-id \
  --cli-input-json file://asset-model-payload.json
```

Dopo aver eseguito il comando, `assetModelId` annotatelo nella risposta.

Addestramento di una previsione e inizio dell'inferenza (CLI)

Ora che la definizione di previsione è stata definita, potete addestrare gli asset in base ad essa e avviare l'inferenza. Se vuoi addestrare la tua previsione ma non iniziare l'inferenza, passa a. Addestramento di una previsione (CLI) Per addestrare la previsione e iniziare l'inferenza sulla risorsa, avrai bisogno della `assetId` risorsa di destinazione.

Per addestrare e avviare l'inferenza della previsione

1. Esegui il seguente comando per trovare quanto segue`assetModelCompositeModelId`. `assetModelCompositeModelSummaries` *asset-model-id*Sostituitelo con l'ID del modello di asset in cui avete creatoAggiornamento di un modello di asset o componente ()AWS CLI.

   ```
   aws iotsitewise describe-asset-model \
     --asset-model-id asset-model-id \
   ```

2. Eseguite il comando seguente per trovare `actionDefinitionId` l'`TrainingWithInference`azione. Sostituisci *asset-model-id*con l'ID utilizzato nel passaggio precedente e sostituisci *asset-model-composite-model-id*con l'ID restituito nel passaggio precedente.

   ```
   aws iotsitewise describe-asset-model-composite-model \
     --asset-model-id asset-model-id \
   ```

```
  --asset-model-composite-model-id asset-model-composite-model-id \
```

3. Create un file chiamato `train-start-inference-prediction.json` e aggiungete il codice seguente, sostituendo il seguente:
   - *asset-id*con l'ID della risorsa di destinazione
   - *action-definition-id*con l'ID dell' TrainingWithInference azione
   - *StartTime*con l'inizio dei dati di allenamento, forniti in secondi d'epoca
   - *EndTime*con i dati di fine addestramento, forniti in secondi d'epoca

```
{
  "targetResource": {
    "assetId": "asset-id"
  },
  "actionDefinitionId": "action-definition-Id",
  "actionPayload":{
    "stringValue": "{\"l4ETrainingWithInference\":{\"trainingWithInferenceMode
\":\"START\",\"trainingPayload\":{\"exportDataStartTime\":StartTime,
\"exportDataEndTime\":EndTime},\"inferencePayload\":{\"dataDelayOffsetInMinutes
\":0,\"dataUploadFrequency\":\"PT5M\"}}}"
  }
}
```

4. Esegui il seguente comando per avviare l'addestramento e l'inferenza:

```
aws iotsitewise execute-action --cli-input-json file://train-start-inference-
prediction.json
```

Addestramento di una previsione (CLI)

Ora che la definizione di previsione è stata definita, puoi addestrare gli asset in base ad essa. Per addestrare la previsione sull'asset, avrai bisogno della risorsa `assetId` di destinazione.

Per addestrare la previsione

1. Esegui il seguente comando per trovare quanto segue`assetModelCompositeModelId`. `assetModelCompositeModelSummaries` *asset-model-id*Sostituitelo con l'ID del

modello di asset in cui avete creatoAggiornamento di un modello di asset o componente ()AWS CLI.

```
aws iotsitewise describe-asset-model \
  --asset-model-id asset-model-id \
```

2. Eseguite il comando seguente per trovare `actionDefinitionId` l'`Training`azione. Sostituisci *`asset-model-id`*con l'ID utilizzato nel passaggio precedente e sostituisci *`asset-model-composite-model-id`*con l'ID restituito nel passaggio precedente.

```
aws iotsitewise describe-asset-model-composite-model \
  --asset-model-id asset-model-id \
  --asset-model-composite-model-id asset-model-composite-model-id \
```

3. Create un file chiamato `train-prediction.json` e aggiungete il codice seguente, sostituendo il seguente:
   - *`asset-id`*con l'ID della risorsa di destinazione
   - *`action-definition-id`*con l'ID dell'azione formativa
   - *`StartTime`*con i dati di inizio dell'allenamento, forniti in secondi epocali
   - *`EndTime`*con i dati di fine addestramento, forniti in secondi d'epoca
   - (Facoltativo) *`BucketName`* con il nome del bucket Amazon S3 che contiene i dati dell'etichetta
   - (Facoltativo) *`Prefix`* con il prefisso associato al bucket Amazon S3.

   > **Note**
   >
   > Includi sia il nome che il prefisso del bucket o nessuno dei due.

```
{
  "targetResource": {
    "assetId": "asset-id"
  },
  "actionDefinitionId": "action-definition-Id",
  "actionPayload":{ "stringValue": "{\"l4ETraining\": {\"trainingMode\":
\"START\",\"exportDataStartTime\": StartTime, \"exportDataEndTime\": EndTime,
 \"labelInputConfiguration\": {\"bucketName\": \"BucketName\", \"prefix\":
 \"Prefix\"}}}"
```

```
}
```

```
}
```

4. Esegui il seguente comando per iniziare l'allenamento:

```
aws iotsitewise execute-action --cli-input-json file://train-prediction.json
```

Prima di iniziare l'inferenza, è necessario completare l'addestramento. Per verificare lo stato della formazione, effettuate una delle seguenti operazioni:

- Dalla console, accedi alla risorsa su cui si basa la previsione.

- Da AWS CLI, chiama `BatchGetAssetPropertyValue` utilizzando l'indirizzo `propertyId` della `trainingStatus` proprietà.

Avvio o interruzione dell'inferenza su una previsione (CLI)

Una volta addestrata la previsione, puoi avviare l'inferenza per dire a Lookout for Equipment di iniziare a monitorare le tue risorse. Per avviare o interrompere l'inferenza, avrai bisogno della risorsa `assetId` di destinazione.

Per iniziare l'inferenza

1. Esegui il seguente comando per trovare il `assetModelCompositeModelId` sotto`assetModelCompositeModelSummaries`. *`asset-model-id`*Sostituitelo con l'ID del modello di asset in cui avete creatoAggiornamento di un modello di asset o componente ()AWS CLI.

```
aws iotsitewise describe-asset-model \
  --asset-model-id asset-model-id \
```

2. Eseguite il comando seguente per trovare `actionDefinitionId` l'`Inference`azione. Sostituisci *`asset-model-id`*con l'ID utilizzato nel passaggio precedente e sostituisci *`asset-model-composite-model-id`*con l'ID restituito nel passaggio precedente.

```
aws iotsitewise describe-asset-model-composite-model \
  --asset-model-id asset-model-id \
  --asset-model-composite-model-id asset-model-composite-model-id \
```

3. Create un file chiamato `start-inference.json` e aggiungete il codice seguente, sostituendo il seguente:

   - *`asset-id`*con l'ID della risorsa di destinazione
   - *`action-definition-id`*con l'ID dell'azione di inferenza iniziale
   - *`Offset`*con la quantità di buffer da usare
   - *`Frequency`*con la frequenza con cui vengono caricati i dati

   ```
   {
     "targetResource": {
       "assetId": "asset-id"
     },
     "actionDefinitionId": "action-definition-Id",
     "actionPayload":{ "stringValue": "{\"l4EInference\": {\"inferenceMode\":
   \"START\",\"dataDelayOffsetInMinutes\": Offset, \"dataUploadFrequency\":
    \"Frequency\"}}"
   }}
   ```

4. Esegui il seguente comando per avviare l'inferenza:

   ```
   aws iotsitewise execute-action --cli-input-json file://start-inference.json
   ```

Per interrompere l'inferenza

1. Esegui il seguente comando per trovare il `assetModelCompositeModelId` sotto`assetModelCompositeModelSummaries`. *`asset-model-id`*Sostituitelo con l'ID del modello di asset in cui avete creatoAggiornamento di un modello di asset o componente ()AWS CLI.

   ```
   aws iotsitewise describe-asset-model \
     --asset-model-id asset-model-id \
   ```

2. Eseguite il comando seguente per trovare `actionDefinitionId` l'`Inferenceazione`. Sostituisci *`asset-model-id`*con l'ID utilizzato nel passaggio precedente e sostituisci *`asset-model-composite-model-id`*con l'ID restituito nel passaggio precedente.

   ```
   aws iotsitewise describe-asset-model-composite-model \
     --asset-model-id asset-model-id \
   ```

```
  --asset-model-composite-model-id asset-model-composite-model-id \
```

3. Create un file chiamato `stop-inference.json` e aggiungete il codice seguente, sostituendo il seguente:
   - *`asset-id`*con l'ID della risorsa di destinazione
   - *`action-definition-id`*con l'ID dell'azione di inferenza iniziale

```
{
  "targetResource": {
    "assetId": "asset-id"
  },
  "actionDefinitionId": "action-definition-Id",
  "actionPayload":{ "stringValue": "{\"l4EInference\":{\"inferenceMode\":\"STOP
\"}}"
}}
```

4. Esegui il comando seguente per interrompere l'inferenza:

```
aws iotsitewise execute-action --cli-input-json file://stop-inference.json
```

.

Visualizza le operazioni

Configura SiteWise Monitor per creare applicazioni web per i tuoi dipendenti operativi. Le applicazioni web aiutano i dipendenti a visualizzare le vostre operazioni. Gestisci vari livelli di accesso per i tuoi dipendenti utilizzando IAM Identity Center o IAM. Configura accessi e autorizzazioni unici per ogni dipendente per visualizzare sottoinsiemi specifici di un'intera operazione industriale. AWS IoT SiteWise fornisce una guida applicativa per questi dipendenti per imparare a usare Monitor. SiteWise

Per ulteriori informazioni sulla visualizzazione delle operazioni, vedere Monitoraggio dei dati con AWS IoT SiteWise Monitor

Archivia dati

Puoi integrare lo storage di serie temporali con il tuo data lake industriale. AWS IoT SiteWise dispone di tre livelli di storage per i dati industriali:

- Un livello di archiviazione a caldo ottimizzato per applicazioni in tempo reale.
- Un livello di storage caldo ottimizzato per carichi di lavoro analitici.
- Un livello di cold storage gestito dal cliente che utilizza Amazon S3 per applicazioni di dati operativi con elevata tolleranza di latenza.

AWS IoT SiteWise ti aiuta a gestire i costi di storage conservando i dati recenti nel livello di archiviazione a caldo. Quindi, si definiscono le politiche di conservazione dei dati per spostare i dati storici su uno storage di livello caldo o freddo. Per ulteriori informazioni, consulta

È possibile AWS IoT SiteWise configurare il salvataggio dei dati nei seguenti livelli di storage:

Livello più elevato

L'hot storage tier è uno storage AWS IoT SiteWise gestito in serie temporali. Hot tier è più efficace per i dati a cui si accede di frequente, con bassa write-to-read latenza. I dati archiviati nell'hot tier vengono utilizzati dalle applicazioni industriali che richiedono un accesso rapido ai valori più recenti delle misurazioni delle apparecchiature. Ciò include applicazioni che visualizzano metriche in tempo reale con una dashboard interattiva o applicazioni che monitorano le operazioni e lanciano allarmi per identificare problemi di prestazioni.

Per impostazione predefinita, i dati inseriti vengono archiviati nel livello più AWS IoT SiteWise elevato. È possibile definire un periodo di conservazione per il livello caldo, dopodiché AWS IoT SiteWise spostare i dati nel livello più elevato su uno storage di livello caldo o freddo, in base alla configurazione. Per ottimizzare le prestazioni e l'efficienza in termini di costi, imposta il periodo di conservazione dei livelli più elevati in modo che sia più lungo del tempo necessario per recuperare spesso i dati. Viene utilizzato per metriche, allarmi e scenari di monitoraggio in tempo reale. Se non è impostato un periodo di conservazione, i dati vengono archiviati a tempo indeterminato nel livello più elevato.

Livello caldo

Il warm storage tier è un livello AWS IoT SiteWise gestito efficace per l'archiviazione economica dei dati storici. È ideale per recuperare grandi volumi di dati con caratteristiche di latenza media write-to-read . Utilizza il livello «warm» per archiviare i dati storici necessari per carichi di lavoro di grandi dimensioni. Ad esempio, viene utilizzato per il recupero dei dati per analisi, applicazioni di business intelligence (BI), strumenti di reporting e formazione di modelli di machine learning (ML). Se si abilita il livello di conservazione a freddo, è possibile definire un periodo di conservazione del livello caldo. Al termine del periodo di conservazione, AWS IoT SiteWise elimina i dati dal livello caldo.

Livello freddo

Il livello di cold storage utilizza un bucket Amazon S3 per archiviare dati usati raramente. Con il cold tier abilitato, AWS IoT SiteWise replica le serie temporali, incluse misurazioni, metriche, trasformazioni e aggregazioni e le definizioni dei modelli di asset ogni 6 ore. Cold tier viene utilizzato per archiviare dati che tollerano un'elevata latenza di lettura per report cronologici e backup.

Argomenti

Configurare le impostazioni di archiviazione

È possibile configurare le impostazioni di archiviazione per attivare lo storage warm tier gestito dal servizio e anche per replicare i dati sul piano freddo. Per ulteriori informazioni sul periodo di conservazione per i livelli caldo e caldo, consultaImpatto sulla conservazione dei dati. Durante la configurazione delle impostazioni di archiviazione, procedi come segue:

- Conservazione a livello elevato: imposta un periodo di conservazione per quanto tempo i dati vengono archiviati nel livello più elevato prima che vengano eliminati e spostati nello storage a livello caldo o a livello freddo gestito dal servizio in base alle impostazioni di archiviazione. AWS IoT SiteWise eliminerà tutti i dati del livello più elevato che esistevano prima della fine del periodo di conservazione. Se non imposti un periodo di conservazione, i tuoi dati vengono archiviati a tempo indeterminato nel livello più elevato.
- Conservazione a livello caldo: imposta un periodo di conservazione per quanto tempo i dati vengono archiviati nel livello caldo prima che vengano eliminati dallo AWS IoT SiteWise storage e trasferiti nello storage cold tier gestito dal cliente. AWS IoT SiteWise elimina tutti i dati dal livello caldo che esisteva prima della fine del periodo di conservazione. Se non è impostato un periodo di conservazione, i dati vengono archiviati a tempo indeterminato nel livello caldo.

> **Note**
>
> Per migliorare le prestazioni delle query, imposta un periodo di conservazione di livello elevato con lo storage di livello caldo.

Impatto della conservazione dei dati nello storage di livello caldo e caldo

- Quando si riduce il periodo di conservazione dello storage hot tier, i dati vengono trasferiti in modo permanente dal livello caldo a quello caldo o freddo. Quando si riduce il periodo di conservazione del livello caldo, i dati vengono spostati sul livello freddo ed eliminati definitivamente dal livello caldo.
- Quando si aumenta il periodo di conservazione dello storage di livello caldo o caldo, la modifica influisce sui dati inviati AWS IoT SiteWise da quel momento in poi. AWS IoT SiteWise non recupera i dati dallo storage a caldo o a freddo per inserirli nel livello più caldo. Ad esempio, se il periodo di conservazione dello storage hot tier è inizialmente impostato su 30 giorni e poi aumentato a 60 giorni, occorrono 30 giorni perché lo storage hot tier contenga 60 giorni di dati.

Argomenti

Configura le impostazioni di archiviazione per il livello caldo (console)

La procedura seguente mostra come configurare le impostazioni di archiviazione per replicare i dati sul livello warm della AWS IoT SiteWise console.

Per configurare le impostazioni di archiviazione nella console

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, in Impostazioni, scegli Archiviazione.
3. Nell'angolo in alto a destra, scegliere Edit (Modifica).
4. Nella pagina Modifica spazio di archiviazione, procedi come segue:

5. Per le impostazioni Hot tier, procedi come segue:

   - Se desideri impostare un periodo di conservazione per il periodo di archiviazione dei dati nel livello più elevato prima di essere eliminati e spostati nello storage di livello caldo gestito dal servizio, scegli Abilita periodo di conservazione.
   - Per configurare un periodo di conservazione, inserisci un numero intero e scegli un'unità. Il periodo di conservazione deve essere maggiore o uguale a 30 giorni.

   AWS IoT SiteWise elimina tutti i dati del livello più importante che sono più vecchi del periodo di conservazione. Se non imposti un periodo di conservazione, i dati vengono archiviati a tempo indeterminato.

6. (Consigliato) Per le impostazioni del livello Warm, procedi come segue:

   - Per attivare l'archiviazione di livello caldo, seleziona Confermo e attiva l'opzione di archiviazione di livello caldo per attivare l'archiviazione di livello caldo.
   - (Facoltativo) Per configurare un periodo di conservazione, inserisci un numero intero e scegli un'unità. Il periodo di conservazione deve essere maggiore o uguale a 365 giorni.

   AWS IoT SiteWise elimina i dati del livello «warm» che esistevano prima del periodo di conservazione. Se non imposti un periodo di conservazione, i dati vengono archiviati a tempo indeterminato.

   > **Note**
   >
   > - Quando si opta per il livello caldo, la configurazione viene visualizzata una sola volta.
   > - Per impostare la conservazione a caldo, è necessario disporre di un livello di archiviazione a caldo o a freddo. Per l'efficienza in termini di costi e il recupero dei dati storici, AWS IoT SiteWise consiglia di archiviare i dati a lungo termine nel livello caldo.
   > - Per impostare la conservazione del livello caldo, è necessario disporre di un livello di conservazione a freddo.

7. Scegli Salva per salvare le impostazioni di archiviazione.

Nella sezione AWS IoT SiteWise Archiviazione, lo storage Warm tier si trova in uno di questi stati:

- Abilitato: se i dati esistevano prima del periodo di conservazione del livello più elevato, li AWS IoT SiteWise sposta nel livello caldo».

- Disabilitato: lo storage warm tier è disabilitato.

Configura le impostazioni di archiviazione per warm tier (AWS CLI)

È possibile configurare le impostazioni di archiviazione per spostare i dati al livello caldo utilizzando AWS CLI i comandi seguenti.

Per evitare di sovrascrivere la configurazione esistente, recupera le informazioni sulla configurazione di archiviazione corrente eseguendo il comando seguente:

```
aws iotsitewise describe-storage-configuration
```

Example risposta senza una configurazione di livello freddo esistente

```
{
         "storageType": "SITEWISE_DEFAULT_STORAGE",
         "disassociatedDataStorage": "ENABLED",
         "configurationStatus": {
             "state": "ACTIVE"
         },
         "lastUpdateDate": "2021-10-14T15:53:35-07:00",
         "warmTier": "DISABLED"
}
```

Example risposta con la configurazione Cold Tier esistente

```
{
      "storageType": "MULTI_LAYER_STORAGE",
         "multiLayerStorage": {
           "customerManagedS3Storage": {
           "s3ResourceArn": "arn:aws:s3:::bucket-name/prefix/",
```

```
      },
       "configurationStatus": {
       "state": "ACTIVE"
      },
      "lastUpdateDate": "2023-10-25T15:59:46-07:00",
      "warmTier": "DISABLED"
}
```

Configura le impostazioni di archiviazione per il piano caldo con AWS CLI

Esegui il comando seguente per configurare le impostazioni di archiviazione. Sostituisci `file-name` con il nome del file che contiene la configurazione AWS IoT SiteWise di archiviazione.

```
aws iotsitewise put-storage-configuration --cli-input-json file://file-name.json
```

Example AWS IoT SiteWise configurazione con livello caldo e caldo

```
{
            "storageType": "SITEWISE_DEFAULT_STORAGE",
            "disassociatedDataStorage": "ENABLED",
            "warmTier": "ENABLED",
            "retentionPeriod": {
               "numberOfDays": hot-tier-retention-in-days
             }

}
```

`hot-tier-retention-in-days`deve essere un numero intero maggiore o uguale a 30 giorni.

Example response

```
{
```

Configura le impostazioni di archiviazione con AWS CLI un piano freddo esistente

Configura le impostazioni di archiviazione utilizzando AWS CLI lo storage a livello freddo esistente

- Esegui il comando seguente per configurare le impostazioni di archiviazione. Sostituisci *file-name* con il nome del file che contiene la configurazione AWS IoT SiteWise di archiviazione.

```
aws iotsitewise put-storage-configuration --cli-input-json file://file-name.json
```

Example AWS IoT SiteWise configurazione dello storage

- Sostituisci *bucket-name con il nome del* tuo bucket Amazon S3.
- Sostituisci il *prefisso* con il tuo prefisso Amazon S3.
- Sostituiscilo *aws-account-id*con l'ID del tuo account. AWS
- Sostituisci *role-name* con il nome del ruolo di accesso Amazon S3 che AWS IoT SiteWise consente di inviare dati ad Amazon S3.
- Sostituisci *hot-tier-retention-in-days* con un numero intero maggiore o uguale a 30 giorni.
- Sostituisci *warm-tier-retention-in-days* con un numero intero maggiore o uguale a 365 giorni.

> **Note**
>
> AWS IoT SiteWise eliminerà tutti i dati del livello caldo più vecchi del periodo di conservazione del livello freddo. Se non imposti un periodo di conservazione, i dati vengono archiviati a tempo indeterminato.

```
{
      "storageType": "MULTI_LAYER_STORAGE",
        "multiLayerStorage": {
          "customerManagedS3Storage": {
              "s3ResourceArn": "arn:aws:s3:::bucket-name/prefix/",
              "roleArn": "arn:aws:iam::aws-account-id:role/role-name"
              }
          },
    "disassociatedDataStorage": "ENABLED",
```

```
    "retentionPeriod": {
      "numberOfDays": hot-tier-retention-in-days
    },
    "warmTier": "ENABLED",
    "warmTierRetentionPeriod": {
      "numberOfDays": warm-tier-retention-in-days
    }
}
```

Example response

```
{
      "storageType": "MULTI_LAYER_STORAGE",
      "configurationStatus": {
        "state": "UPDATE_IN_PROGRESS"
       }
}
```

Configura le impostazioni di archiviazione per il livello freddo (console)

La procedura seguente mostra come configurare le impostazioni di archiviazione per replicare i dati nel livello freddo della AWS IoT SiteWise console.

Per configurare le impostazioni di archiviazione nella console

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, in Impostazioni, scegli Archiviazione.
3. Nell'angolo in alto a destra, scegliere Edit (Modifica).
4. Nella pagina Modifica spazio di archiviazione, procedi come segue:
   a. Per le impostazioni di archiviazione, scegli Abilita archiviazione a freddo. La memorizzazione a livello freddo è disabilitata per impostazione predefinita.
   b. Per la posizione del bucket S3, inserisci il nome di un bucket Amazon S3 esistente e un prefisso.

> **Note**
>
> - Amazon S3 utilizza il prefisso come nome di cartella nel bucket Amazon S3. Il prefisso deve contenere da 1 a 255 caratteri e terminare con una barra (/). AWS IoT SiteWise I dati vengono salvati in questa cartella.
> - Se non disponi di un bucket Amazon S3, scegli Visualizza, quindi creane uno nella console Amazon S3. Per ulteriori informazioni, consulta Crea il tuo primo bucket S3 nella Amazon S3 User Guide.

c. Per il ruolo di accesso S3, esegui una delle seguenti operazioni:

- Scegli Crea un ruolo da un modello AWS gestito, crea AWS automaticamente un ruolo IAM che consente di AWS IoT SiteWise inviare dati ad Amazon S3.
- Scegli Usa un ruolo esistente, quindi scegli il ruolo che hai creato dall'elenco.

> **Note**
>
> - È necessario utilizzare lo stesso nome di bucket Amazon S3 per la posizione del bucket S3 utilizzato nel passaggio precedente e nella policy IAM.
> - Assicurati che il tuo ruolo disponga delle autorizzazioni mostrate nell'esempio seguente.
>
>   Example politica delle autorizzazioni:

```
{
      "Version": "2012-10-17",
      "Statement": [
          {
              "Effect": "Allow",
              "Action": [
                  "s3:PutObject",
                  "s3:GetObject",
                  "s3:DeleteObject",
                  "s3:GetBucketLocation",
                  "s3:ListBucket"
              ],
              "Resource": [
                  "arn:aws:s3:::bucket-name",
```

```
                "arn:aws:s3:::bucket-name/*"
            ]
        }
    ]
}
```

Sostituisci *bucket-name* con il nome del tuo bucket Amazon S3.

d. Per configurare l'hot tier, consulta la Fase 5 del Configura le impostazioni di archiviazione per il livello caldo (console)

e. (Facoltativo) Per AWS IoT Analytics l'integrazione, procedi come segue.

i. Se desideri utilizzarli AWS IoT Analytics per interrogare i tuoi dati, scegli Archivio AWS IoT Analytics dati abilitato.

ii. AWS IoT SiteWise genera un nome per il tuo data store oppure puoi inserire un nome diverso.

AWS IoT SiteWise crea automaticamente un data store in AWS IoT Analytics cui salvare i dati. Per interrogare i dati, puoi usarli AWS IoT Analytics per creare set di dati. Per ulteriori informazioni, consulta Lavorare con AWS IoT SiteWise i dati nella Guida per l'AWS IoT Analytics utente.

f. Selezionare Salva.

Nella sezione AWS IoT SiteWise Archiviazione, lo storage Cold tier può avere uno dei seguenti valori:

- Abilitato: AWS IoT SiteWise replica i dati nel bucket Amazon S3 specificato.
- Abilitazione: AWS IoT SiteWise sta elaborando la richiesta per abilitare lo storage a freddo. Il completamento di questo processo può richiedere diversi minuti.
- Enable_Failed: AWS IoT SiteWise impossibile elaborare la tua richiesta di abilitare lo storage a freddo. Se hai abilitato AWS IoT SiteWise l'invio di log ad Amazon CloudWatch Logs, puoi utilizzare questi log per risolvere i problemi. Per ulteriori informazioni, consulta Monitoraggio con Amazon CloudWatch Logs.
- Disabilitato: lo storage a livello freddo è disabilitato.

Configura le impostazioni di archiviazione per il livello freddo (AWS CLI)

La procedura seguente mostra come configurare le impostazioni di archiviazione per replicare i dati nel livello freddo utilizzando AWS CLI.

Per configurare le impostazioni di archiviazione utilizzando AWS CLI

1. Per esportare i dati in un bucket Amazon S3 nel tuo account, esegui il seguente comando per configurare le impostazioni di archiviazione. Sostituisci *file-name* con il nome del file che contiene la configurazione di storage. AWS IoT SiteWise

   ```
   aws iotsitewise put-storage-configuration --cli-input-json file://file-name.json
   ```

   Example AWS IoT SiteWise configurazione dello storage

   - Sostituisci *bucket-name con il nome del* tuo bucket Amazon S3.
   - Sostituisci il *prefisso* con il tuo prefisso Amazon S3.
   - Sostituiscilo *aws-account-id*con l'ID del tuo account. AWS
   - Sostituisci *role-name* con il nome del ruolo di accesso Amazon S3 che AWS IoT SiteWise consente di inviare dati ad Amazon S3.
   - Sostituisci *retention-in-days*con un numero intero maggiore o uguale a 30 giorni.

   ```
   {
         "storageType": "MULTI_LAYER_STORAGE",
         "multiLayerStorage": {
             "customerManagedS3Storage": {
                 "s3ResourceArn": "arn:aws:s3:::bucket-name/prefix/",
                 "roleArn": "arn:aws:iam::aws-account-id:role/role-name"
             }
         },
         "retentionPeriod": {
             "numberOfDays": retention-in-days,
             "unlimited": false
         }
     }
   ```

Note

- È necessario utilizzare lo stesso nome di bucket Amazon S3 nella configurazione AWS IoT SiteWise dello storage e nella policy IAM.
- Assicurati che il tuo ruolo disponga delle autorizzazioni mostrate nell'esempio seguente.
  Example politica delle autorizzazioni:

```
{
      "Version": "2012-10-17",
      "Statement": [
          {
              "Effect": "Allow",
              "Action": [
                  "s3:PutObject",
                  "s3:GetObject",
                  "s3:DeleteObject",
                  "s3:GetBucketLocation",
                  "s3:ListBucket"
              ],
              "Resource": [
                  "arn:aws:s3:::bucket-name",
                  "arn:aws:s3:::bucket-name/*"
              ]
          }
      ]
  }
```

  Sostituisci *bucket-name* con il nome del tuo bucket Amazon S3.

Example response

```
{
    "storageType": "MULTI_LAYER_STORAGE",
    "retentionPeriod": {
        "numberOfDays": 100,
        "unlimited": false
```

```
    },
    "configurationStatus": {
        "state": "UPDATE_IN_PROGRESS"
    }
}
```

> **Note**
>
> L'aggiornamento della configurazione di storage può richiedere alcuni minuti. AWS IoT SiteWise

2. Per recuperare le informazioni sulla configurazione dello storage, esegui il comando seguente.

```
aws iotsitewise describe-storage-configuration
```

Example response

```
{
      "storageType": "MULTI_LAYER_STORAGE",
      "multiLayerStorage": {
          "customerManagedS3Storage": {
              "s3ResourceArn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/torque/",
              "roleArn": "arn:aws:iam::123456789012:role/SWAccessS3Role"
          }
      },
      "retentionPeriod": {
          "numberOfDays": 100,
          "unlimited": false
      },
      "configurationStatus": {
          "state": "ACTIVE"
      },
      "lastUpdateDate": "2021-03-30T15:54:14-07:00"
  }
```

3. Per interrompere l'esportazione dei dati nel bucket Amazon S3, esegui il seguente comando per configurare le impostazioni di archiviazione.

```
aws iotsitewise put-storage-configuration --storage-type SITEWISE_DEFAULT_STORAGE
```

> **Note**
>
> Per impostazione predefinita, i tuoi dati vengono archiviati solo nel livello più elevato di. AWS IoT SiteWise

Example response

```
{
      "storageType": "SITEWISE_DEFAULT_STORAGE",
      "configurationStatus": {
          "state": "UPDATE_IN_PROGRESS"
      }
  }
```

4. Per recuperare le informazioni sulla configurazione dello storage, esegui il comando seguente.

```
aws iotsitewise describe-storage-configuration
```

Example response

```
{
      "storageType": "SITEWISE_DEFAULT_STORAGE",
      "configurationStatus": {
          "state": "ACTIVE"
      },
      "lastUpdateDate": "2021-03-30T15:57:14-07:00"
  }
```

(Facoltativo) Creare un archivio AWS IoT Analytics dati ()AWS CLI

Un AWS IoT Analytics data store è un repository scalabile e interrogabile che riceve e archivia dati. Puoi utilizzare la AWS IoT SiteWise console o le AWS IoT Analytics API per creare un archivio dati per salvare AWS IoT Analytics i tuoi dati. AWS IoT SiteWise Per interrogare i dati, crei set di dati utilizzando. AWS IoT Analytics Per ulteriori informazioni, consulta Lavorare con AWS IoT SiteWise i dati nella Guida per l'AWS IoT Analytics utente.

I passaggi seguenti consentono AWS CLI di creare un archivio dati in AWS IoT Analytics.

Per creare un archivio dati, esegui il comando seguente. Sostituisci *file-name* con il nome del file che contiene la configurazione del data store.

```
aws iotanalytics create-datastore --cli-input-json file://file-name.json
```

> **Note**
>
> - È necessario specificare il nome di un bucket Amazon S3 esistente. Se non disponi di un bucket Amazon S3, creane prima uno. Per ulteriori informazioni, consulta Crea il tuo primo bucket S3 nella Guida per l'utente di Amazon S3.

- È necessario utilizzare lo stesso nome di bucket Amazon S3 nella configurazione AWS IoT SiteWise dello storage, nella policy IAM e nella configurazione del AWS IoT Analytics data store.

Example AWS IoT Analytics configurazione del data store

Sostituisci *s3-bucket-name con il nome del* tuo AWS IoT Analytics data store *data-store-name*e il nome del bucket Amazon S3.

```
{
    "datastoreName": "data-store-name",
    "datastoreStorage": {
        "iotSiteWiseMultiLayerStorage": {
            "customerManagedS3Storage": {
                "bucket": "s3-bucket-name"
            }
        }
    },
    "retentionPeriod": {
        "numberOfDays": 90
    }
```

```
    "retentionPeriod": {
        "numberOfDays": 90,
        "unlimited": false
    }
}
```

Risoluzione dei problemi relativi alle impostazioni di archiviazione

Utilizza le seguenti informazioni per individuare e risolvere i problemi relativi alla configurazione dello storage.

Problemi

Errore: il bucket non esiste

Soluzione: AWS IoT SiteWise non è stato possibile trovare il bucket Amazon S3. Assicurati di inserire il nome di un bucket Amazon S3 esistente nella regione corrente.

Errore: accesso negato al percorso Amazon S3

Soluzione: AWS IoT SiteWise impossibile accedere al tuo bucket Amazon S3. Esegui questa operazione:

- Assicurati di utilizzare lo stesso bucket Amazon S3 specificato nella policy IAM.
- Assicurati che il tuo ruolo disponga delle autorizzazioni mostrate nell'esempio seguente.

  Example policy di autorizzazioni

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
```

```
                "s3:GetObject",
```

```
                "s3:DeleteObject",
                "s3:GetBucketLocation",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ]
        }
    ]
}
```

Sostituisci *bucket-name* con il nome del tuo bucket Amazon S3.

Errore: non è possibile assumere il ruolo ARN

Soluzione: non AWS IoT SiteWise potrei assumere il ruolo IAM per tuo conto. Assicurati che il tuo ruolo si affidi al seguente servizio:`iotsitewise.amazonaws.com`. Per ulteriori informazioni, consulta Non posso assumere un ruolo, consulta la Guida per l'utente IAM.

Errore: accesso al bucket Amazon S3 interregionale non riuscito

Soluzione: il bucket Amazon S3 che hai specificato si trova in una regione diversa. AWS Assicurati che il bucket e gli AWS IoT SiteWise asset Amazon S3 si trovino nella stessa regione.

Percorsi dei file e schemi di dati salvati nella fase fredda

AWS IoT SiteWise archivia i dati nella fase fredda replicando serie temporali, tra cui misurazioni, metriche, trasformazioni e aggregazioni, nonché definizioni di asset e modelli di asset. Di seguito vengono descritti i percorsi dei file e gli schemi dei dati inviati al livello freddo.

Argomenti

- Dati dell'attrezzatura (misurazioni)
- Metriche, trasformazioni e aggregazioni
- Metadati delle risorse
- metadati della gerarchia degli asset
- File di indice dei dati di archiviazione

Dati dell'attrezzatura (misurazioni)

AWS IoT SiteWise esporta i dati dell'apparecchiatura (misurazioni) nella zona fredda una volta ogni sei ore. I dati grezzi vengono salvati nel livello freddo nel formato Apache AVRO (`.avro`).

Percorso del file

AWS IoT SiteWise memorizza i dati dell'apparecchiatura (misurazioni) nel livello freddo utilizzando il seguente modello.

```
{keyPrefix}/raw/startYear={startYear}/startMonth={startMonth}/startDay={startDay}/
```

```
seriesBucket={seriesBucket}/raw_{timeseriesId}_{startTimestamp}_{quality}.avro
```

Ogni percorso di file verso i dati grezzi in Amazon S3 contiene i seguenti componenti.

`keyPrefix`	Il prefisso Amazon S3 che hai specificato nella configurazione dello AWS IoT SiteWise storage. Amazon S3 utilizza il prefisso come nome di cartella nel bucket.
`raw`	La cartella che memorizza i dati delle serie temporali provenienti dall'apparecchiatura (misurazioni). La `raw` cartella viene salvata nella cartella dei prefissi.
`seriesBucket`	Un numero esadecimale compreso tra 00 e ff. Questo numero è derivato da. `timeSerieId` Questa partizione viene utilizzata per aumentare la velocità effettiva durante le operazioni di AWS IoT SiteWise scrittura sul livello freddo. Quando usi Amazon Athena per eseguire query, puoi utilizzare la partizione per il partizionamento fine per migliorare le prestazioni delle query. `seriesBucket` e `timeSeriesBucket` nei metadati degli asset c'è lo stesso numero.

`startYear`	L'anno dell'ora di inizio esclusiva associata ai dati delle serie temporali.
`startMonth`	Il mese dell'ora di inizio esclusiva associata ai dati delle serie temporali.
`startDay`	Il giorno del mese dell'ora di inizio esclusiva associata ai dati delle serie temporali.
`fileName`	Il nome del file utilizza il carattere di sottoline atura (_) come delimitatore per separare quanto segue: • Il prefisso. `raw` • Il `timeSeriesId` valore. • Il timestamp dell'epoca dell'ora di inizio esclusiva associata ai dati delle serie temporali. • La qualità dei dati. Valori validi: `GOODBAD`, e`UNCERTAIN` . Per ulteriori informazioni, AssetPropertyValueconsulta l'AWS IoT SiteWise API Reference. Il file viene salvato nel `.avro` formato utilizzan do la compressione Snappy.

Componente del percorso	Descrizione

Example percorso del file verso i dati grezzi nella fase fredda

```
keyPrefix/raw/startYear=2021/startMonth=1/startDay=2/seriesBucket=a2/
raw_7020c8e2-e6db-40fa-9845-ed0dddd4c77d_95e63da7-d34e-43e1-
bc6f-1b490154b07a_1609577700_GOOD.avro
```

Campi

Lo schema dei dati grezzi esportati nel livello freddo contiene i seguenti campi.

`seriesId`	`string`	N/D	L'ID che identifica i dati delle serie temporali provenienti dall'apparecchiatura (misurazioni). È possibile utilizzare questo campo per unire dati grezzi e metadati delle risorse nelle query.
`timeInSeconds`	`long`	N/D	La data e l'ora, in secondi, nel formato Unix epoch.
			I dati frazionari in nanosecondi sono forniti da. `offsetInNanos`
`offsetInNanos`	`long`	N/D	L'offset in nanosecondi da. `timeInSeconds`
`quality`	`string`	N/D	La qualità del valore delle serie temporali.
`doubleValue`	`double` o `null`	`null`	Dati di serie temporali di tipo double (numero in virgola mobile).
`stringValue`	`string` o `null`	`null`	Dati di serie temporali di tipo string (sequenza di caratteri).

integerValue	int o null	null	Dati di serie temporali di tipo intero (numero intero).
booleanValue	boolean o null	null	Dati di serie temporali di tipo booleano (vero o falso).
jsonValue	string o null	null	Dati di serie temporali di tipo JSON (tipi di dati complessi memorizzati come stringa).
recordVersion	long o null	null	Il numero di versione del record. È possibile utilizzare il numero di versione per selezionare il record più recente. I record più recenti hanno numeri di versione più grandi.
Nome del campo	Tipi supportati	Tipo di predefinito	Descrizione

Example dati grezzi nella fase fredda


```
{"seriesId":"e9687d2a-0dbe-4f65-9ed6-6f443cba41f7_95e63da7-d34e-43e1-
bc6f-1b490154b07a","timeInSeconds":1625675887,"offsetInNanos":0,"quality":"GOOD","doubleValue":
{"double":0.75},"stringValue":null,"integerValue":null,"booleanValue":null,"jsonValue":null,"re
  {"seriesId":"e9687d2a-0dbe-4f65-9ed6-6f443cba41f7_95e63da7-d34e-43e1-
bc6f-1b490154b07a","timeInSeconds":1625675889,"offsetInNanos":0,"quality":"GOOD","doubleValue":
{"double":0.69},"stringValue":null,"integerValue":null,"booleanValue":null,"jsonValue":null,"re
  {"seriesId":"e9687d2a-0dbe-4f65-9ed6-6f443cba41f7_95e63da7-d34e-43e1-
bc6f-1b490154b07a","timeInSeconds":1625675890,"offsetInNanos":0,"quality":"GOOD","doubleValue":
```

```
  {"seriesId":"e9687d2a-0dbe-4f65-9ed6-6f443cba41f7_95e63da7-d34e-43e1-
bc6f-1b490154b07a","timeInSeconds":1625675891,"offsetInNanos":0,"quality":"GOOD","doubleValue":
{"double":0.92},"stringValue":null,"integerValue":null,"booleanValue":null,"jsonValue":null,"re
  {"seriesId":"e9687d2a-0dbe-4f65-9ed6-6f443cba41f7_95e63da7-d34e-43e1-
bc6f-1b490154b07a","timeInSeconds":1625675892,"offsetInNanos":0,"quality":"GOOD","doubleValue":
{"double":0.73},"stringValue":null,"integerValue":null,"booleanValue":null,"jsonValue":null,"re
```

Metriche, trasformazioni e aggregazioni

AWS IoT SiteWise esporta metriche, trasforma e aggrega nel livello freddo una volta ogni sei ore. Le metriche, le trasformazioni e gli aggregati vengono salvati nel livello freddo nel formato Apache AVRO (). `.avro`

Percorso del file

AWS IoT SiteWise archivia metriche, trasformazioni e aggregazioni nel livello freddo utilizzando il seguente modello.

```
{keyPrefix}/agg/startYear={startYear}/startMonth={startMonth}/startDay={startDay}/
seriesBucket={seriesBucket}/agg_{timeseriesId}_{startTimestamp}_{quality}.avro
```

Ogni percorso di file verso metriche, trasformazioni e aggregazioni in Amazon S3 contiene i seguenti componenti.

`keyPrefix`	Il prefisso Amazon S3 che hai specificato nella configurazione dello AWS IoT SiteWise storage. Amazon S3 utilizza il prefisso come nome di cartella nel bucket.
`agg`	La cartella che memorizza i dati delle serie temporali provenienti dalle metriche. La `agg` cartella viene salvata nella cartella dei prefissi.
`seriesBucket`	Un numero esadecimale compreso tra 00 e ff. Questo numero è derivato da. `timeSerieId` Questa partizione viene utilizzata per aumentare la velocità effettiva durante le

	operazioni di AWS IoT SiteWise scrittura sul livello freddo. Quando usi Amazon Athena per eseguire query, puoi utilizzare la partizione per il partizionamento fine per migliorare le prestazioni delle query.
	`seriesBucket` e `timeSeriesBucket` nei metadati degli asset c'è lo stesso numero.
`startYear`	L'anno dell'ora di inizio esclusiva associata ai dati delle serie temporali.
`startMonth`	Il mese dell'ora di inizio esclusiva associata ai dati delle serie temporali.
`startDay`	Il giorno del mese dell'ora di inizio esclusiva associata ai dati delle serie temporali.
`fileName`	Il nome del file utilizza il carattere di sottolineatura (_) come delimitatore per separare quanto segue: • Il prefisso. `raw` • Il `timeSeriesId` valore. • Il timestamp dell'epoca dell'ora di inizio esclusiva associata ai dati delle serie temporali. • La qualità dei dati. Valori validi: `GOODBAD`, e`UNCERTAIN` . Per ulteriori informazioni, AssetPropertyValueconsulta l'AWS IoT SiteWise API Reference. Il file viene salvato nel `.avro` formato utilizzando la compressione Snappy.

Componente del percorso	Descrizione

Example percorso del file verso le metriche nella fase fredda

```
keyPrefix/agg/startYear=2021/startMonth=1/startDay=2/seriesBucket=a2/
agg_7020c8e2-e6db-40fa-9845-ed0dddd4c77d_95e63da7-d34e-43e1-
bc6f-1b490154b07a_1609577700_GOOD.avro
```

Campi

Lo schema di metriche, trasformazioni e aggregati esportati nel livello freddo contiene i seguenti campi.

`seriesId`	`string`	N/D	L'ID che identifica i dati delle serie temporali provenienti da apparecchiature, metriche o trasformazioni. È possibile utilizzare questo campo per unire dati non elaborati e metadati delle risorse nelle query.
`timeInSeconds`	`long`	N/D	La data e l'ora, in secondi, nel formato Unix epoch. I dati frazionari in nanosecondi sono forniti da. `offsetInNanos`
`offsetInNanos`	`long`	N/D	L'offset in nanosecondi da. `timeInSeconds`

`quality`	`string`	N/D	La qualità con cui filtrare i dati degli asset.
`resolution`	`string`	N/D	L'intervallo di tempo in cui aggregare i dati.
`count`	`double` o `null`	`null`	Il numero totale di punti dati per le variabili specificate nell'intervallo di tempo corrente.
`average`	`double` o `null`	`null`	La media dei valori delle variabili specificate nell'intervallo di tempo corrente.
`min`	`double` o `null`	`null`	Il minimo dei valori delle variabili specificate nell'intervallo di tempo corrente.
`max`	`boolean` o `null`	`null`	Il massimo dei valori delle variabili specificate nell'intervallo di tempo corrente.
`sum`	`string` o `null`	`null`	La somma dei valori delle variabili specificate nell'intervallo di tempo corrente.

`recordVersion`	`long` o `null`	`null`	Il numero di versione del record. È possibile utilizzare il numero di versione per selezionare il record più recente. I record più recenti hanno numeri di versione più grandi.

Nome del campo	Tipi supportati	Tipo di predefinito	Descrizione

Example Dati metrici nella fase fredda


```
{"seriesId":"f74c2828-5317-4df3-
ba16-6d41b5bcb531","timeInSeconds":1637334060,"offsetInNanos":0,"quality":"GOOD","resolution":"
{"double":16.0},"min":{"double":1.0},"max":{"double":31.0},"sum":
{"double":496.0},"recordVersion":null}
  {"seriesId":"f74c2828-5317-4df3-
ba16-6d41b5bcb531","timeInSeconds":1637334120,"offsetInNanos":0,"quality":"GOOD","resolution":"
{"double":46.0},"min":{"double":32.0},"max":{"double":60.0},"sum":
{"double":1334.0},"recordVersion":null}
  {"seriesId":"f74c2828-5317-4df3-
ba16-6d41b5bcb531","timeInSeconds":1637334540,"offsetInNanos":0,"quality":"GOOD","resolution":"
{"double":16.0},"min":{"double":1.0},"max":{"double":31.0},"sum":
{"double":496.0},"recordVersion":null}
  {"seriesId":"f74c2828-5317-4df3-
ba16-6d41b5bcb531","timeInSeconds":1637334600,"offsetInNanos":0,"quality":"GOOD","resolution":"
{"double":46.0},"min":{"double":32.0},"max":{"double":60.0},"sum":
```

esporta i metadati degli asset nel livello solo quando modificate le definizioni dei modelli di asset o le definizioni degli asset. I metadati delle risorse vengono salvati nel livello freddo nel formato JSON () delimitato da nuova riga. `.ndjson`

Percorso del file

AWS IoT SiteWise archivia i metadati delle risorse nel livello freddo utilizzando il seguente modello.

```
{keyPrefix}/asset_metadata/asset_{assetId}.ndjson
```

Ogni percorso di file verso i metadati delle risorse nel livello freddo contiene i seguenti componenti.

Componente del percorso	Descrizione
`keyPrefix`	Il prefisso Amazon S3 che hai specificato nella configurazione di storage AWS IoT SiteWise s. Amazon S3 utilizza il prefisso come nome di cartella nel bucket.
`asset_metadata`	La cartella in cui sono archiviati i metadati delle risorse. La `asset_metadata` cartella viene salvata nella cartella dei prefissi.
`fileName`	Il nome del file utilizza il carattere di sottoline atura (_) come delimitatore per separare quanto segue: • Il prefisso. `asset` • Il `assetId` valore. Il file viene salvato nel `.ndjson` formato.

Example percorso del file ai metadati delle risorse nel livello più freddo

```
keyPrefix/asset_metadata/asset_35901915-d476-4dca-8637-d9ed4df939ed.ndjson
```

Campi

Lo schema dei metadati delle risorse che viene esportato nel livello freddo contiene i seguenti campi.

`assetId`	L'ID dell'asset .
`assetName`	Il nome della risorsa.
`assetExternalId`	L'ID esterno della risorsa.
`assetModelId`	L'ID del modello di asset utilizzato per creare questa risorsa.
`assetModelName`	Il nome del modello di asset.
`assetModelExternalId`	L'ID esterno del modello di asset.
`assetPropertyId`	L'ID della proprietà dell'asset.
`assetPropertyName`	Il nome della proprietà dell'asset.
`assetPropertyExternalId`	L'ID esterno della proprietà dell'asset.
`assetPropertyDataType`	Il tipo di dati della proprietà dell'asset.
`assetPropertyUnit`	L'unità della proprietà dell'asset (ad esempio, `Newtons` e`RPM`).
`assetPropertyAlias`	L'alias che identifica la proprietà dell'asset, ad esempio il percorso del flusso di dati del server OPC-UA (ad esempio,). `/company/windfarm/3/turbine/7/temperature`
`timeSeriesId`	L'ID che identifica i dati delle serie temporali provenienti da apparecchiature, metriche o trasformazioni. È possibile utilizzare questo campo per unire dati non elaborati e metadati delle risorse nelle query.
`timeSeriesBucket`	Un numero esadecimale compreso tra 00 e ff. Questo numero è derivato da. `timeSerie`

	`sId` Questa partizione viene utilizzata per aumentare la velocità effettiva durante le operazioni di AWS IoT SiteWise scrittura sul livello freddo. Quando usi Amazon Athena per eseguire query, puoi utilizzare la partizione per il partizionamento fine per migliorare le prestazioni delle query. `timeSeriesBucket` e `seriesBucket` nel percorso del file i dati grezzi sono presenti gli stessi numeri.
`assetCompositeModelId`	L'ID del modello composito.
`assetCompositeModelExternalId`	L'ID esterno del modello composito.
`assetCompositeModelDescription`	La descrizione del modello composito.
`assetCompositeModelName`	Il nome del modello composito.
`assetCompositeModelType`	Il tipo del modello composito. Per i modelli compositi di allarme, questo tipo è `AWS/ALARM` .
`assetCreationDate`	La data di creazione della risorsa, nell'epoca di Unix.
`assetLastUpdateDate`	La data dell'ultimo aggiornamento della risorsa, espressa in Unix Epoch Time.
`assetStatusErrorCode`	Il codice di errore.
`assetStatusErrorMessage`	Messaggio di errore.
`assetStatusState`	Lo stato attuale della risorsa.
Nome campo	Descrizione

Example metadati degli asset nella fase fredda


```
  {"assetId":"7020c8e2-e6db-40fa-9845-
ed0dddd4c77d","assetExternalId":null,"assetName":"Wind Turbine Asset
 2","assetModelId":"ec1d924f-f07d-444f-b072-
e2994c165d35","assetModelExternalId":null,"assetModelName":"Wind
 Turbine Asset Model","assetPropertyId":"95e63da7-d34e-43e1-
bc6f-1b490154b07a","assetPropertyExternalId":null,"assetPropertyName":"Temperature","assetPrope
Washington/Seattle/WT2/temp","timeSeriesId":"7020c8e2-e6db-40fa-9845-
ed0dddd4c77d_95e63da7-d34e-43e1-
bc6f-1b490154b07a","timeSeriesBucket":"f6","assetArn":null,"assetCompositeModelDescription":nul
  {"assetId":"7020c8e2-e6db-40fa-9845-
ed0dddd4c77d","assetExternalId":null,"assetName":"Wind Turbine Asset
 2","assetModelId":"ec1d924f-f07d-444f-b072-
e2994c165d35","assetModelExternalId":null,"assetModelName":"Wind Turbine Asset
 Model","assetPropertyId":"c706d54d-4c11-42dc-9a01-63662fc697b4","assetPropertyExternalId":null
Washington/Seattle/WT2/pressure","timeSeriesId":"7020c8e2-e6db-40fa-9845-
ed0dddd4c77d_c706d54d-4c11-42dc-9a01-63662fc697b4","timeSeriesBucket":"1e","assetArn":null,"ass
  {"assetId":"7020c8e2-e6db-40fa-9845-
ed0dddd4c77d","assetExternalId":null,"assetName":"Wind Turbine Asset
 2","assetModelId":"ec1d924f-f07d-444f-b072-
e2994c165d35","assetModelExternalId":null,"assetModelName":"Wind
 Turbine Asset Model","assetPropertyId":"8cf1162f-dead-4fbe-b468-
c8e24cde9f50","assetPropertyExternalId":null,"assetPropertyName":"Max
```

modifiche al modello degli asset o alle definizioni degli asset. I metadati della gerarchia degli asset vengono salvati nel livello freddo nel formato JSON () delimitato da nuova riga. `.ndjson`

Un identificatore esterno per la gerarchia, la risorsa di destinazione o la risorsa di origine viene recuperato chiamando l'API. DescribeAsset

Percorso del file

AWS IoT SiteWise archivia i metadati della gerarchia degli asset nel livello freddo utilizzando il seguente modello.

```
{keyPrefix}/asset_hierarchy_metadata/{parentAssetId}_{hierarchyId}.ndjson
```

Ogni percorso di file verso i metadati della gerarchia degli asset nel livello freddo contiene i seguenti componenti.

Componente del percorso	Descrizione
`keyPrefix`	Il prefisso Amazon S3 che hai specificato nella configurazione dello AWS IoT SiteWise storage. Amazon S3 utilizza il prefisso come nome di cartella nel bucket.
`asset_hierarchy_metadata`	La cartella che memorizza i metadati della gerarchia degli asset. La `asset_hie`
	`rarchy_metadata` cartella viene salvata nella cartella dei prefissi.
`fileName`	Il nome del file utilizza il carattere di sottoline atura (_) come delimitatore per separare quanto segue: • Il valore. `parentAssetId` • Il `hierarchyId` valore.
	Il file viene salvato nel `.ndjson` formato.

Example percorso del file ai metadati della gerarchia degli asset nel livello freddo

```
keyPrefix/asset_hierarchy_metadata/35901915-d476-4dca-8637-
d9ed4df939ed_c5b3ced8-589a-48c7-9998-cdccfc9747a0.ndjson
```

Campi

Lo schema dei metadati della gerarchia degli asset che viene esportato nel livello freddo contiene i seguenti campi.

Nome campo	Descrizione
`sourceAssetId`	L'ID della risorsa di origine in questa relazione tra asset.
`targetAssetId`	L'ID della risorsa di destinazione in questa relazione tra asset.
`hierarchyId`	L'ID della gerarchia.
`associationType`	Il tipo di associazione di questa relazione tra asset.
	Il valore deve essere`CHILD`. La risorsa di destinazione è una risorsa secondaria della risorsa di origine.

Example metadati della gerarchia degli asset nel livello freddo

```
{"sourceAssetId":"80388e72-2284-44fb-9c89-
bfbaf0dfedd2","targetAssetId":"2b866c25-0c74-4750-bdf5-
b73683c8a2a2","hierarchyId":"bbed9f59-0412-4585-
a61d-6044db526aee","associationType":"CHILD"}
  {"sourceAssetId":"80388e72-2284-44fb-9c89-
bfbaf0dfedd2","targetAssetId":"6b51246e-984d-460d-
bc0b-470ea47d1e31","hierarchyId":"bbed9f59-0412-4585-
a61d-6044db526aee","associationType":"CHILD"}
```

Per visualizzare i dati nella fase fredda

1. Accedi alla console Amazon S3.
2. Nel pannello di navigazione, scegli Bucket, quindi scegli il tuo bucket Amazon S3.
3. Passa alla cartella che contiene i dati grezzi, i metadati degli asset o i metadati della gerarchia degli asset.
4. Seleziona i file, quindi da Azioni scegli Scarica.

File di indice dei dati di archiviazione

AWS IoT SiteWise utilizza questi file per ottimizzare le prestazioni delle query di dati. Vengono visualizzati nel bucket Amazon S3, ma non è necessario utilizzarli.

Percorso del file

AWS IoT SiteWise archivia i file di indice dei dati nella fase fredda utilizzando il seguente modello.

```
keyPrefix/index/series=timeseriesId/startYear=startYear/startMonth=startMonth/
startDay=startDay/index_timeseriesId_startTimestamp_quality
```

Example percorso del file del file di indice di archiviazione dei dati

```
keyPrefix/index/series=7020c8e2-e6db-40fa-9845-ed0dddd4c77d_95e63da7-
d34e-43e1-bc6f-1b490154b07a/startYear=2022/startMonth=02/startDay=03/
index_7020c8e2-e6db-40fa-9845-ed0dddd4c77d_95e63da7-d34e-43e1-
bc6f-1b490154b07a_1643846400_GOOD
```

.

Puoi anche importare ed esportare i metadati delle risorse. Per ulteriori informazioni, consulta

Quando abiliti AWS IoT SiteWise l'esportazione dei dati nel livello freddo per la prima volta, i metadati degli asset vengono esportati nel livello freddo. Dopo la configurazione iniziale, AWS IoT SiteWise esporta i metadati degli asset nel livello solo quando modificate le definizioni dei modelli di asset o le definizioni degli asset. I metadati delle risorse vengono salvati nel livello freddo nel formato JSON () delimitato da nuova riga. `.ndjson`

Percorso del file

AWS IoT SiteWise archivia i metadati delle risorse nel livello freddo utilizzando il seguente modello.

```
{keyPrefix}/asset_metadata/asset_{assetId}.ndjson
```

Ogni percorso di file verso i metadati delle risorse nel livello freddo contiene i seguenti componenti.

Componente del percorso	Descrizione
`keyPrefix`	Il prefisso Amazon S3 che hai specificato nella configurazione di storage AWS IoT SiteWise s. Amazon S3 utilizza il prefisso come nome di cartella nel bucket.
`asset_metadata`	La cartella in cui sono archiviati i metadati delle risorse. La `asset_metadata` cartella viene salvata nella cartella dei prefissi.
`fileName`	Il nome del file utilizza il carattere di sottoline atura (_) come delimitatore per separare quanto segue: • Il prefisso. `asset` • Il `assetId` valore. Il file viene salvato nel `.ndjson` formato.

Example percorso del file ai metadati delle risorse nel livello più freddo

```
keyPrefix/asset_metadata/asset_35901915-d476-4dca-8637-d9ed4df939ed.ndjson
```

Campi

Lo schema dei metadati delle risorse che viene esportato nel livello freddo contiene i seguenti campi.

`assetId`	L'ID dell'asset .
`assetName`	Il nome della risorsa.

`assetExternalId`	L'ID esterno della risorsa.
`assetModelId`	L'ID del modello di asset utilizzato per creare questa risorsa.
`assetModelName`	Il nome del modello di asset.
`assetModelExternalId`	L'ID esterno del modello di asset.
`assetPropertyId`	L'ID della proprietà dell'asset.
`assetPropertyName`	Il nome della proprietà dell'asset.
`assetPropertyExternalId`	L'ID esterno della proprietà dell'asset.
`assetPropertyDataType`	Il tipo di dati della proprietà dell'asset.
`assetPropertyUnit`	L'unità della proprietà dell'asset (ad esempio, `Newtons` e `RPM`).
`assetPropertyAlias`	L'alias che identifica la proprietà dell'asset, ad esempio il percorso del flusso di dati del server OPC-UA (ad esempio,). `/company/windfarm/3/turbine/7/temperature`
`timeSeriesId`	L'ID che identifica i dati delle serie temporali provenienti da apparecchiature, metriche o trasformazioni. È possibile utilizzare questo campo per unire dati non elaborati e metadati delle risorse nelle query.

`timeSeriesBucket`	Un numero esadecimale compreso tra 00 e ff. Questo numero è derivato da. `timeSeriesId` Questa partizione viene utilizzata per aumentare la velocità effettiva durante le operazioni di AWS IoT SiteWise scrittura sul livello freddo. Quando usi Amazon Athena per eseguire query, puoi utilizzare la partizione e per il partizionamento fine per migliorare le prestazioni delle query. `timeSeriesBucket` e `seriesBucket` nel percorso del file i dati grezzi sono presenti gli stessi numeri.
`assetCompositeModelId`	L'ID del modello composito.
`assetCompositeModelExternalId`	L'ID esterno del modello composito.
`assetCompositeModelDescription`	La descrizione del modello composito.
`assetCompositeModelName`	Il nome del modello composito.
`assetCompositeModelType`	Il tipo del modello composito. Per i modelli compositi di allarme, questo tipo è `AWS/ALARM` .
`assetCreationDate`	La data di creazione della risorsa, nell'epoca di Unix.
`assetLastUpdateDate`	La data dell'ultimo aggiornamento della risorsa, espressa in Unix Epoch Time.
`assetStatusErrorCode`	Il codice di errore.
`assetStatusErrorMessage`	Messaggio di errore.
`assetStatusState`	Lo stato attuale della risorsa.
Nome campo	Descrizione

Example metadati degli asset nella fase fredda


```
 {"assetId":"7020c8e2-e6db-40fa-9845-
ed0dddd4c77d","assetExternalId":null,"assetName":"Wind Turbine Asset
 2","assetModelId":"ec1d924f-f07d-444f-b072-
e2994c165d35","assetModelExternalId":null,"assetModelName":"Wind
 Turbine Asset Model","assetPropertyId":"95e63da7-d34e-43e1-
bc6f-1b490154b07a","assetPropertyExternalId":null,"assetPropertyName":"Temperature","assetPrope
Washington/Seattle/WT2/temp","timeSeriesId":"7020c8e2-e6db-40fa-9845-
ed0dddd4c77d_95e63da7-d34e-43e1-
bc6f-1b490154b07a","timeSeriesBucket":"f6","assetArn":null,"assetCompositeModelDescription":nul
 {"assetId":"7020c8e2-e6db-40fa-9845-
ed0dddd4c77d","assetExternalId":null,"assetName":"Wind Turbine Asset
 2","assetModelId":"ec1d924f-f07d-444f-b072-
e2994c165d35","assetModelExternalId":null,"assetModelName":"Wind Turbine Asset
 Model","assetPropertyId":"c706d54d-4c11-42dc-9a01-63662fc697b4","assetPropertyExternalId":null
Washington/Seattle/WT2/pressure","timeSeriesId":"7020c8e2-e6db-40fa-9845-
ed0dddd4c77d_c706d54d-4c11-42dc-9a01-63662fc697b4","timeSeriesBucket":"1e","assetArn":null,"ass
 {"assetId":"7020c8e2-e6db-40fa-9845-
ed0dddd4c77d","assetExternalId":null,"assetName":"Wind Turbine Asset
 2","assetModelId":"ec1d924f-f07d-444f-b072-
e2994c165d35","assetModelExternalId":null,"assetModelName":"Wind
 Turbine Asset Model","assetPropertyId":"8cf1162f-dead-4fbe-b468-
```

Integrazione con altri servizi

AWS IoT SiteWise si integra con diversi AWS servizi per sviluppare una AWS IoT soluzione completa nel AWS cloud. Per ulteriori informazioni, consulta Interazione con altri servizi AWS

AWS IoT SiteWise concetti

Di seguito sono riportati i concetti fondamentali di AWS IoT SiteWise:

Aggregazione

Gli aggregati sono metriche fondamentali, o misurazioni, che calcolano AWS IoT SiteWise automaticamente tutti i dati delle serie temporali. Per ulteriori informazioni, consulta Esecuzione di query sugli aggregati delle proprietà di asset.

Asset

Quando si inseriscono o si inseriscono dati AWS IoT SiteWise dalle apparecchiature industriali, tutti i dispositivi, le apparecchiature e i processi vengono visualizzati come risorse. A ogni risorsa sono associati dati. Ad esempio, un'apparecchiatura potrebbe avere un numero di serie, un'ubicazione, una marca e un modello e una data di installazione. Potrebbe anche avere valori di serie temporali relativi a disponibilità, prestazioni, qualità, temperatura, pressione e altro. Raggruppa le risorse in gerarchie, consentendo alle risorse di accedere ai dati archiviati nelle risorse secondarie. Per ulteriori informazioni, consulta Modellazione degli asset industriali.

Gerarchia di asset

Imposta gerarchie di asset per creare rappresentazioni logiche delle tue operazioni industriali. A tale scopo, definite una gerarchia in un modello di asset e associate gli asset creati da quel modello alla gerarchia specificata. Le metriche degli asset principali possono combinare i dati delle proprietà degli asset secondari, consentendovi di calcolare metriche che offrono informazioni dettagliate sull'attività complessiva o su una parte specifica di essa. Per ulteriori informazioni, consulta Definizione delle gerarchie dei modelli di asset.

Modello di asset

Ogni risorsa viene creata utilizzando un modello di asset. I modelli di asset sono strutture che definiscono e standardizzano il formato degli asset. Garantiscono informazioni coerenti su più risorse dello stesso tipo, consentendoti di gestire i dati in risorse che rappresentano gruppi di dispositivi. In ogni modello di asset, è possibile definire attributi, input serie temporali (misure),

trasformazioni di serie temporali (trasformazioni), aggregazioni di serie temporali (parametri) e gerarchie di asset. Per ulteriori informazioni, consulta Modellazione degli asset industriali.

Decidete dove vengono elaborate le proprietà del vostro modello di asset configurando il modello di asset per l'edge. Utilizzate questa funzionalità per gestire e monitorare i dati degli asset sui dispositivi locali.

Proprietà di asset

Le proprietà degli asset sono le strutture all'interno di ciascun asset che contengono dati industriali. Ogni proprietà ha un tipo di dati e può anche avere un'unità. Una proprietà può essere un attributo, una misura, una trasformazione o un parametro. Per ulteriori informazioni, consulta Definizione delle proprietà dei dati.

Configura le proprietà degli asset per l'elaborazione periferica. Per ulteriori informazioni sull'elaborazione dei dati all'edge, consultathe section called “Abilitare l'elaborazione dei dati edge”.

Attributo

Gli attributi sono proprietà di una risorsa che in genere rimangono costanti, come il produttore del dispositivo o la posizione del dispositivo. Gli attributi possono avere valori preimpostati. Ogni risorsa creata da un modello di asset include i valori predefiniti degli attributi definiti in quel modello. Per ulteriori informazioni, consulta Definizione di dati statici (attributi).

Dashboard

Ogni progetto contiene un set di pannelli di controllo. I pannelli di controllo forniscono un set di visualizzazioni per i valori di un set di asset. I proprietari del progetto creano i pannelli di controllo e le visualizzazioni contenute. Quando il proprietario di un progetto è pronto a condividere il set di pannelli di controllo, il proprietario può invitare i visualizzatori al progetto, consentendo loro di accedere a tutti i pannelli di controllo del progetto. Se si desidera un set diverso di visualizzatori per pannelli di controllo diversi, è necessario dividere i pannelli di controllo tra i progetti. Quando gli spettatori guardano le dashboard, possono personalizzare l'intervallo di tempo per esaminare dati specifici.

Flusso di dati

Inserisci o inserisci dati industriali AWS IoT SiteWise ancor prima di creare modelli e asset di asset. AWS IoT SiteWise genera automaticamente flussi di dati per raccogliere flussi di dati grezzi dalle apparecchiature.

Alias del flusso di dati

Gli alias del flusso di dati consentono di identificare facilmente un flusso di dati. Ad esempio, l'alias `server1-windfarm/3/turbine/7/temperature` indica i valori di temperatura provenienti dalla turbina #7 del parco eolico #3. Il termine `server1` è il nome della fonte di dati che aiuta a identificare il server OPC-UA ed `server1-` è un prefisso allegato a tutti i flussi di dati riportati da questo server OPC-UA.

Associazione del flusso di dati

Dopo aver creato modelli e asset di asset, associate i flussi di dati alle proprietà degli asset definite negli asset per strutturare i dati. AWS IoT SiteWise può quindi utilizzare modelli e risorse di asset per gestire i dati in entrata dai flussi di dati. È inoltre possibile dissociare i flussi di dati dalle proprietà degli asset. Per ulteriori informazioni, consulta Gestione dei flussi di dati.

Formula

Ogni proprietà di trasformazione e metrica viene fornita con una formula che delinea come la proprietà trasforma o aggrega i dati. Queste formule includono input di proprietà, operatori e funzioni offerte da. AWS IoT SiteWise Per ulteriori informazioni, consulta Utilizzo delle espressioni di formula.

Misura

Le misurazioni sono proprietà di una risorsa che rappresenta i flussi di dati grezzi delle serie temporali del sensore provenienti da un dispositivo o un'apparecchiatura. Per ulteriori informazioni, consulta Definizione dei flussi di dati provenienti dalle apparecchiature (misurazioni).

Parametro

Le metriche sono proprietà di una risorsa che rappresentano dati aggregati di serie temporali. Ogni metrica è accompagnata da un'espressione matematica (formula) che descrive come aggregare i punti dati e da un intervallo di tempo per il calcolo di tale aggregazione. Le metriche generano un singolo punto dati per ogni intervallo di tempo specificato. Per ulteriori informazioni, consulta Aggregazione di dati da proprietà e altre risorse (metriche).

Pacchetti

SiteWise Gli edge gateway utilizzano pacchetti per determinare come raccogliere, elaborare e instradare i dati. Attualmente, AWS IoT SiteWise supporta il pacchetto di raccolta dati e il pacchetto di elaborazione dati. Per ulteriori informazioni sui pacchetti disponibili per il gateway SiteWise Edge, consultathe section called “Utilizzo dei pacchetti”.

Pacchetto di raccolta dati

Utilizza il pacchetto di raccolta dati in modo che il tuo gateway SiteWise Edge possa raccogliere i dati industriali e indirizzarli verso la AWS destinazione di tua scelta. Questo pacchetto viene aggiunto automaticamente al gateway SiteWise Edge e non può essere rimosso.

Pacchetto di elaborazione dati

Utilizza il pacchetto di elaborazione dati per elaborare i dati all'edge e conservarli per 30 giorni per utilizzarli nelle applicazioni locali.

Portal

Un AWS IoT SiteWise Monitor portale è un'applicazione web che puoi utilizzare per visualizzare e condividere i tuoi AWS IoT SiteWise dati. Un portale ha uno o più amministratori e contiene zero o più progetti.

Amministratore del portale

Ogni portale SiteWise Monitor dispone di uno o più amministratori del portale. Gli amministratori del portale utilizzano il portale per creare progetti che contengono raccolte di asset e pannelli di controllo. L'amministratore del portale assegna quindi asset e proprietari a ciascun progetto. Controllando l'accesso al progetto, gli amministratori del portale specificano quali asset possono vedere i proprietari e i visualizzatori del progetto.

Progetto

Ogni portale SiteWise Monitor contiene una serie di progetti. Ogni progetto ha un sottoinsieme di asset AWS IoT SiteWise associati. I proprietari del progetto creano uno o più pannelli di controllo per fornire un modo coerente per visualizzare i dati associati agli asset. I proprietari del progetto possono invitare i visualizzatori al progetto per consentire loro di visualizzare gli asset e i pannelli di controllo del progetto. Il progetto è l'unità di condivisione di base all'interno di SiteWise Monitor. I proprietari del progetto possono invitare gli utenti a cui l' AWS amministratore ha concesso l'accesso al portale. Un utente deve avere accesso a un portale prima che un progetto del portale possa essere condiviso con l'utente.

Proprietario del progetto

Ogni progetto SiteWise Monitor ha dei proprietari. I proprietari dei progetti creano visualizzazioni sotto forma di pannelli di controllo al fine di rappresentare i dati operativi in modo coerente. Una volta che i pannelli di controllo sono pronti per la condivisione, il proprietario del progetto

può invitare i visualizzatori al progetto. I proprietari del progetto possono anche assegnare altri proprietari al progetto. I proprietari dei progetti possono configurare le soglie e le impostazioni di notifica per gli allarmi.

Visualizzatore del progetto

Ogni progetto SiteWise Monitor ha dei visualizzatori. I visualizzatori del progetto possono connettersi al portale per visualizzare i pannelli di controllo creati dai proprietari del progetto. In ogni dashboard, i visualizzatori dei progetti possono regolare l'intervallo di tempo per comprendere meglio i dati operativi. I visualizzatori del progetto possono visualizzare solo i pannelli di controllo nei progetti a cui hanno accesso. I visualizzatori del progetto possono confermare e posticipare gli allarmi.

Alias di proprietà

È possibile creare alias sulle proprietà degli asset, ad esempio il percorso del flusso di dati del server OPC-UA (ad esempio, /company/windfarm/3/turbine/7/temperature), semplificando l'identificazione di una proprietà dell'asset durante l'acquisizione o il recupero dei dati degli asset. Quando utilizzate un gateway SiteWise Edge per importare dati dai server, gli alias delle proprietà devono corrispondere ai percorsi dei flussi di dati grezzi. Per ulteriori informazioni, consulta Mappatura dei flussi di dati industriali alle proprietà degli asset.

Notifica di proprietà

Quando abilitate le notifiche di proprietà per una proprietà di un asset, AWS IoT SiteWise pubblica un messaggio MQTT AWS IoT Core ogni volta che tale proprietà riceve un nuovo valore. Il payload del messaggio include dettagli sull'aggiornamento del valore di quella proprietà. Utilizzate le notifiche sul valore delle proprietà per creare soluzioni che collegano i dati industriali AWS IoT SiteWise ad altri AWS servizi. Per ulteriori informazioni, consulta Interazione con altri servizi AWS.

SiteWise Gateway Edge

Un gateway SiteWise Edge è situato presso la sede del cliente per raccogliere, gestire e indirizzare i dati. Un gateway SiteWise Edge si collega alle fonti di dati industriali tramite il protocollo OPC-UA per raccogliere ed elaborare i dati, inviandoli al AWS cloud. SiteWise I gateway Edge possono anche connettersi alle fonti di dati dei partner. SiteWise I gateway edge utilizzano pacchetti per la raccolta dei dati, l'elaborazione edge e altro ancora. Per ulteriori informazioni sui pacchetti disponibili, vederethe section called “Utilizzo dei pacchetti”.

Hai la flessibilità necessaria per creare un gateway SiteWise Edge su qualsiasi dispositivo o piattaforma in grado di funzionare AWS IoT Greengrass. Per ulteriori informazioni, consulta Utilizzo dei gateway SiteWise Edge.

Trasformazione

Le trasformazioni sono proprietà di una risorsa che rappresentano dati di serie temporali trasformati. Ogni trasformazione è accompagnata da un'espressione matematica (formula) che specifica come convertire i punti dati da un modulo all'altro. I punti dati trasformati mantengono una one-to-one relazione con i punti dati di input. Per ulteriori informazioni, consulta Trasformazione dei dati (trasformazioni).

Visualizzazione

In ogni dashboard, i proprietari del progetto decidono come visualizzare le proprietà e gli allarmi delle risorse associate al progetto. La disponibilità potrebbe essere rappresentata come un grafico a linee, mentre altri valori potrebbero essere visualizzati come grafici a barre o indicatori chiave di prestazione (KPI). Gli allarmi vengono visualizzati al meglio come griglie di stato e linee temporali di stato. I proprietari del progetto personalizzano ogni visualizzazione per fornire la migliore comprensione dei dati per l'asset.

Casi d'uso per AWS IoT SiteWise

AWS IoT SiteWise viene utilizzato in una varietà di settori per molte applicazioni di raccolta e analisi di dati industriali.

Raccogli dati in modo coerente da tutte le tue fonti per risolvere rapidamente i problemi. AWS IoT SiteWise offre il monitoraggio remoto per raccogliere i dati direttamente in loco o raccoglierli da più fonti in molte strutture. AWS IoT SiteWise fornisce la flessibilità necessaria per le soluzioni di dati IoT industriali.

Settore manifatturiero

AWS IoT SiteWise può semplificare il processo di raccolta e utilizzo dei dati dalle apparecchiature per individuare e ridurre al minimo le inefficienze, migliorando le operazioni industriali. AWS IoT SiteWise aiuta a raccogliere dati dalle linee e dalle apparecchiature di produzione. Con AWS IoT SiteWise, puoi trasferire i dati sul AWS cloud e creare metriche prestazionali per apparecchiature e processi specifici. Puoi utilizzare le metriche prodotte per comprendere l'efficacia complessiva delle tue operazioni e identificare opportunità di innovazione e miglioramento. È inoltre possibile visualizzare il processo di produzione e identificare carenze nelle apparecchiature e nei processi, lacune di produzione o difetti del prodotto.

Settore alimentare

Le strutture dell'industria alimentare gestiscono un'enorme quantità di processi di trasformazione del cibo, tra cui la macinatura del grano per la farina, la macellazione e il confezionamento della carne, così come l'assemblaggio, la cottura e la congelazione di cibi precotti. Gli impianti di trasformazione alimentare spesso si estendono su più sedi e gli operatori degli impianti e delle apparecchiature si trovano in una posizione centralizzata per monitorare processi e apparecchiature. Ad esempio, le unità di refrigerazione valutano la manipolazione e la scadenza degli ingredienti. Monitorano la produzione di rifiuti tra le strutture per garantire l'efficienza operativa. Con AWS IoT SiteWise, puoi raggruppare i flussi di dati dei sensori provenienti da più sedi per linea di produzione e strutture in modo che i tuoi ingegneri di processo possano comprendere meglio e apportare miglioramenti tra le strutture.

Energia e utenze

Con AWS IoT SiteWise, è possibile risolvere i problemi relativi alle apparecchiature in modo più semplice ed efficiente. È possibile monitorare le prestazioni degli asset da remoto e in tempo reale. Accedi ai dati storici delle apparecchiature da qualsiasi luogo per individuare potenziali problemi, inviare risorse accurate e prevenire e risolvere i problemi più rapidamente.

Guida introduttiva con AWS IoT SiteWise

Con AWS IoT SiteWise, puoi raccogliere, organizzare, analizzare e visualizzare i tuoi dati.

AWS IoT SiteWise fornisce una demo che puoi utilizzare per esplorare il servizio senza configurare una vera fonte di dati. Per ulteriori informazioni, consulta Utilizzo della AWS IoT SiteWise demo.

Puoi completare i seguenti tutorial per esplorare alcune funzionalità di: AWS IoT SiteWise

- Acquisizione di dati dagli oggetti AWS IoT
- Visualizzazione e condivisione dei dati dei parchi eolici in Monitor SiteWise
- Pubblicazione degli aggiornamenti dei valori delle proprietà su Amazon DynamoDB

Per ulteriori informazioni, consulta i seguenti argomenti: AWS IoT SiteWise

- Inserimento di dati in AWS IoT SiteWise
- Modellazione degli asset industriali
- Abilitare l'elaborazione dei dati edge
- Monitoraggio dei dati con AWS IoT SiteWise Monitor
- Interroga dati da AWS IoT SiteWise
- Interazione con altri servizi AWS

Argomenti

Requisiti

Devi averne uno con Account AWS cui iniziare AWS IoT SiteWise. Se non lo hai, consultare Configurare un Account AWS.

Usa una regione dove AWS IoT SiteWise è disponibile. Per ulteriori informazioni, consulta Endpoint e quote per AWS IoT SiteWise. È possibile utilizzare il selettore della regione in AWS Management Console per passare a una di queste regioni.

Configurare un Account AWS

Argomenti

Iscriviti per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

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

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

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente amministrativo e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Creazione di un utente amministratore

Dopo la registrazione Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .

2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Creazione di un utente amministratore

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .

2. In IAM Identity Center, assegna l'accesso amministrativo a un utente amministratore.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con l'impostazione predefinita IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accesso come utente amministratore

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Utilizzo della AWS IoT SiteWise demo

Puoi esplorare facilmente AWS IoT SiteWise utilizzando la AWS IoT SiteWise demo. AWS IoT SiteWise fornisce la demo come AWS CloudFormation modello che è possibile implementare per creare modelli di asset, risorse e un portale SiteWise Monitor e generare dati di esempio per un massimo di una settimana.

> **Important**
>
> Una volta creata la demo, inizierai a farti pagare per le risorse create e utilizzate da questa demo.

Argomenti

Creazione della demo AWS IoT SiteWise

È possibile creare la AWS IoT SiteWise demo dalla AWS IoT SiteWise console.

> **Note**
>
> La demo crea funzioni Lambda, una regola CloudWatch Events e i ruoli AWS Identity and Access Management (IAM) richiesti per la demo. Potresti vedere queste risorse nel tuo Account AWS. Ti consigliamo di conservare queste risorse finché non hai terminato la demo. Se elimini le risorse, la demo potrebbe smettere di funzionare correttamente.

Per creare la demo nella AWS IoT SiteWise console

1. Vai alla AWS IoT SiteWise console e trova la SiteWise demo nell'angolo in alto a destra della pagina.
2. (Facoltativo) In SiteWise demo, modifica il campo Giorni di conservazione delle risorse demo per specificare per quanti giorni conservare la demo prima di eliminarla.
3. (Facoltativo) Per creare un portale di SiteWise monitoraggio per monitorare i dati di esempio, procedi come segue.

   > **Note**
   >
   > Ti verranno addebitate le risorse di SiteWise Monitor create e utilizzate in questa demo. Per ulteriori informazioni, consulta SiteWise Monitor nella sezione AWS IoT SiteWise Prezzi.

a. Scegli Monitora le risorse.

b. Scegli Autorizzazione.

c. Scegli un ruolo IAM esistente che garantisca ai tuoi utenti IAM federati l'accesso al portale.

> **Important**
>
> Il tuo ruolo IAM deve avere le seguenti autorizzazioni.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iotsitewise:Describe*",
                "iotsitewise:List*",
                "iotsitewise:Get*",
                "cloudformation:DescribeStacks",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedRolePolicies",
                "sso:DescribeRegisteredRegions",
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

Per ulteriori informazioni su come lavorare con SiteWise Monitor, consulta Cos'è AWS IoT SiteWise Monitor? nella Guida all'AWS IoT SiteWise Monitor applicazione.

4. Seleziona Create demo (Crea demo).

La creazione della demo richiederà circa tre minuti. Nel caso in cui l'operazione non riuscisse, verifica le autorizzazioni, probabilmente insufficienti, del tuo account. Passa a un account con autorizzazioni amministrative oppure esegui la procedura seguente per eliminare la demo e riprovare:

a. Scegli Delete demo (Elimina demo).

   L'eliminazione della demo richiede circa 15 minuti.

b. Se la demo non viene eliminata, apri la AWS CloudFormation console, scegli lo stack denominato IoT SiteWiseDemoAssets e scegli Elimina nell'angolo in alto a destra.

c. Se la demo non riesce a eliminare nuovamente, segui i passaggi indicati nella AWS CloudFormation console per ignorare le risorse che non sono state eliminate e riprova.

5. Una volta creata correttamente la demo, puoi esplorare le risorse e i dati della demo nella AWS IoT SiteWise console.

Eliminazione della demo AWS IoT SiteWise

La AWS IoT SiteWise demo si elimina automaticamente dopo una settimana o dopo il numero di giorni che hai scelto se hai creato lo stack demo dalla console. AWS CloudFormation Puoi eliminare la demo prima se hai finito di usare le risorse della demo. Inoltre puoi eliminare la demo se la demo non viene creata. Attieniti alla seguente procedura per eliminare manualmente la demo.

Per eliminare la demo AWS IoT SiteWise

1. Passare alla console AWS CloudFormation.
2. Scegliere IoTSiteWiseDemoAssets dall'elenco di stack.
3. Scegli Elimina.

   Quando si elimina lo stack, tutte le risorse create per la demo vengono eliminate.

4. Nella finestra di dialogo di conferma scegliere Delete stack (Elimina stack).

   L'eliminazione dello stack richiede circa 15 minuti. Se la demo non riuscisse a finalizzare l'eliminazione, seleziona nuovamente Delete (Elimina) nell'angolo in alto a destra. Se la demo non viene nuovamente eliminata, segui i passaggi indicati nella AWS CloudFormation console per ignorare le risorse che non sono state eliminate e riprova.

AWS IoT SiteWise tutorial

Benvenuto nella pagina AWS IoT SiteWise dei tutorial. Questa crescente raccolta di tutorial ti fornisce le conoscenze e le competenze necessarie per navigare nelle complessità di. AWS IoT SiteWise Questi tutorial offrono una vasta gamma di argomenti di base per soddisfare le tue esigenze. Man mano che approfondisci i tutorial, scopri informazioni preziose su vari aspetti di. AWS IoT SiteWise

Ogni tutorial utilizza un esempio di attrezzatura specifico. Questi tutorial sono destinati agli ambienti di test e utilizzano nomi di società, modelli, risorse, proprietà fittizi e così via. Il loro scopo è di fornire linee guida di carattere generico. I tutorial non sono destinati all'uso diretto in un ambiente di produzione senza un'attenta revisione e adattamento per soddisfare le esigenze specifiche dell'organizzazione.

Argomenti

Calcolo dell'OEE in AWS IoT SiteWise

Questo tutorial fornisce un esempio specifico di come calcolare l'OEE (Overall Equipment Effectiveness, efficienza complessiva delle apparecchiature) di un processo di produzione. Trattandosi di un esempio, i tuoi calcoli o le formule reali dell'OEE potrebbero variare rispetto a quelli mostrati. In generale, l'OEE è definito da `Availability * Quality * Performance`. Per ulteriori informazioni sul calcolo dell'OEE, consulta Overall equipment effectiveness su Wikipedia.

Prerequisiti

Per completare questo tutorial, è necessario configurare l'acquisizione di dati per un dispositivo con i seguenti tre flussi di dati:

- `Equipment_State`— Un codice numerico che rappresenta lo stato della macchina, ad esempio inattività, guasto, arresto pianificato o funzionamento normale.
- `Good_Count`— Un flusso di dati in cui ogni punto dati contiene il numero di operazioni riuscite a partire dall'ultimo punto dati.

- `Bad_Count`— Un flusso di dati in cui ogni punto dati contiene il numero di operazioni non riuscite dall'ultimo punto dati.

Per configurare l'acquisizione di dati, consulta Inserimento di dati in AWS IoT SiteWise. In assenza di un'operazione industriale disponibile, è possibile creare uno script che generi e carichi dati esemplificativi tramite l'API di AWS IoT SiteWise .

Come calcolare l'OEE

In questo tutorial, si crea un modello di asset che calcola l'OEE in base a tre flussi di dati di input: `Equipment_State`, `Good_Count` e `Bad_Count`. In questo esempio, prendiamo in esame una macchina generica per il packaging, come quelle utilizzate per il confezionamento dello zucchero, delle patatine o della vernice. Nella AWS IoT SiteWise console, crea un modello di AWS IoT SiteWise asset con le seguenti misurazioni, trasformazioni e metriche. Quindi, potete creare una risorsa per rappresentare la macchina per l'imballaggio e osservare come AWS IoT SiteWise calcola l'OEE.

Definisci le seguenti misurazioni per rappresentare i flussi di dati non elaborati provenienti dalla macchina confezionatrice.

Misurazioni

- `Equipment_State`— Un flusso di dati (o misurazione) che fornisce lo stato attuale della macchina confezionatrice in codici numerici:
  - `1024`— La macchina è inattiva.
  - `1020`— Un guasto, ad esempio un errore o un ritardo.
  - `1000`— Una sosta pianificata.
  - `1111`— Un'operazione normale.
- `Good_Count`— Un flusso di dati in cui ogni punto dati contiene il numero di operazioni riuscite a partire dall'ultimo punto dati.
- `Bad_Count`— Un flusso di dati in cui ogni punto dati contiene il numero di operazioni non riuscite dall'ultimo punto dati.

Utilizzando il flusso di dati di misurazione `Equipment_State` e i relativi codici, è possibile definire le seguenti trasformazioni (o misurazioni derivate). Le trasformazioni hanno una one-to-one relazione con le misurazioni grezze.

Trasformazioni

- `Idle = eq(Equipment_State, 1024)`— Un flusso di dati trasformato che contiene lo stato di inattività della macchina.
- `Fault = eq(Equipment_State, 1020)`— Un flusso di dati trasformato che contiene lo stato di guasto della macchina.
- `Stop = eq(Equipment_State, 1000)`— Un flusso di dati trasformato che contiene lo stato di arresto pianificato della macchina.
- `Running = eq(Equipment_State, 1111)`— Un flusso di dati trasformato che contiene il normale stato operativo della macchina.

Utilizzando le misurazioni non elaborate e quelle trasformate, è possibile definire i seguenti parametri che aggregano i dati della macchina per intervalli di tempo specificati. Per tutti i parametri che si vanno a definire in questa sezione bisogna scegliere lo stesso intervallo di tempo.

Metriche

- `Successes = sum(Good_Count)`— Il numero di pacchi riempiti con successo nell'intervallo di tempo specificato.
- `Failures = sum(Bad_Count)`— Il numero di pacchi riempiti senza successo nell'intervallo di tempo specificato.
- `Idle_Time = statetime(Idle)`— Il tempo di inattività totale della macchina (in secondi) per intervallo di tempo specificato.
- `Fault_Time = statetime(Fault)`— Il tempo totale di guasto della macchina (in secondi) per intervallo di tempo specificato.
- `Stop_Time = statetime(Stop)`— Il tempo di arresto totale pianificato della macchina (in secondi) per intervallo di tempo specificato.
- `Run_Time = statetime(Running)`— Il tempo totale di funzionamento della macchina (in secondi) senza problemi per un intervallo di tempo specificato.
- `Down_Time = Idle_Time + Fault_Time + Stop_Time`— Il tempo di inattività totale della macchina (in secondi) nell'intervallo di tempo specificato, calcolato come somma degli stati della macchina diversi da. `Run_Time`
- `Availability = Run_Time / (Run_Time + Down_Time)`— Il tempo di attività della macchina o la percentuale di tempo programmato in cui la macchina è disponibile a funzionare nell'intervallo di tempo specificato.

- `Quality = Successes / (Successes + Failures)`— La percentuale della macchina di imballaggi riempiti con successo negli intervalli di tempo specificati.
- `Performance = ((Successes + Failures) / Run_Time) / Ideal_Run_Rate`— Le prestazioni della macchina nell'intervallo di tempo specificato, espresse in percentuale rispetto alla velocità di esecuzione ideale (in secondi) per il processo.

  Ad esempio, l'`Ideal_Run_Rate` potrebbero essere 60 pacchetti al minuto (1 pacchetto al secondo). Se il `Ideal_Run_Rate` valore è espresso al minuto o all'ora, è necessario dividerlo per il fattore di conversione unitario appropriato, espresso `Run_Time` in secondi.
- `OEE = Availability * Quality * Performance`— L'efficacia complessiva dell'attrezzatura della macchina nell'intervallo di tempo specificato. Questa formula calcola l'OEE come una frazione su 1.

Acquisizione di dati dagli oggetti AWS IoT

Scopri come importare dati AWS IoT SiteWise da una serie di dispositivi utilizzando AWS IoT le ombre dei dispositivi in questo tutorial. Le ombre dei dispositivi sono oggetti JSON che memorizzano le informazioni sullo stato corrente di un dispositivo. AWS IoT Per ulteriori informazioni, consulta Device shadow service nella Device ShadowAWS IoT Guide.

Dopo aver completato questo tutorial, puoi impostare un'operazione in AWS IoT SiteWise base agli AWS IoT elementi. Utilizzando AWS IoT le cose, è possibile integrare l'operazione con altre utili funzionalità di AWS IoT. Ad esempio, è possibile configurare AWS IoT le funzionalità per eseguire le seguenti attività:

- Configura regole aggiuntive per lo streaming di dati verso AWS IoT EventsAmazon DynamoDB e altro. Servizi AWS Per ulteriori informazioni, consulta Rules nella AWS IoT Developer Guide.
- Indicizza, cerca e aggrega i dati del tuo dispositivo con il servizio di indicizzazione del AWS IoT parco veicoli. Per ulteriori informazioni, consulta il servizio di indicizzazione del parco veicoli nella Guida per gli sviluppatori.AWS IoT
- Controlla e proteggi i tuoi dispositivi con. AWS IoT Device Defender Per ulteriori informazioni, consulta la sezione AWS IoT Device Defender nella Guida per gli sviluppatori di AWS IoT .

In questo tutorial, imparerai a trasferire i dati dalle ombre dei dispositivi AWS IoT Things agli asset in esso contenuti. AWS IoT SiteWise A tale scopo, create uno o più AWS IoT elementi ed eseguite uno script che aggiorna l'ombra del dispositivo di ogni elemento con i dati sull'utilizzo della CPU

e della memoria. In questo tutorial usi i dati di utilizzo della CPU e della memoria per imitare i dati realistici del sensore. Quindi, crei una regola con un' AWS IoT SiteWise azione che invia questi dati a una risorsa AWS IoT SiteWise ogni volta che lo shadow del dispositivo si aggiorna. Per ulteriori informazioni, consulta Acquisizione di dati tramite regole AWS IoT Core.

Argomenti

Prerequisiti

Per completare questo tutorial, è necessario quanto segue:

- Un Account AWS. Se non lo hai, consultare Configurare un Account AWS.
- Un computer di sviluppo che esegue WindowsmacOS,Linux, o Unix per accedere a AWS Management Console. Per ulteriori informazioni, consulta Nozioni di base su AWS Management Console.
- Un utente AWS Identity and Access Management (IAM) con autorizzazioni di amministratore.
- Python3 installato sul tuo computer di sviluppo o installato sul dispositivo che desideri registrare come dispositivo AWS IoT .

Fase 1: Creazione di una AWS IoT politica

In questa procedura, crea una AWS IoT politica che consenta ai tuoi AWS IoT oggetti di accedere alle risorse utilizzate in questo tutorial.

Per creare una AWS IoT politica

1. Accedi alla AWS Management Console.
2. Consulta le AWS regioni in cui AWS IoT SiteWise è supportato. Passare a una di queste regioni supportate, se necessario.
3. Passare alla console AWS IoT. Se viene visualizzato il pulsante Connect device, selezionalo.
4. Nel riquadro di navigazione a sinistra, scegli Sicurezza, quindi scegli Politiche.
5. Scegli Crea.
6. Inserisci un nome per la AWS IoT politica (ad esempio,**`SiteWiseTutorialDevicePolicy`**).
7. In Documento di politica, scegli JSON per inserire la seguente politica in formato JSON. Sostituire*`region`* e *`account-id`* con la regione e l'ID account, ad esempio **`us-east-1`** e **`123456789012`**.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iot:Connect",
      "Resource": "arn:aws:iot:region:account-id:client/SiteWiseTutorialDevice*"
    },
    {
      "Effect": "Allow",
      "Action": "iot:Publish",
      "Resource": [
        "arn:aws:iot:region:account-id:topic/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/update",
        "arn:aws:iot:region:account-id:topic/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/delete",
        "arn:aws:iot:region:account-id:topic/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/get"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "iot:Receive",
      "Resource": [
        "arn:aws:iot:region:account-id:topic/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/update/accepted",
```

```
        "arn:aws:iot:region:account-id:topic/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/delete/accepted",
        "arn:aws:iot:region:account-id:topic/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/get/accepted",
        "arn:aws:iot:region:account-id:topic/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/update/rejected",
        "arn:aws:iot:region:account-id:topic/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/delete/rejected"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "iot:Subscribe",
      "Resource": [
        "arn:aws:iot:region:account-id:topicfilter/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/update/accepted",
        "arn:aws:iot:region:account-id:topicfilter/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/delete/accepted",
        "arn:aws:iot:region:account-id:topicfilter/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/get/accepted",
        "arn:aws:iot:region:account-id:topicfilter/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/update/rejected",
        "arn:aws:iot:region:account-id:topicfilter/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/delete/rejected"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:GetThingShadow",
        "iot:UpdateThingShadow",
        "iot:DeleteThingShadow"
      ],
      "Resource": "arn:aws:iot:region:account-id:thing/SiteWiseTutorialDevice*"
    }
  ]
}
```

Questa politica consente ai AWS IoT dispositivi di stabilire connessioni e comunicare con le ombre dei dispositivi utilizzando messaggi MQTT. Per ulteriori informazioni sui messaggi MQTT, consulta Che cos'è MQTT? . Per interagire con AWS IoT le ombre dei dispositivi, i tuoi dispositivi pubblicano e ricevono messaggi MQTT su argomenti che iniziano con. `$aws/things/thing-`

name/shadow/ Questa politica incorpora una variabile di policy relativa agli oggetti nota come. ${iot:Connection.Thing.ThingName} Questa variabile sostituisce il nome dell'oggetto connesso in ogni argomento. L'iot:Connectistruzione stabilisce delle limitazioni sui dispositivi che possono stabilire connessioni, assicurando che la variabile thing policy possa sostituire solo i nomi che iniziano con. SiteWiseTutorialDevice

Per ulteriori informazioni, vedere Thing policy variables nella AWS IoT Developer Guide.

> **Note**
>
> Questa policy si applica agli oggetti i cui nomi iniziano con SiteWiseTutorialDevice. Per utilizzare un nome diverso per gli oggetti, è necessario aggiornare la policy di conseguenza.

8. Scegli Create (Crea).

Fase 2: Creare e configurare qualsiasi cosa AWS IoT

In questa procedura, si crea e si configura qualsiasi AWS IoT cosa. È possibile designare il computer di sviluppo come qualsiasi AWS IoT cosa. Man mano che progredisci, ricorda che i principi che stai imparando qui possono essere applicati a progetti reali. Hai la flessibilità di creare e configurare AWS IoT cose su qualsiasi dispositivo in grado di eseguire un AWS IoT SDK, inclusi AWS IoT Greengrass FreerTOS. Per ulteriori informazioni, consulta gli AWS IoT SDK nella Guida per gli sviluppatori.AWS IoT

Per creare e configurare qualsiasi cosa AWS IoT

1. Aprire una riga di comando ed eseguire il comando seguente per creare una directory per questo tutorial.

```
mkdir iot-sitewise-rule-tutorial
cd iot-sitewise-rule-tutorial
```

2. Eseguire il seguente comando per creare una directory per i certificati dell'oggetto.

```
mkdir device1
```

Se si stanno creando altri oggetti, incrementa il numero nel nome della directory di conseguenza per tenere traccia di quali certificati appartengono a quale oggetto.

3. Passare alla console AWS IoT.
4. Nel riquadro di navigazione a sinistra, scegli Tutti i dispositivi nella sezione Gestisci. Quindi, scegliere Things (Oggetti).
5. Se viene visualizzata la finestra di dialogoYou don't have any things yet (Non hai ancora oggetti), selezionare Create a thing (Crea un oggetto). Altrimenti, scegli Crea cose.
6. Nella pagina Creazione di elementi, scegli Crea un singolo elemento, quindi scegli Avanti.
7. Nella pagina Specificare le proprietà dell'oggetto, inserisci un nome per l' AWS IoT oggetto (ad esempio**`SiteWiseTutorialDevice1`**), quindi scegli Avanti. Se si stanno creando altri oggetti, incrementare il numero nel nome dell'oggetto di conseguenza.

   > **Important**
   >
   > Il nome dell'oggetto deve corrispondere al nome utilizzato nella politica creata nel Passaggio 1: Creazione di una AWS IoT politica. In caso contrario, il dispositivo non potrà connettersi a AWS IoT.

8. Nella pagina Configura il certificato del dispositivo - opzionale, scegli Genera automaticamente un nuovo certificato (consigliato), quindi scegli Avanti. I certificati consentono AWS IoT di identificare in modo sicuro i dispositivi.
9. Nella pagina Allega politiche al certificato - opzionale, seleziona la politica creata nel Passaggio 1: Creazione di una AWS IoT politica e scegli Crea oggetto.
10. Nella finestra di dialogo Scarica certificati e chiavi, procedi come segue:

    a. Scegliere i collegamenti Download per scaricare il certificato, la chiave pubblica e la chiave privata dell'oggetto. Salvare tutti e tre i file nella directory creata per i certificati dell'oggetto (ad esempio, `iot-sitewise-rule-tutorial/device1`).

       > **Important**
       >
       > Questo è l'unico momento in cui è possibile scaricare il certificato e le chiavi dell'oggetto, necessari per connettere correttamente il dispositivo ad AWS IoT.

    b. Scegliete il link Download per scaricare un certificato CA root. Salvare il certificato CA radice in `iot-sitewise-rule-tutorial`. Consigliamo di scaricare Amazon Root CA 1.

11. Seleziona Fatto.

Ora hai registrato qualsiasi AWS IoT cosa sul tuo computer. Esegui uno dei seguenti passaggi successivi:

- Continua con la Fase 3: Creazione di un modello di asset del dispositivo senza creare AWS IoT elementi aggiuntivi. È possibile completare questo tutorial con un solo oggetto.
- Ripetere la procedura descritta in questa sezione su un altro computer o dispositivo per creare altri oggetti AWS IoT . Per questo tutorial, si consiglia di seguire questa opzione in modo da poter inserire dati di utilizzo univoci della CPU e della memoria da più dispositivi.
- Ripetere la procedura descritta in questa sezione sullo stesso dispositivo (computer) per creare più oggetti AWS IoT . Ogni AWS IoT oggetto riceve dati simili sull'utilizzo della CPU e della memoria dal computer, quindi utilizza questo approccio per dimostrare l'acquisizione di dati non univoci da più dispositivi.

Fase 3: Creazione di un modello di asset del dispositivo

In questa procedura, create un modello di asset AWS IoT SiteWise per rappresentare i dispositivi che trasmettono i dati sull'utilizzo della CPU e della memoria. Per elaborare i dati in asset che rappresentano gruppi di dispositivi, i modelli di asset applicano informazioni coerenti su più asset dello stesso tipo. Per ulteriori informazioni, consulta Modellazione degli asset industriali.

Per creare un modello di asset che rappresenta un dispositivo

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione a sinistra scegliere Models (Modelli).
3. Scegli Crea modello.
4. In Dettagli del modello, inserisci un nome per il tuo modello. Ad esempio, **`SiteWise Tutorial Device Model`**.
5. In Measurement definitions (Definizioni misurazione), effettuare le seguenti operazioni:
    a. In Nome, inserisci **`CPU Usage`**.
    b. In Unit (Unità), immettere `%`.
    c. Lasciare Data type (Tipo di dati) come Double (Doppio).

Le proprietà di misurazione rappresentano i flussi di dati non elaborati di un dispositivo. Per ulteriori informazioni, consulta Definizione dei flussi di dati provenienti dalle apparecchiature (misurazioni).

6. Scegli Aggiungi nuova misurazione per aggiungere una seconda proprietà di misurazione.
7. Nella seconda riga sotto Measurement definitions (Definizioni misurazione), effettuare le seguenti operazioni:

   a. In Nome, inserisci **`Memory Usage`**.

   b. In Unit (Unità), immettere **`%`**.

   c. Lasciare Data type (Tipo di dati) come Double (Doppio).
8. In Metric definitions (Definizioni parametri), effettuare le seguenti operazioni:

   a. In Nome, inserisci **`Average CPU Usage`**.

   b. In Formula (Formula), immettere **`avg(CPU Usage)`** . Scegliere CPU Usage dall'elenco di completamento automatico quando viene visualizzato.

   c. In Time interval (Intervallo di tempo), immettere **`5 minutes`**.

   Le proprietà dei parametri definiscono i calcoli di aggregazione che elaborano tutti i punti dati di input per un intervallo e generano un singolo punto dati per ogni intervallo. Questa proprietà dei parametri calcola l'utilizzo medio della CPU di ogni dispositivo ogni 5 minuti. Per ulteriori informazioni, consulta Aggregazione di dati da proprietà e altre risorse (metriche).
9. Scegli Aggiungi nuova metrica per aggiungere una seconda proprietà metrica.
10. Nella seconda riga sotto Metric definitions (Definizioni parametri), effettuare le seguenti operazioni:

    a. In Nome, inserisci **`Average Memory Usage`**.

    b. In Formula (Formula), immettere **`avg(Memory Usage)`** . Scegliere Memory Usage dall'elenco di completamento automatico quando viene visualizzato.

    c. In Time interval (Intervallo di tempo), immettere **`5 minutes`**.

    Questa proprietà dei parametri calcola l'utilizzo medio della memoria di ogni dispositivo ogni 5 minuti.

11. (Facoltativo) Aggiungere altri parametri che devono essere calcolati per ogni dispositivo. Alcune funzioni interessanti sono `min` e `max`. Per ulteriori informazioni, consulta Utilizzo delle espressioni di formula. Nella Fase 4: Creazione di un modello di asset per il parco dispositivi, crei una risorsa principale in grado di calcolare le metriche utilizzando i dati dell'intero parco dispositivi.
12. Scegli Crea modello.

Fase 4: Creazione di un modello di asset per la flotta di dispositivi

In questa procedura, create un modello di asset AWS IoT SiteWise per simboleggiare la vostra collezione di dispositivi. All'interno di questo modello di asset, stabilisci una struttura che ti consente di collegare numerosi dispositivi a un unico asset globale della flotta. Successivamente, definisci le metriche nel modello di asset della flotta per consolidare i dati di tutti gli asset dei dispositivi connessi. Questo approccio fornisce informazioni complete sulle prestazioni collettive dell'intero parco veicoli.

Per creare un modello di asset che rappresenta un parco istanze dei dispositivi

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione a sinistra scegliere Models (Modelli).
3. Scegli Crea modello.
4. In Dettagli del modello, inserisci un nome per il tuo modello. Ad esempio, **`SiteWise Tutorial Device Fleet Model`**.
5. In Hierarchy definitions (Definizioni gerarchie), effettuare le seguenti operazioni:

    a. In Hierarchy name (Nome gerarchia), immettere **`Device`**.

    b. Nel Hierarchy model (Modello gerarchia), scegliere il modello di asset dispositivo (**`SiteWise Tutorial Device Model`**).

    Una gerarchia definisce una relazione tra un modello di asset padre (parco istanze) e un modello di asset figlio (dispositivo). Gli asset padre possono accedere ai dati delle proprietà degli asset figlio. Quando si creano gli asset in un secondo momento, è necessario associare gli asset figlio agli asset padre in base a una definizione di gerarchia nel modello di asset padre. Per ulteriori informazioni, consulta Definizione delle gerarchie dei modelli di asset.
6. In Metric definitions (Definizioni parametri), effettuare le seguenti operazioni:

    a. In Nome, inserisci **`Average CPU Usage`**.

b. In Formula (Formula), immettere **`avg(Device | Average CPU Usage)`** . Quando viene visualizzato l'elenco di completamento automatico, selezionare Device per scegliere una gerarchia, quindi selezionare Average CPU Usage per scegliere il parametro dall'asset dispositivo creato in precedenza.

c. In Time interval (Intervallo di tempo), immettere **`5 minutes`**.

Questa proprietà del parametro calcola l'utilizzo medio della CPU di tutti gli asset dispositivo associati a un asset parco istanze tramite la gerarchia **`Device`**.

7. Scegli Aggiungi nuova metrica per aggiungere una seconda proprietà metrica.
8. Nella seconda riga sotto Metric definitions (Definizioni parametri), effettuare le seguenti operazioni:

   a. In Nome, inserisci **`Average Memory Usage`**.

   b. In Formula (Formula), immettere **`avg(Device | Average Memory Usage)`** . Quando viene visualizzato l'elenco di completamento automatico, selezionare Device per scegliere una gerarchia, quindi selezionare Average Memory Usage per scegliere il parametro dall'asset dispositivo creato in precedenza.

   c. In Time interval (Intervallo di tempo), immettere **`5 minutes`**.

   Questa proprietà del parametro calcola l'utilizzo medio della memoria di tutti gli asset dispositivo associati a un asset parco istanze tramite la gerarchia **`Device`**.

9. (Facoltativo) Aggiungere altri parametri che devono essere calcolati per il parco istanze dei dispositivi.
10. Scegli Crea modello.

Fase 5: Creazione e configurazione di una risorsa del dispositivo

In questa procedura, si genera una risorsa del dispositivo basata sul modello di risorsa del dispositivo. Quindi, definisci gli alias per ogni proprietà di misurazione. Un alias di proprietà è una stringa univoca che identifica la proprietà di una risorsa. Successivamente, potete identificare una proprietà per il caricamento dei dati utilizzando gli alias anziché l'ID della risorsa e l'ID della proprietà. Per ulteriori informazioni, consulta Mappatura dei flussi di dati industriali alle proprietà degli asset.

Per creare un asset dispositivo e definire gli alias di proprietà

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione a sinistra, scegli Asset.
3. Selezionare Create asset (Crea asset).
4. In Informazioni sul modello, scegliete il modello di asset del dispositivo,**`SiteWise Tutorial Device Model`**.
5. In Informazioni sulla risorsa, inserite un nome per la risorsa. Ad esempio, **`SiteWise Tutorial Device 1`**.
6. Selezionare Create asset (Crea asset).
7. Per il nuovo asset dispositivo, scegliere Edit (Modifica).
8. In CPU Usage, immettere **`/tutorial/device/SiteWiseTutorialDevice1/cpu`** come alias di proprietà. Includi il nome dell' AWS IoT oggetto nell'alias della proprietà, in modo da poter importare i dati da tutti i tuoi dispositivi utilizzando un'unica AWS IoT regola.
9. In Memory Usage, immettere **`/tutorial/device/SiteWiseTutorialDevice1/memory`** come alias di proprietà.
10. Selezionare Salva.

Se hai creato più AWS IoT elementi in precedenza, ripeti i passaggi da 3 a 10 per ogni dispositivo e incrementa di conseguenza il numero nel nome della risorsa e negli alias delle proprietà. Ad esempio, il nome del secondo asset dispositivo dovrebbe essere **`SiteWise Tutorial Device 2`** e i relativi alias di proprietà dovrebbero essere **`/tutorial/device/SiteWiseTutorialDevice2/cpu`** e **`/tutorial/device/SiteWiseTutorialDevice2/memory`**.

Fase 6: Creazione e configurazione di un parco dispositivi

In questa procedura, crei un asset di parco dispositivi derivato dal tuo modello di parco dispositivi. Quindi, colleghi le risorse dei singoli dispositivi alla risorsa del parco dispositivi. Questa associazione consente alle proprietà metriche dell'asset della flotta di compilare e analizzare i dati provenienti da più dispositivi. Questi dati forniscono una visione consolidata delle prestazioni collettive dell'intera flotta.

Per creare un asset parco istanze dei dispositivi e associare asset dispositivo

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione a sinistra, scegli Asset.

3. Selezionare Create asset (Crea asset).
4. In Informazioni sul modello, scegli il modello di asset della flotta di dispositivi,**`SiteWise Tutorial Device Fleet Model`**.
5. In Informazioni sull'asset, inserisci un nome per il tuo asset. Ad esempio, **`SiteWise Tutorial Device Fleet 1`**.
6. Selezionare Create asset (Crea asset).
7. Per il nuovo asset parco istanze dei dispositivi, scegliere Edit (Modifica).
8. In Risorse associate a questa risorsa, scegliete Aggiungi risorsa associata ed effettuate le seguenti operazioni:

   a. In Hierarchy (Gerarchia), scegliere Device. Questa gerarchia identifica la relazione di gerarchia tra gli asset parco istanze dei dispositivi e gli asset dispositivi. Questa gerarchia è stata definita nel modello di asset parco istanze dei dispositivi in precedenza in questo tutorial.

   b. In Asset, scegliere l'asset dispositivo SiteWise Tutorial Device 1.
9. (Facoltativo) Se in precedenza avete creato più risorse per dispositivo, ripetete i passaggi da 8 a 10 per ogni risorsa del dispositivo che avete creato.
10. Selezionare Salva.

    A questo punto gli asset dispositivo vengono visualizzati organizzati in gerarchia.

Passaggio 7: creazione di una regola in AWS IoT Core per inviare dati alle risorse del dispositivo

In questa procedura, si stabilisce una regola in AWS IoT Core. La regola è progettata per interpretare i messaggi di notifica provenienti dalle ombre del dispositivo e trasmettere i dati alle risorse del dispositivo in AWS IoT SiteWise.Ogni volta che il dispositivo si aggiorna lo shadow, AWS IoT invia un messaggio MQTT. Puoi creare una regola che intraprende un'azione quando le shadow del dispositivo cambiano in base al messaggio MQTT. In questo caso, l'obiettivo è gestire il messaggio di aggiornamento, estrarre i valori delle proprietà e trasmetterli alle risorse del dispositivo. AWS IoT SiteWise

Creare una regola con un' AWS IoT SiteWise azione

1. Passare alla console AWS IoT.

2. Nel riquadro di navigazione a sinistra, scegli Routing dei messaggi, quindi scegli Regole.
3. Scegli Crea regola.
4. Inserisci un nome e una descrizione per la regola, quindi scegli Avanti.
5. Immettete la seguente istruzione SQL e scegliete Avanti.

```
SELECT
  *
FROM
  '$aws/things/+/shadow/update/accepted'
WHERE
  startsWith(topic(3), "SiteWiseTutorialDevice")
```

Questa istruzione di query di regola funziona perché il servizio shadow del dispositivo pubblica gli aggiornamenti shadow in `$aws/things/thingName/shadow/update/accepted`. Per ulteriori informazioni sulle ombre dei dispositivi, consulta Device shadow service nella AWS IoT Device Shadow Guide.

Nella clausola `WHERE`, questa istruzione di query di regola utilizza la funzione `topic(3)` per ottenere il nome dell'oggetto dal terzo segmento dell'argomento. Quindi, l'istruzione esclude i dispositivi con nomi che non corrispondono a quelli dei dispositivi del tutorial. Per ulteriori informazioni su AWS IoT SQL, consulta il riferimento AWS IoT SQL nella AWS IoT Developer Guide.

6. In Azioni relative alle regole, scegliete Invia i dati dei messaggi alle proprietà degli asset in AWS IoT SiteWise ed effettuate le seguenti operazioni:

   a. Scegliere By property alias (Per alias di proprietà).
   b. In Property alias (Alias proprietà), immettere **`/tutorial/device/${topic(3)}/cpu`**.

      La `${...}` sintassi è un modello sostitutivo. AWS IoT valuta il contenuto all'interno delle parentesi. Questo modello di sostituzione esegue il pull del nome dell'oggetto dall'argomento per creare un alias univoco per ogni oggetto. Per ulteriori informazioni, consulta Modelli sostitutivi nella Guida per gli sviluppatori.AWS IoT

      > **Note**
      >
      > Poiché un'espressione in un modello di sostituzione viene valutata separatamente dall'istruzione `SELECT`, non puoi utilizzare un modello di sostituzione per fare riferimento a un alias creato utilizzando una clausola `AS`. È possibile fare riferimento

solo alle informazioni presenti nel payload originale, oltre alle funzioni e agli operatori supportati.

c. In Entry ID, facoltativo, inserisci. **`${concat(topic(3), "-cpu-", floor(state.reported.timestamp))}`**

   Gli ID voce identificano in modo univoco ogni tentativo di immissione del valore. Se una voce restituisce un errore, è possibile trovare l'ID voce nell'output dell'errore per risolvere il problema. Il modello di sostituzione in questo ID voce combina il nome dell'oggetto e il timestamp restituito del dispositivo. Ad esempio, l'ID voce risultante potrebbe essere simile a `SiteWiseTutorialDevice1-cpu-1579808494`.

d. In Time in seconds (Ora in secondi), immettere **`${floor(state.reported.timestamp)}`**.

   Questo modello di sostituzione calcola l'ora in secondi dal timestamp restituito del dispositivo. In questo tutorial, i dispositivi restituiscono il timestamp in secondi nel formato di ora epoch Unix come numero a virgola mobile.

e. In Offset in nanos - opzionale, inserisci. **`${floor((state.reported.timestamp % 1) * 1E9)}`**

   Questo modello di sostituzione calcola l'offset in nanosecondi dall'ora in secondi convertendo la parte decimale del timestamp restituito del dispositivo.

   > **Note**
   >
   > AWS IoT SiteWise richiede che i dati abbiano un timestamp corrente in Unix Epoch Time. Se i dispositivi non restituiscono l'ora in modo accurato, è possibile che l'ora corrente restituita dal motore di regole AWS IoT sia timestamp(). Questa funzione segnala l'ora in millisecondi, quindi è necessario aggiornare i parametri dell'ora dell'azione di regola ai seguenti valori:
   >
   > - In Time in seconds (Ora in secondi), immettere **`${floor(timestamp() / 1E3)}`**.
   > - In Offset in nanos (Offset in nanosecondi), immettere **`${(timestamp() % 1E3) * 1E6}`**.

f. In Data type (Tipo di dati), scegliere Double (Doppio).

Questo tipo di dati deve corrispondere al tipo di dati della proprietà dell'asset definita nel modello di asset.

g. In Valore, immetti **`${state.reported.cpu}`**. Nei modelli di sostituzione, è possibile utilizzare l'operatore **`.`** per recuperare un valore all'interno di una struttura JSON.

h. Scegliere Add entry (Aggiungi voce) per aggiungere una nuova voce per la proprietà di utilizzo della memoria e completare nuovamente i passaggi seguenti per questa proprietà:

   i. Scegliere By property alias (Per alias di proprietà).

   ii. In Property alias (Alias proprietà), immettere **`/tutorial/device/${topic(3)}/memory`**.

   iii. In Entry ID - facoltativo, inserisci. **`${concat(topic(3), "-memory-", floor(state.reported.timestamp))}`**

   iv. In Time in seconds (Ora in secondi), immettere **`${floor(state.reported.timestamp)}`**.

   v. In Offset in nanos - opzionale, inserisci. **`${floor((state.reported.timestamp % 1) * 1E9)}`**

   vi. In Data type (Tipo di dati), scegliere Double (Doppio).

   vii. In Valore, immetti **`${state.reported.memory}`**.

i. In Ruolo IAM, scegli Crea nuovo ruolo per creare un ruolo IAM per questa azione della regola. Questo ruolo consente di AWS IoT inviare dati alle proprietà della flotta di dispositivi e della relativa gerarchia degli asset.

j. Inserisci il nome del ruolo e scegli Crea.

7. (Facoltativo) Configurare un'azione di errore che è possibile utilizzare per risolvere i problemi della regola. Per ulteriori informazioni, consulta la pagina Risoluzione dei problemi relativi a una regola.

8. Seleziona Next (Successivo).

9. Controlla le impostazioni e scegli Crea per creare la regola.

Fase 8: Esecuzione dello script client del dispositivo

In questo tutorial, non stai utilizzando un dispositivo reale per riportare i dati. Invece, esegui uno script per aggiornare l'ombra del dispositivo in uso con l'utilizzo della CPU e della memoria per imitare i dati reali dei sensori. AWS IoT Per eseguire lo script, è necessario prima installare Python i pacchetti

richiesti. In questa procedura, si Python installano i pacchetti richiesti e quindi si esegue lo script client del dispositivo.

Per configurare ed eseguire lo script client del dispositivo

1. Passare alla console AWS IoT.
2. Nella parte inferiore del riquadro di spostamento a sinistra scegliere Settings (Impostazioni).
3. Salvare l'endpoint personalizzato da utilizzare con lo script client del dispositivo. Usare questo endpoint per interagire con le shadow dell'oggetto. Questo endpoint è univoco per l'account nella regione corrente.

   L'endpoint personalizzato è simile all'esempio seguente.

   ```
   identifier.iot.region.amazonaws.com
   ```

4. Aprire una riga di comando ed eseguire il comando seguente per passare alla directory creata in precedenza nel tutorial.

   ```
   cd iot-sitewise-rule-tutorial
   ```

5. Eseguire il comando seguente per installare SDK per dispositivi AWS IoT per Python.

   ```
   pip3 install AWSIoTPythonSDK
   ```

   Per ulteriori informazioni, consulta SDK per dispositivi AWS IoT per Pythonla Guida per AWS IoT gli sviluppatori
6. Eseguire il seguente comando per installare psutil, un processo multipiattaforma e una libreria di utilità di sistema.

   ```
   pip3 install psutil
   ```

   Per ulteriori informazioni, consultare psutil nell'indice dei pacchetti Python.
7. Creare un file chiamato `thing_performance.py` nella directory `iot-sitewise-rule-tutorial` e quindi copiare il seguente codice Python nel file.

   ```
   import AWSIoTPythonSDK.MQTTLib as AWSIoTPyMQTT

   import json
   ```

```
import psutil
import argparse
import logging
import time


# Configures the argument parser for this program.
def configureParser():
    parser = argparse.ArgumentParser()
    parser.add_argument(
        "-e",
        "--endpoint",
        action="store",
        required=True,
        dest="host",
        help="Your AWS IoT custom endpoint",
    )
    parser.add_argument(
        "-r",
        "--rootCA",
        action="store",
        required=True,
        dest="rootCAPath",
        help="Root CA file path",
    )
    parser.add_argument(
        "-c",
        "--cert",
        action="store",
        required=True,
        dest="certificatePath",
        help="Certificate file path",
    )
    parser.add_argument(
        "-k",
        "--key",
        action="store",
        required=True,
        dest="privateKeyPath",
        help="Private key file path",
    )
    parser.add_argument(
        "-p",
        "--port",
```

```
        action="store",
        dest="port",
        type=int,
        default=8883,
        help="Port number override",
    )
    parser.add_argument(
        "-n",
        "--thingName",
        action="store",
        required=True,
        dest="thingName",
        help="Targeted thing name",
    )
    parser.add_argument(
        "-d",
        "--requestDelay",
        action="store",
        dest="requestDelay",
        type=float,
        default=1,
        help="Time between requests (in seconds)",
    )
    parser.add_argument(
        "-v",
        "--enableLogging",
        action="store_true",
        dest="enableLogging",
        help="Enable logging for the AWS IoT Device SDK for Python",
    )
    return parser


# An MQTT shadow client that uploads device performance data to AWS IoT at a
 regular interval.
class PerformanceShadowClient:
    def __init__(
        self,
        thingName,
        host,
        port,
        rootCAPath,
        privateKeyPath,
        certificatePath,
```

```
        requestDelay,
    ):
        self.thingName = thingName
        self.host = host
        self.port = port
        self.rootCAPath = rootCAPath
        self.privateKeyPath = privateKeyPath
        self.certificatePath = certificatePath
        self.requestDelay = requestDelay

    # Updates this thing's shadow with system performance data at a regular
 interval.
    def run(self):
        print("Connecting MQTT client for {}...".format(self.thingName))
        mqttClient = self.configureMQTTClient()
        mqttClient.connect()
        print("MQTT client for {} connected".format(self.thingName))
        deviceShadowHandler = mqttClient.createShadowHandlerWithName(
            self.thingName, True
        )

        print("Running performance shadow client for {}...
\n".format(self.thingName))
        while True:
            performance = self.readPerformance()
            print("[{}]".format(self.thingName))
            print("CPU:\t{}%".format(performance["cpu"]))
            print("Memory:\t{}%\n".format(performance["memory"]))
            payload = {"state": {"reported": performance}}
            deviceShadowHandler.shadowUpdate(
                json.dumps(payload), self.shadowUpdateCallback, 5
            )
            time.sleep(args.requestDelay)

    # Configures the MQTT shadow client for this thing.
    def configureMQTTClient(self):
        mqttClient = AWSIoTPyMQTT.AWSIoTMQTTShadowClient(self.thingName)
        mqttClient.configureEndpoint(self.host, self.port)
        mqttClient.configureCredentials(
            self.rootCAPath, self.privateKeyPath, self.certificatePath
        )
        mqttClient.configureAutoReconnectBackoffTime(1, 32, 20)
        mqttClient.configureConnectDisconnectTimeout(10)
        mqttClient.configureMQTTOperationTimeout(5)
```

```
        return mqttClient

    # Returns the local device's CPU usage, memory usage, and timestamp.
    def readPerformance(self):
        cpu = psutil.cpu_percent()
        memory = psutil.virtual_memory().percent
        timestamp = time.time()
        return {"cpu": cpu, "memory": memory, "timestamp": timestamp}

    # Prints the result of a shadow update call.
    def shadowUpdateCallback(self, payload, responseStatus, token):
        print("[{}]".format(self.thingName))
        print("Update request {} {}\n".format(token, responseStatus))


# Configures debug logging for the AWS IoT Device SDK for Python.
def configureLogging():
    logger = logging.getLogger("AWSIoTPythonSDK.core")
    logger.setLevel(logging.DEBUG)
    streamHandler = logging.StreamHandler()
    formatter = logging.Formatter(
        "%(asctime)s - %(name)s - %(levelname)s - %(message)s"
    )
    streamHandler.setFormatter(formatter)
    logger.addHandler(streamHandler)


# Runs the performance shadow client with user arguments.
if __name__ == "__main__":
    parser = configureParser()
    args = parser.parse_args()
    if args.enableLogging:
        configureLogging()
    thingClient = PerformanceShadowClient(
        args.thingName,
        args.host,
        args.port,
        args.rootCAPath,
        args.privateKeyPath,
        args.certificatePath,
        args.requestDelay,
    )
    thingClient.run()
```

8. Esegui `thing_performance.py` dalla riga di comando con i parametri seguenti:

   - `-n`, `--thingName` — Nome del tuo oggetto, ad esempio**`SiteWiseTutorialDevice1`**.
   - `-e`, `--endpoint` — L' AWS IoT endpoint personalizzato salvato in precedenza in questa procedura.
   - `-r`, `--rootCA` — Il percorso del certificato CA AWS IoT principale.
   - `-c`, `--cert` — Il percorso del tuo certificato AWS IoT Thing.
   - `-k`, `--key` — Il percorso della chiave privata del tuo AWS IoT Thing Certificate.
   - `-d`, `--requestDelay` — (Facoltativo) Il tempo di attesa, in secondi, tra un aggiornamento dello shadow del dispositivo e l'altro. Il valore predefinito è 1 secondo.
   - `-v`, `--enableLogging` — (Facoltativo) Se questo parametro è presente, lo script stampa i messaggi di debug da. SDK per dispositivi AWS IoT per Python

   Il comando è simile al seguente esempio:

   ```
   python3 thing_performance.py \
     --thingName SiteWiseTutorialDevice1 \
     --endpoint identifier.iot.region.amazonaws.com \
     --rootCA AmazonRootCA1.pem \
     --cert device1/thing-id-certificate.pem.crt \
     --key device1/thing-id-private.pem.key
   ```

   Se state eseguendo lo script per altre AWS IoT operazioni, aggiornate di conseguenza il nome dell'oggetto e la directory del certificato.

9. Provare ad aprire e chiudere i programmi sul dispositivo per vedere come cambiano gli utilizzi della CPU e della memoria. Lo script stampa ogni lettura dell'utilizzo della CPU e della memoria. Se lo script carica i dati nel servizio shadow del dispositivo correttamente, l'output dello script è simile all'esempio seguente.

   ```
   [SiteWiseTutorialDevice1]
   CPU:    24.6%
   Memory: 85.2%

   [SiteWiseTutorialDevice1]
   Update request e6686e44-fca0-44db-aa48-3ca81726f3e3 accepted
   ```

10. Attenersi alla seguente procedura per verificare che lo script aggiorni la shadow del dispositivo:

a. Passare alla console AWS IoT.

b. Nel riquadro di navigazione a sinistra, scegli Tutti i dispositivi, quindi scegli Cose.

c. Scegli quello che fa per te, SiteWiseTutorialDevice.

d. Scegliete la scheda Device Shadows, scegliete Classic Shadow e verificate che lo stato Shadow sia simile al seguente esempio.

```
{
  "reported": {
    "cpu": 24.6,
    "memory": 85.2,
    "timestamp": 1579567542.2835066
  }
}
```

Se lo stato shadow della cosa è vuoto o non assomiglia all'esempio precedente, controlla che lo script sia in esecuzione e che la connessione sia avvenuta correttamente. AWS IoT Se lo script continua a scadere durante la connessione a AWS IoT, verifica che la policy relativa alle cose sia configurata in base a questo tutorial.

11. Attenersi alla seguente procedura per verificare che l'azione di regola invii dati ad AWS IoT SiteWise:

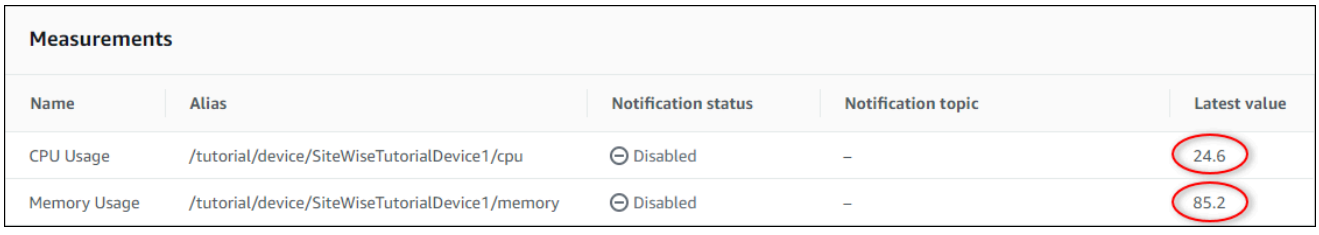
a. Passare alla console AWS IoT SiteWise.

b. Nel riquadro di navigazione a sinistra, scegli Asset.

c. Scegliere la freccia accanto all'asset parco istanze dei dispositivi (SiteWise Tutorial Device Fleet 1 1) per espandere la gerarchia degli asset, quindi scegliere l'asset dispositivo (SiteWise Tutorial Device 1).

d. Scegliere Measurements (Misurazioni).

e. Verificare che le celle Latest value (Valore più recente) abbiano i valori per le proprietà CPU Usage e Memory Usage.



f. Se le proprietà CPU Usage e Memory Usage non hanno i valori più recenti, aggiornare la pagina. Se i valori non vengono visualizzati dopo pochi minuti, consultare Risoluzione dei problemi relativi a una regola.

12. Il tutorial è stato completato. Per esplorare le visualizzazioni dei dati in tempo reale, è possibile configurare un portale in AWS IoT SiteWise Monitor. Per ulteriori informazioni, consulta Monitoraggio dei dati con AWS IoT SiteWise Monitor. In caso contrario, è possibile premere CTRL+C nel prompt dei comandi per arrestare lo script client del dispositivo. È improbabile che il programma Python invii un numero di messaggi tale da comportare un addebito, ma è consigliabile arrestare il programma al termine delle operazioni.

Fase 9: Pulizia delle risorse dopo il tutorial

Dopo aver completato il tutorial sull'acquisizione di dati dagli AWS IoT oggetti, ripulisci le risorse per evitare di incorrere in costi aggiuntivi.

Per eliminare risorse gerarchiche in AWS IoT SiteWise

1. Vai alla console AWS IoT SiteWise
2. Nel riquadro di navigazione a sinistra, scegli Asset.
3. Quando eliminate delle risorse in AWS IoT SiteWise, dovete prima dissociarle.

   Completare la procedura seguente per dissociare gli asset del dispositivo dall'asset parco istanze dei dispositivi:

   a. Scegliete la risorsa del parco dispositivi (SiteWise Tutorial Device Fleet 1).
   b. Scegli Modifica.
   c. In Assets associated to this asset (Asset associati a questo asset), scegliere Disassociate (Dissocia) per ogni asset dispositivo associato a questo asset parco istanze dei dispositivi.
   d. Selezionare Salva.

      A questo punto gli asset dispositivo non sono più organizzati in gerarchia.
4. Scegliere l'asset dispositivo (SiteWise Tutorial Device 1).
5. Scegli Elimina.
6. Nella finestra di dialogo di conferma immettere **`Delete`** e quindi scegliere Delete (Elimina).
7. Ripeti i passaggi da 4 a 6 per ogni risorsa del dispositivo e per la risorsa del parco dispositivi (SiteWise Tutorial Device Fleet 1).

Per eliminare i modelli di asset gerarchici in AWS IoT SiteWise

1. Passare alla console AWS IoT SiteWise.
2. Se non è già stato fatto, eliminare gli asset del dispositivo e del parco istanze dei dispositivi. Per ulteriori informazioni, consultare la procedura precedente. Non è possibile eliminare un modello se sono presenti asset creati da quel modello.
3. Nel riquadro di navigazione a sinistra scegliere Models (Modelli).
4. Scegliere l'asset parco istanze dei dispositivi (SiteWise Tutorial Device Fleet Model).

   Quando eliminate i modelli di asset gerarchici, iniziate eliminando prima il modello di asset principale.
5. Scegli Elimina.
6. Nella finestra di dialogo di conferma immettere **`Delete`** e quindi scegliere Delete (Elimina).
7. Ripetere i passaggi da 4 a 6 per il modello di asset del dispositivo (SiteWise Tutorial Device Model).

Per disabilitare o eliminare una regola in AWS IoT Core

1. Passare alla console AWS IoT.
2. Nel riquadro di navigazione a sinistra, scegli Routing dei messaggi, quindi scegli Regole.
3. Seleziona la tua regola e scegli Elimina.
4. Nella finestra di dialogo di conferma, inserisci il nome della regola, quindi scegli Elimina.

Visualizzazione e condivisione dei dati dei parchi eolici in Monitor SiteWise

Questo tutorial spiega come visualizzare e condividere dati industriali tramite applicazioni web gestite, note come portali. AWS IoT SiteWise Monitor Ogni portale comprende progetti e offre la flessibilità di scegliere quali dati sono accessibili all'interno di ciascun progetto. Quindi, specifica le persone della tua organizzazione che possono accedere a ciascun portale. I tuoi utenti accedono ai portali utilizzando AWS IAM Identity Center gli account, in modo che tu possa utilizzare il tuo archivio di identità esistente o uno store gestito da AWS.

Tu e gli utenti con le autorizzazioni sufficienti potete creare i pannelli di controllo in ogni progetto per visualizzare i dati di settore in modo significativo. Quindi, gli utenti possono visualizzare questi

pannelli di controllo per ottenere rapidamente informazioni dettagliate sui dati e monitorare le operazioni. Puoi configurare autorizzazioni amministrative o di sola lettura per ogni progetto e per ogni utente della società. Per ulteriori informazioni, consulta Monitoraggio dei dati con AWS IoT SiteWise Monitor.

Nel corso del tutorial, migliorerai la AWS IoT SiteWise demo, fornendo un set di dati di esempio per un parco eolico. Si configura un portale in SiteWise Monitor, si crea un progetto e si creano dashboard per visualizzare i dati del parco eolico. Il tutorial copre anche la creazione di utenti aggiuntivi, insieme all'assegnazione delle autorizzazioni per possedere o visualizzare il progetto e le dashboard associate.

> **Note**
>
> Quando usi SiteWise Monitor, ti viene addebitato un costo per utente che accede a un portale (al mese). In questo tutorial vengono creati tre utenti, ma dovrà accedere solo un utente. Dopo aver completato questo tutorial, ti vengono addebitati i costi per un utente. Per ulteriori informazioni, consulta la sezione Prezzi di AWS IoT SiteWise.

Argomenti

Prerequisiti

Per completare questo tutorial, è necessario quanto segue:

- Un Account AWS. Se non lo hai, consultare Configurare un Account AWS.
- Un computer di sviluppo che esegue WindowsmacOS,Linux, o Unix per accedere a AWS Management Console. Per ulteriori informazioni, consulta Nozioni di base su AWS Management Console.

- Un utente AWS Identity and Access Management (IAM) con autorizzazioni di amministratore.
- Una demo di un parco AWS IoT SiteWise eolico funzionante. Quando configuri la demo, definisce i modelli e gli asset AWS IoT SiteWise e trasmette loro i dati per rappresentare un parco eolico. Per ulteriori informazioni, consulta Utilizzo della AWS IoT SiteWise demo.
- Se hai abilitato IAM Identity Center nel tuo account, accedi al tuo account di AWS Organizations gestione. Per ulteriori informazioni, consulta Concetti e terminologia di AWS Organizations. Se non hai abilitato IAM Identity Center, lo abiliterai in questo tutorial e imposterai il tuo account come account di gestione.

  Se non riesci ad accedere al tuo account di AWS Organizations gestione, puoi completare parzialmente il tutorial purché nella tua organizzazione sia presente un utente IAM Identity Center. In questo caso, puoi creare il portale e le dashboard, ma non puoi creare nuovi utenti IAM Identity Center da assegnare ai progetti.

Passaggio 1: crea un portale in Monitor SiteWise

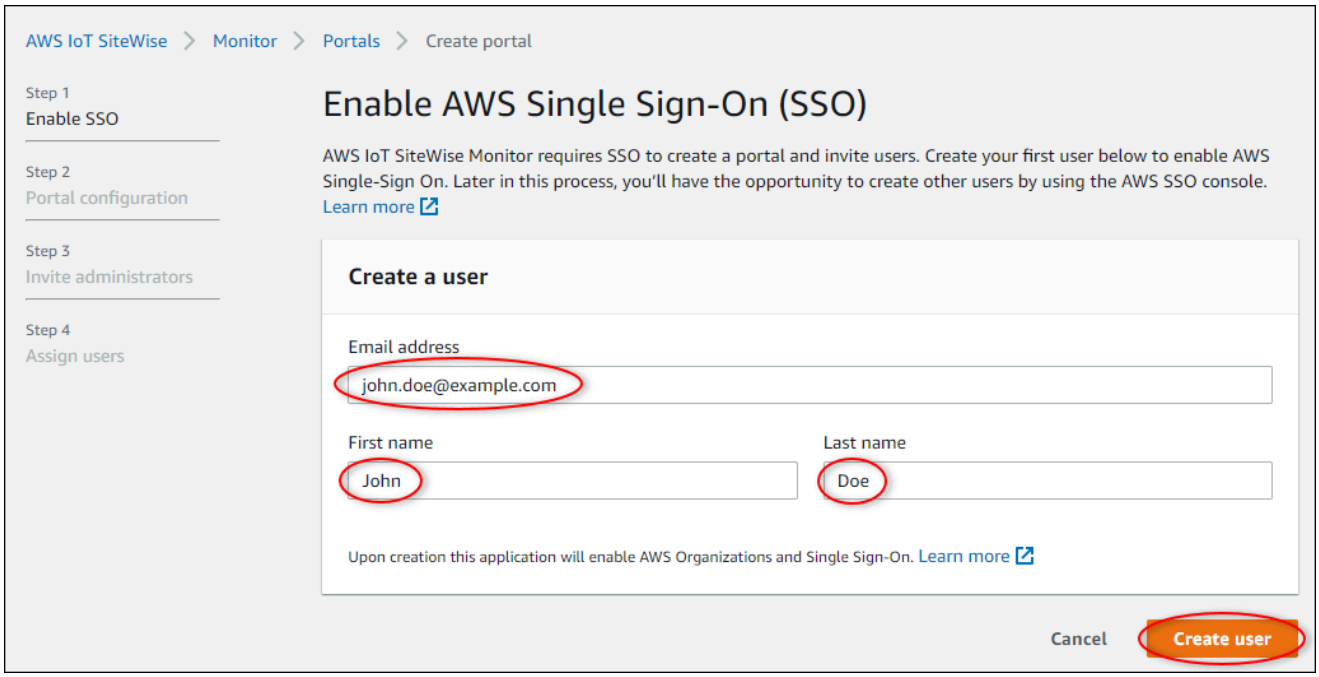
In questa procedura crei un portale in AWS IoT SiteWise Monitor. Ogni portale è un'applicazione web gestita a cui tu e i tuoi utenti potete accedere con AWS IAM Identity Center gli account. Con IAM Identity Center, puoi utilizzare l'archivio di identità esistente della tua azienda o crearne uno gestito da AWS. I dipendenti della tua azienda possono accedere senza creare file separati Account AWS.

Per creare un portale

1. Accedi alla console AWS IoT SiteWise.
2. Controlla gli AWS IoT SiteWise endpoint e le quote dove AWS IoT SiteWise è supportato e cambia regione, se necessario. È necessario eseguire la AWS IoT SiteWise demo nella stessa regione.
3. Nel riquadro di navigazione a sinistra scegliere Portals (Portali).
4. Selezionare Create portal (Crea portale).
5. Se hai già abilitato IAM Identity Center, vai al passaggio 6. Altrimenti, completa i seguenti passaggi per abilitare IAM Identity Center:

   a. Nella pagina Abilita AWS IAM Identity Center (SSO), inserisci il tuo indirizzo e-mail, nome e cognome per creare un utente IAM Identity Center che diventi amministratore del portale. Utilizza un indirizzo e-mail a cui puoi accedere in modo da ricevere un'e-mail per impostare una password per il tuo nuovo utente IAM Identity Center.

In un portale, l'amministratore del portale crea i progetti e assegna gli utenti ai progetti. Sarà possibile configurare altri utenti in un secondo momento.



b. Selezionare Create user (Crea utente).

6. Nella pagina Portal configuration (Configurazione portale) completare i passaggi seguenti:

   a. Immettere un nome per il portale, ad esempio **`WindFarmPortal`**.

   b. (Facoltativo) Inserire una descrizione del portale. Se si dispone di più portali, utilizzare descrizioni significative per tenere traccia dei contenuti di ciascuno.

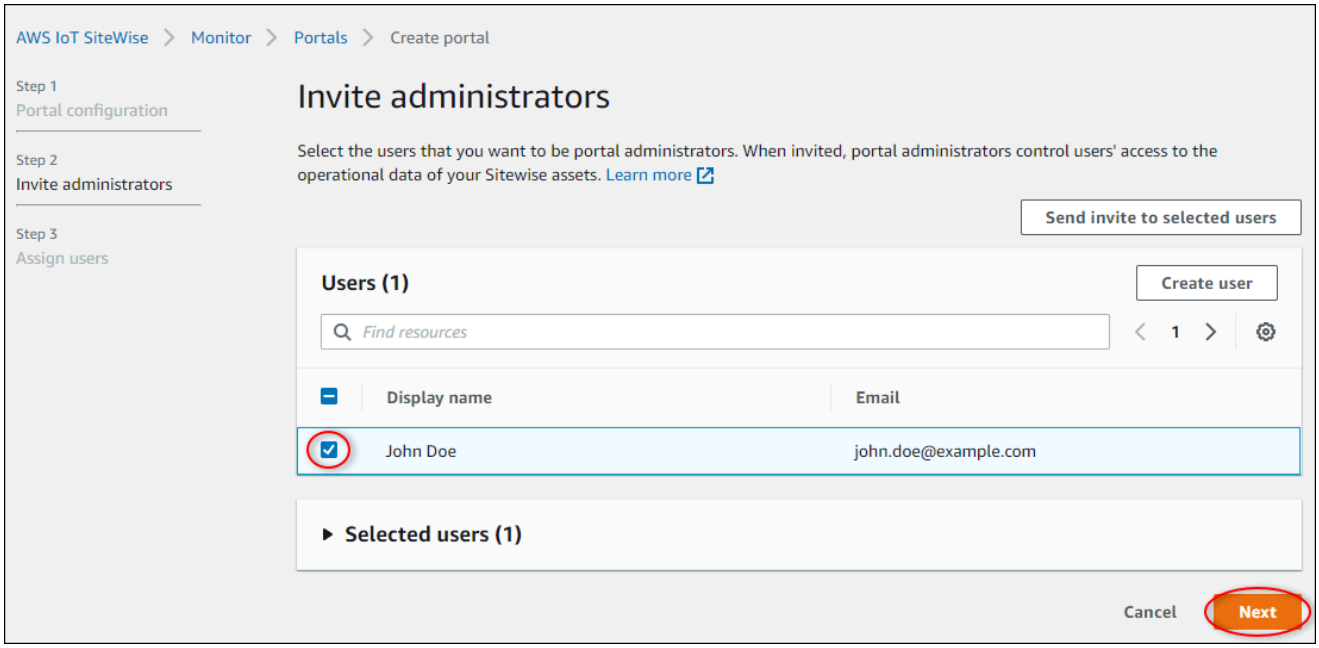
   c. (Facoltativo) Carica un'immagine da visualizzare nel portale.

   d. Immettete un indirizzo e-mail che gli utenti del portale possano contattare in caso di problemi con il portale e necessitano dell'aiuto dell' AWS amministratore dell'azienda per risolverlo.

   e. Selezionare Create portal (Crea portale).

7. Nella pagina Invita amministratori, puoi assegnare gli utenti di IAM Identity Center al portale come amministratori. Gli amministratori del portale gestiscono le autorizzazioni e i progetti all'interno di un portale. In questa pagina, effettuate le seguenti operazioni:

   a. Seleziona un utente come amministratore del portale. Se hai abilitato IAM Identity Center in precedenza in questo tutorial, seleziona l'utente che hai creato.



b. Facoltativamente, è possibile avvalersi del comando Send invite to selected users (Manda un invito agli utenti selezionati). Il tuo client di posta elettronica si apre e nel corpo del messaggio viene visualizzato un invito. È possibile personalizzare il messaggio e-mail prima di inviarlo agli amministratori del portale. È inoltre possibile inviare l'e-mail agli amministratori del portale in un secondo momento. Se stai provando SiteWise Monitor per la prima volta e sarai l'amministratore del portale, non devi inviarti un'e-mail.

c. Seleziona Successivo.

8. Nella pagina Assegna utenti, puoi assegnare gli utenti di IAM Identity Center al portale. Gli amministratori del portale possono successivamente assegnare questi utenti come proprietari o visualizzatori del progetto. I proprietari dei progetti possono creare dashboard nei progetti. I visualizzatori dei progetti hanno accesso in sola lettura ai progetti a cui sono assegnati. In questa pagina, puoi creare utenti IAM Identity Center da aggiungere al portale.

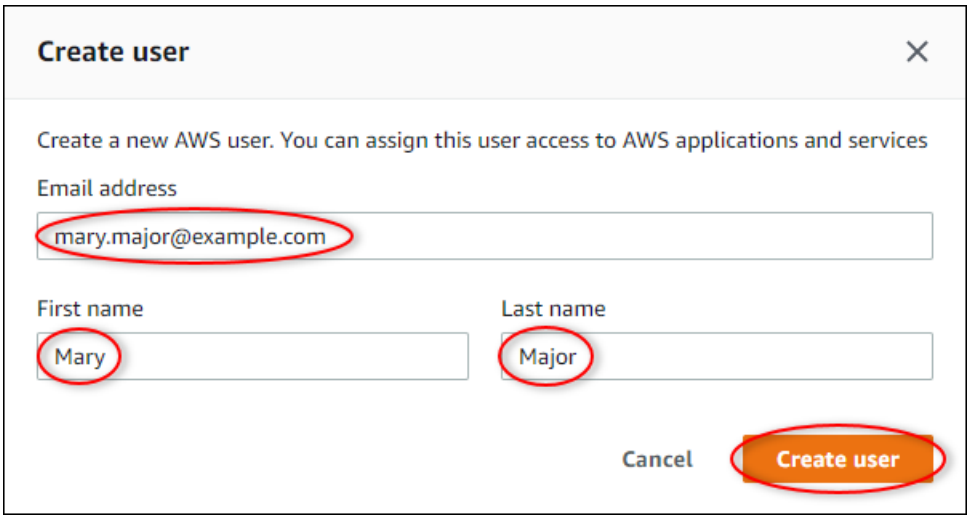
> **Note**
>
> Se non hai effettuato l'accesso al tuo account di AWS Organizations gestione, non puoi creare utenti IAM Identity Center. Scegli Assegna utenti per creare il portale senza utenti del portale, quindi salta questo passaggio.

In questa pagina, effettuate le seguenti operazioni:

a. Completa due volte i seguenti passaggi per creare due utenti IAM Identity Center:

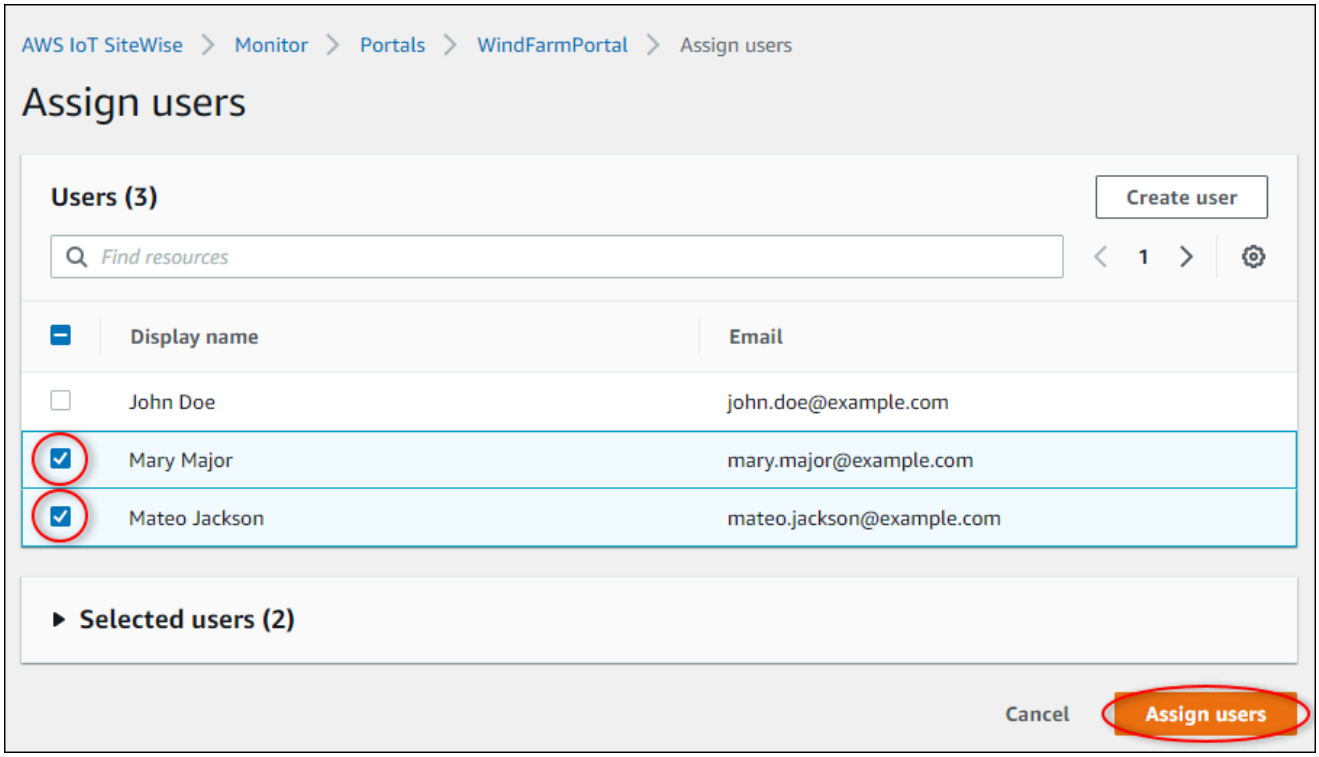
i. Scegli Crea utente per aprire una finestra di dialogo in cui inserire i dettagli per il nuovo utente.

ii. Inserisci un indirizzo e-mail, nome e cognome per il nuovo utente. IAM Identity Center invia all'utente un'e-mail per consentirgli di impostare la password. Se desideri accedere al portale come questi utenti, scegli un indirizzo email a cui puoi accedere. Ogni indirizzo e-mail deve essere unico. I tuoi utenti accedono al portale utilizzando il loro indirizzo e-mail come nome utente.



iii. Selezionare Create user (Crea utente).

b. Seleziona i due utenti IAM Identity Center che hai creato nel passaggio precedente.



c. Scegli Assegna utenti per aggiungere questi utenti al portale.

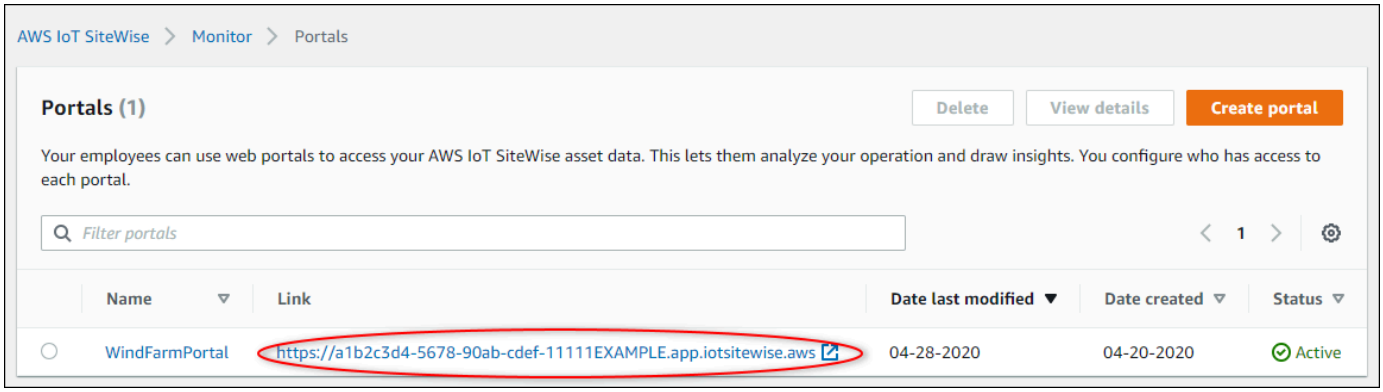
La pagina dei portali si apre con il nuovo portale elencato.

Passaggio 2: accedi a un portale

In questa procedura, si accede al nuovo portale utilizzando l' AWS IAM Identity Center utente che è stato aggiunto al portale.

Per accedere a un portale

1. Nella pagina Portals (Portali) scegliere il collegamento del nuovo portale per aprire il portale in una nuova scheda.



2. Se hai creato il tuo primo utente IAM Identity Center in precedenza nel tutorial, utilizza i seguenti passaggi per creare una password per il tuo utente:

   a. Cercare l'email con l'oggetto Invitation to join AWS IAM Identity Center.

   b. Aprire l'e-mail di invito e scegliere Accept invitation.

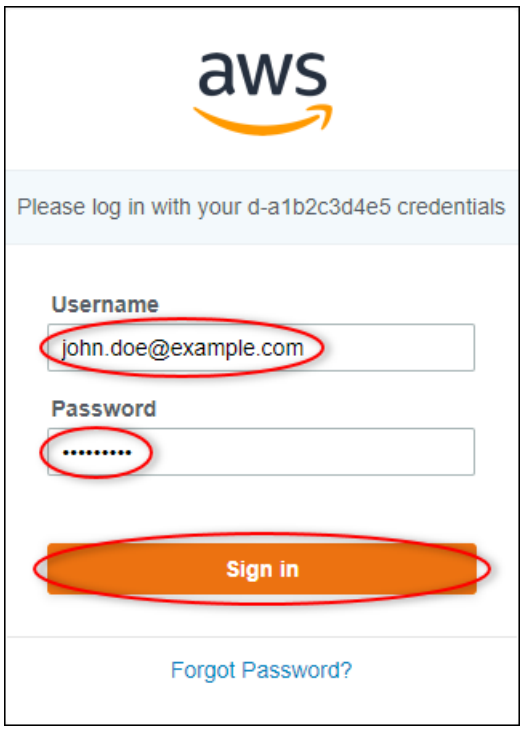
   c. Nella nuova finestra, imposta una password per il tuo utente IAM Identity Center.

   Se desideri accedere successivamente al portale come secondo e terzo utente IAM Identity Center che hai creato in precedenza, puoi anche completare questi passaggi per impostare le password per quegli utenti.

   > **Note**
   >
   > Se non hai ricevuto un'e-mail, puoi generare una password per il tuo utente nella console IAM Identity Center. Per ulteriori informazioni, consulta Reimpostazione di una password utente nella Guida AWS IAM Identity Center per l'utente.

3. Accedi al tuo IAM Identity Center Usernamee Password. Se hai creato il tuo utente IAM Identity Center in precedenza in questo tutorial, il tuo Usernameè l'indirizzo email dell'utente amministratore del portale che hai creato.

   Tutti gli utenti del portale, incluso l'amministratore del portale, devono accedere con le proprie credenziali utente IAM Identity Center. Tali credenziali, in genere, non corrispondono a quelle utilizzate per accedere alla AWS Management Console.



4. Scegli Sign in.

   Viene visualizzato il portale.

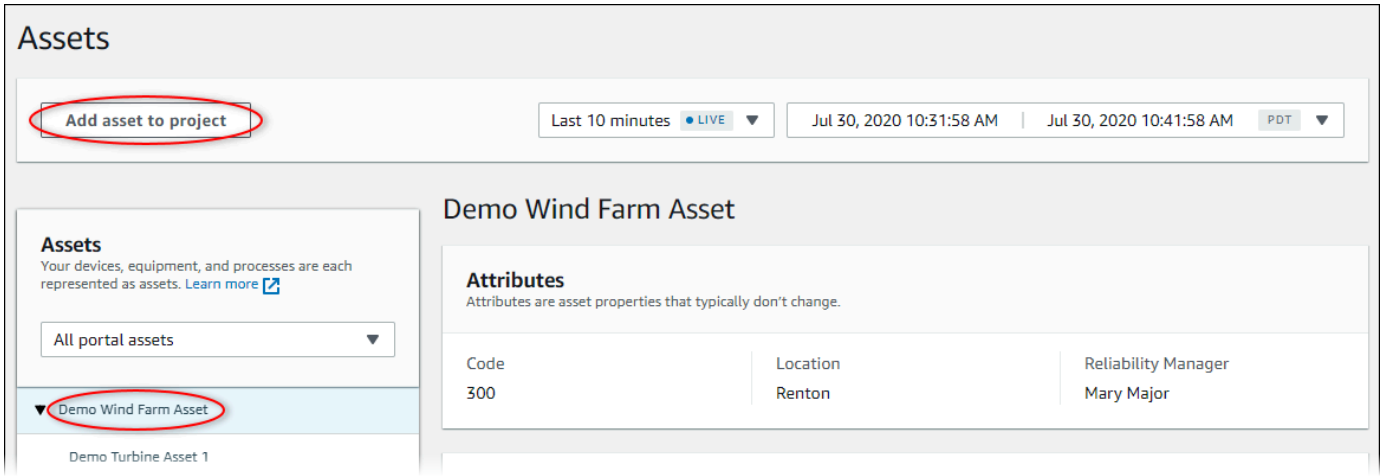
Fase 3: Creare un progetto per un parco eolico

In questa procedura crei un progetto nel portale. I progetti sono risorse che definiscono una serie di autorizzazioni, risorse e dashboard, che puoi configurare per visualizzare i dati delle risorse in quel progetto. Con i progetti, è possibile definire chi ha accesso a sottoinsiemi specifici dell'operazione e come vengono visualizzati i dati di tali sottoinsiemi. È possibile assegnare agli utenti del portale come proprietari o visualizzatori di ciascun progetto. I proprietari del progetto possono creare dashboard per visualizzare i dati e condividere il progetto con altri utenti. I visualizzatori del progetto possono visualizzare i pannelli di controllo ma non modificarli. Per ulteriori informazioni sui ruoli in SiteWise Monitor, consulta. SiteWise Monitora i ruoli

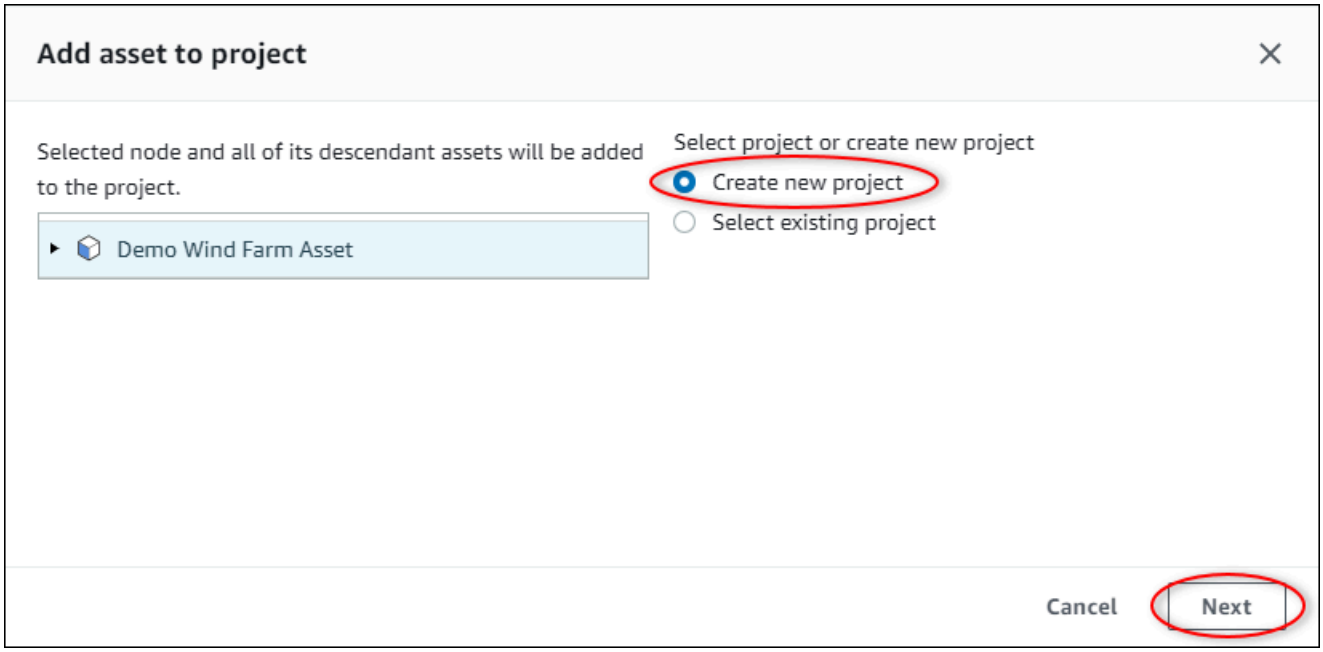
Per creare un progetto di centrale eolica

1. Nel riquadro di navigazione a sinistra del portale, scegli la scheda Risorse. Nella pagina Risorse, puoi esplorare tutte le risorse disponibili nel portale e aggiungere risorse ai progetti.

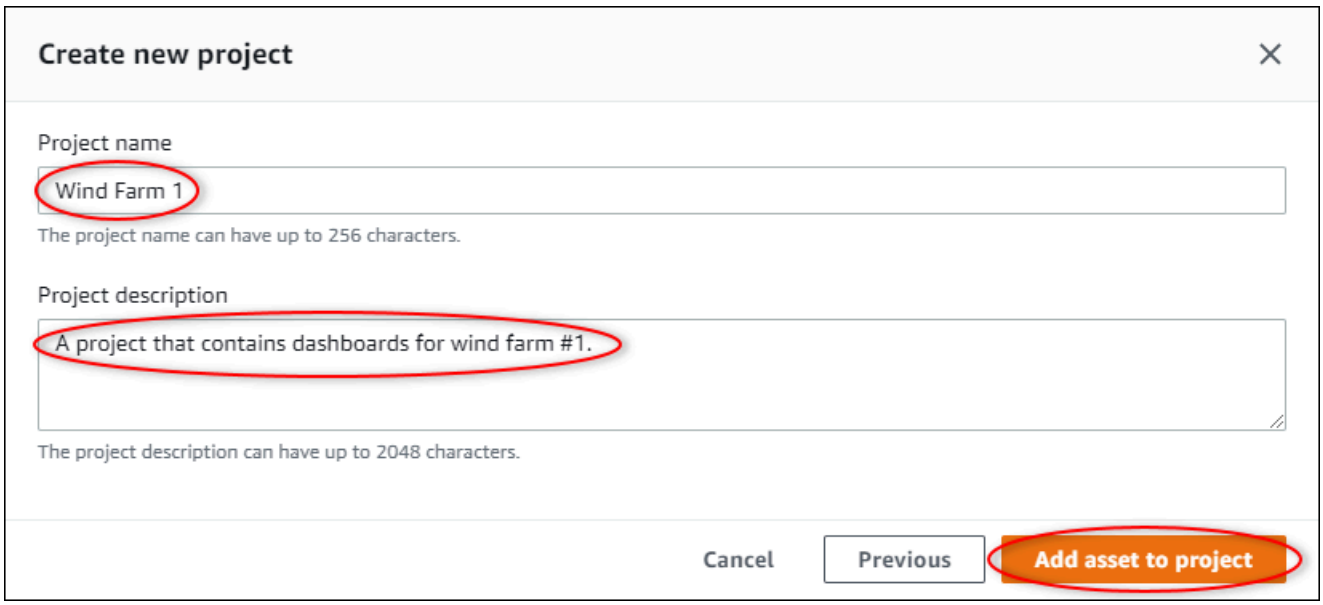
2. Nel browser degli asset, scegliere Demo Wind Farm Asset. Quando scegli una risorsa, puoi esplorare i dati storici e in tempo reale di quella risorsa. Puoi anche premere Shift per selezionare più risorse e confrontarne i dati side-by-side.
3. Scegli Aggiungi risorsa al progetto in alto a sinistra. I progetti contengono i pannelli di controllo che gli utenti del portale possono visualizzare per esplorare i dati. Ogni progetto ha accesso a un sottoinsieme delle tue risorse in AWS IoT SiteWise. Quando si aggiunge un asset a un progetto, tutti gli utenti con accesso a tale progetto possono anche accedere ai dati relativi all'asset e ai relativi elementi figlio.



4. Nella finestra di dialogo Aggiungi risorsa al progetto, scegli Crea nuovo progetto, quindi scegli Avanti.



5. Nella finestra di dialogo Crea nuovo progetto, inserisci un nome e una descrizione del progetto per il tuo progetto, quindi scegli Aggiungi risorsa al progetto.



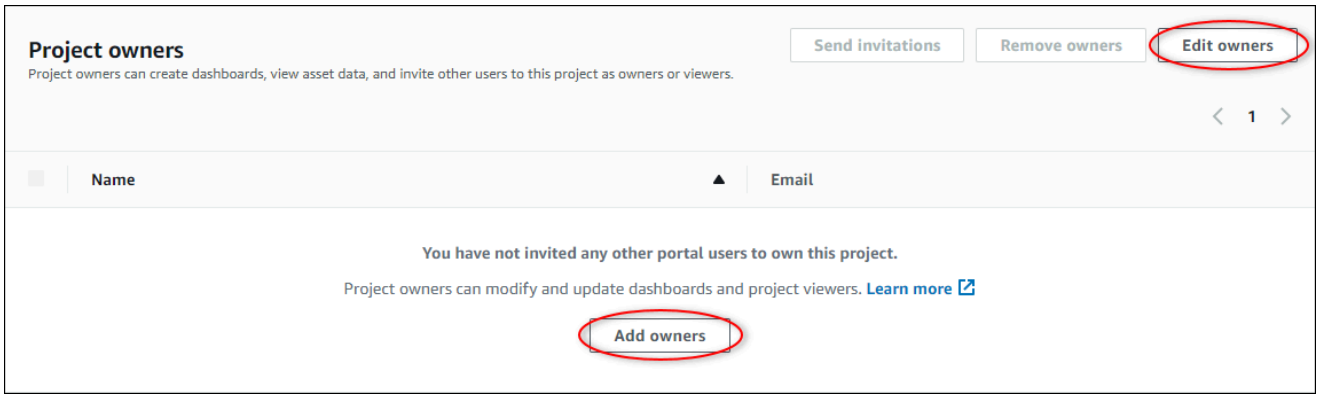
Viene visualizzata la pagina del nuovo progetto.

6. Nella pagina del progetto, è possibile aggiungere utenti del portale come proprietari o visualizzatori del progetto.

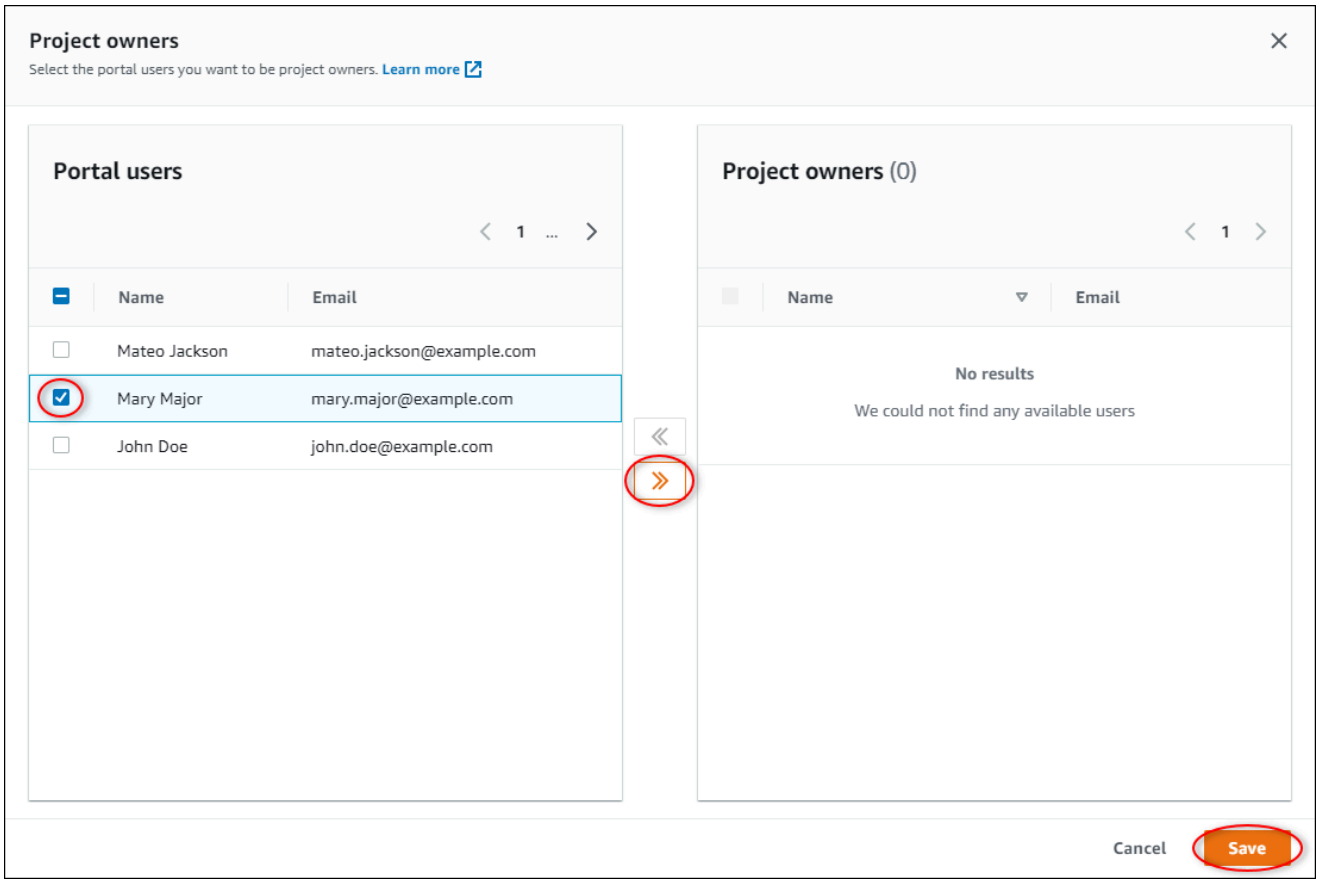
> **Note**
>
> Se non hai effettuato l'accesso al tuo account di AWS Organizations gestione, potresti non avere utenti del portale da assegnare a questo progetto, quindi puoi saltare questo passaggio.

In questa pagina, procedi come segue:

a. In Proprietari del progetto, scegli Aggiungi proprietari o Modifica utenti.



b. Scegliere l'utente da aggiungere come proprietario del progetto, Mary Major), quindi scegliere l'icona >>.



c. Selezionare Salva.

Il tuo utente IAM Identity Center Mary Majorpuò accedere a questo portale per modificare i dashboard di questo progetto e condividerlo con altri utenti in questo portale.

d. In Visualizzatori del progetto, scegli Aggiungi visualizzatori o Modifica utenti.

e. Scegliete l'utente da aggiungere come visualizzatore del progetto (ad esempio, Mateo Jackson), quindi scegliete l'icona >>.

f. Selezionare Salva.

L'utente di IAM Identity Center Mateo Jacksonpuò accedere a questo portale per visualizzare, ma non modificare, le dashboard del progetto del parco eolico.

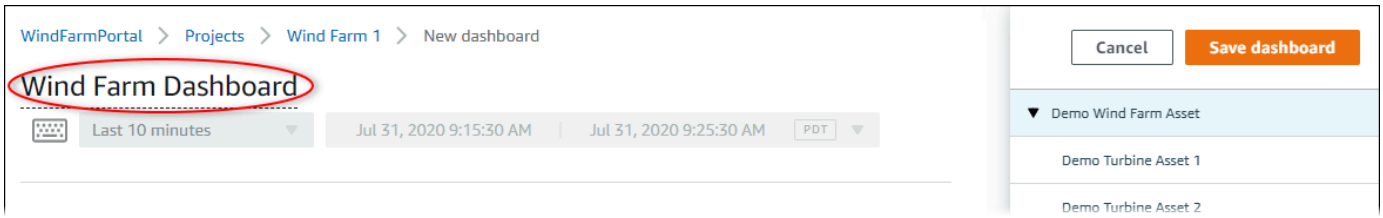
Fase 4: Crea una dashboard per visualizzare i dati del parco eolico

In questa procedura crei i pannelli di controllo per visualizzare i dati demo della centrale eolica. I pannelli di controllo contengono visualizzazioni personalizzabili dei dati degli asset del progetto. Ogni visualizzazione può avere un tipo diverso, ad esempio un grafico a linee, un grafico a barre o un indicatore chiave di prestazione (KPI). Puoi scegliere il tipo di visualizzazione più adatto ai dati. I proprietari dei progetti possono modificare le dashboard, mentre i visualizzatori dei progetti possono solo visualizzare le dashboard per ottenere informazioni dettagliate.

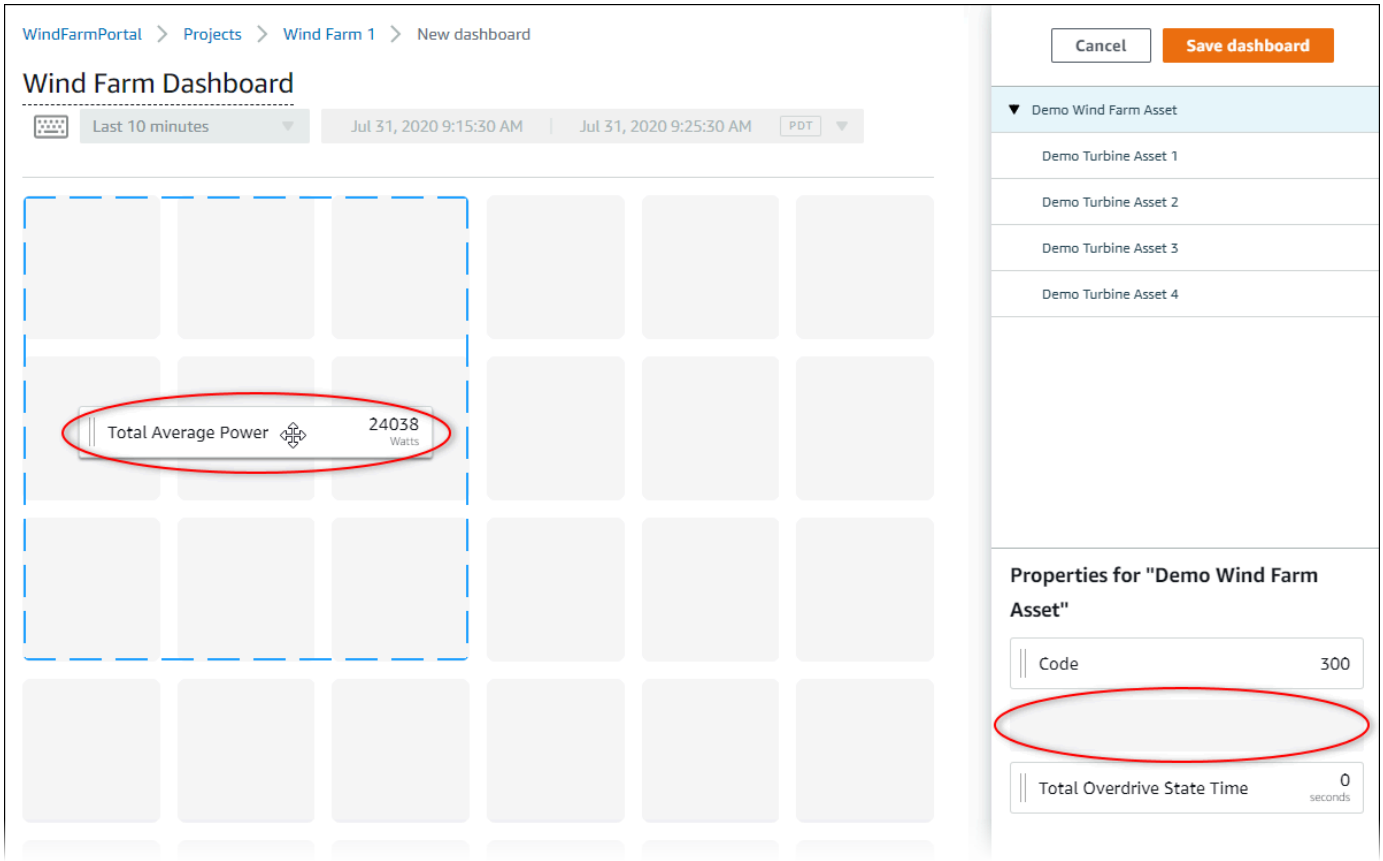
Per creare un pannello di controllo con visualizzazioni

1. Nella pagina del nuovo progetto, scegli Crea dashboard per creare una dashboard e aprirne la pagina di modifica.

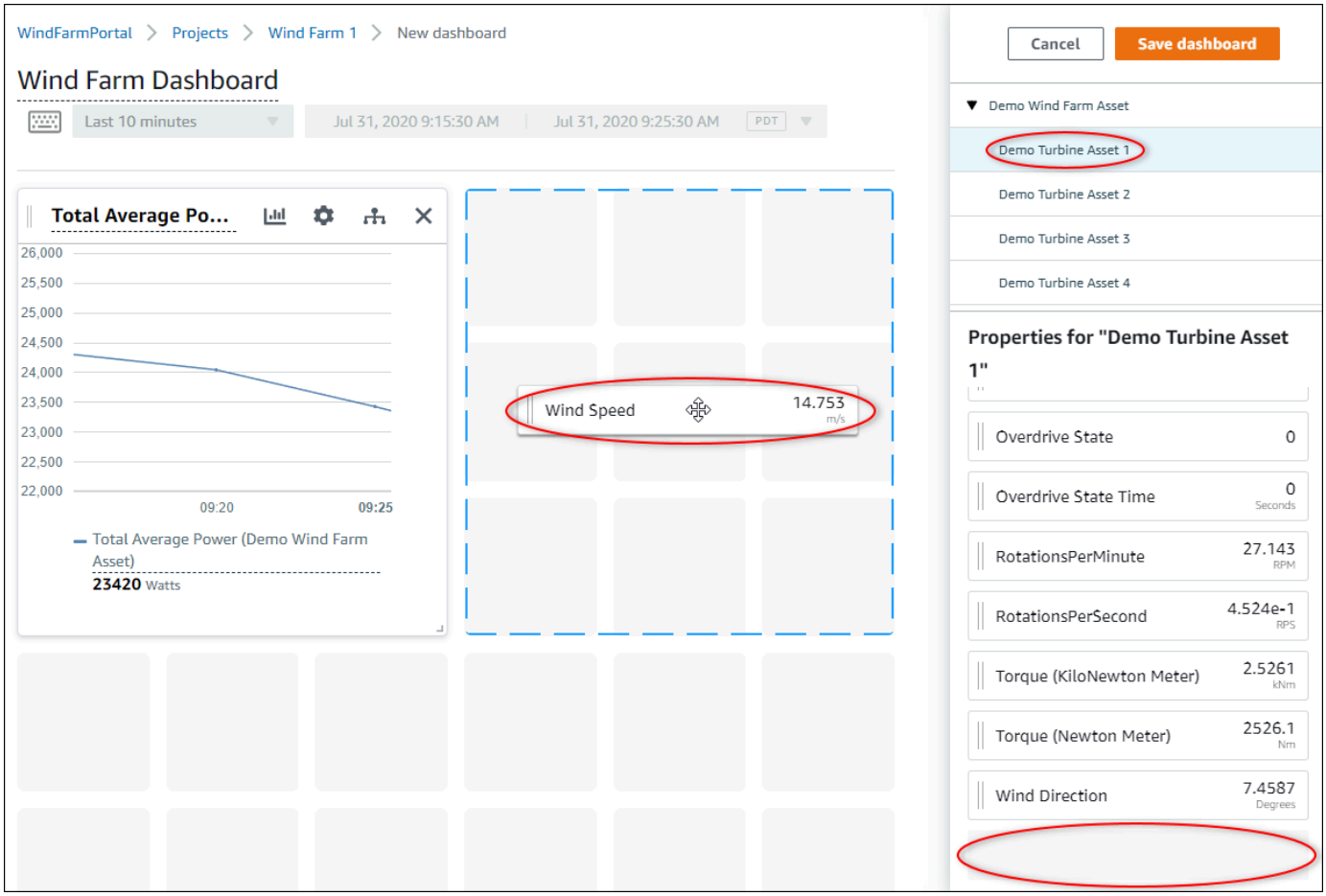
   Nella pagina di modifica di un pannello di controllo è possibile trascinare le proprietà degli asset dalla gerarchia degli asset nel pannello di controllo per creare le visualizzazioni. Quindi è possibile modificare il titolo della visualizzazione, i titoli della legenda, il tipo, le dimensioni e la posizione per ogni visualizzazione nel pannello di controllo.
2. Inserisci un nome per la tua dashboard.



3. Trascinare Total Average Power da Demo Wind Farm Asset nel pannello di controllo per creare una visualizzazione.

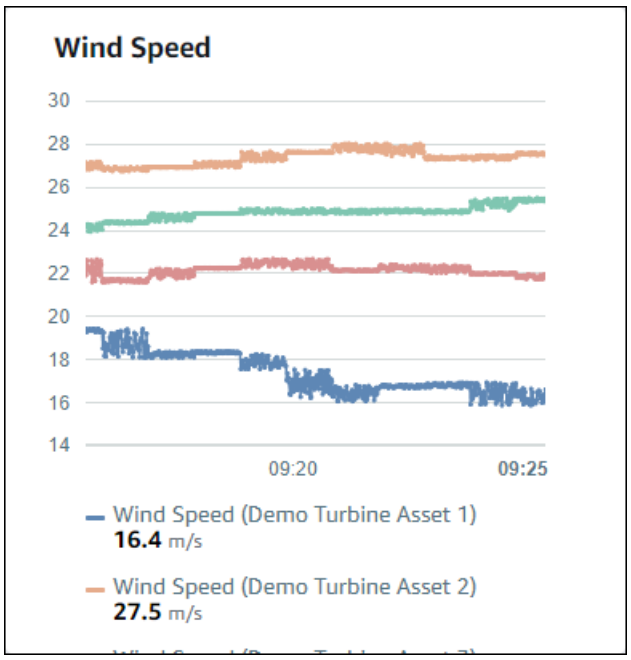


4. Scegli Demo Turbine Asset 1di mostrare le proprietà di quella risorsa, quindi trascinala sulla dashboard Wind Speedper creare una visualizzazione della velocità del vento.

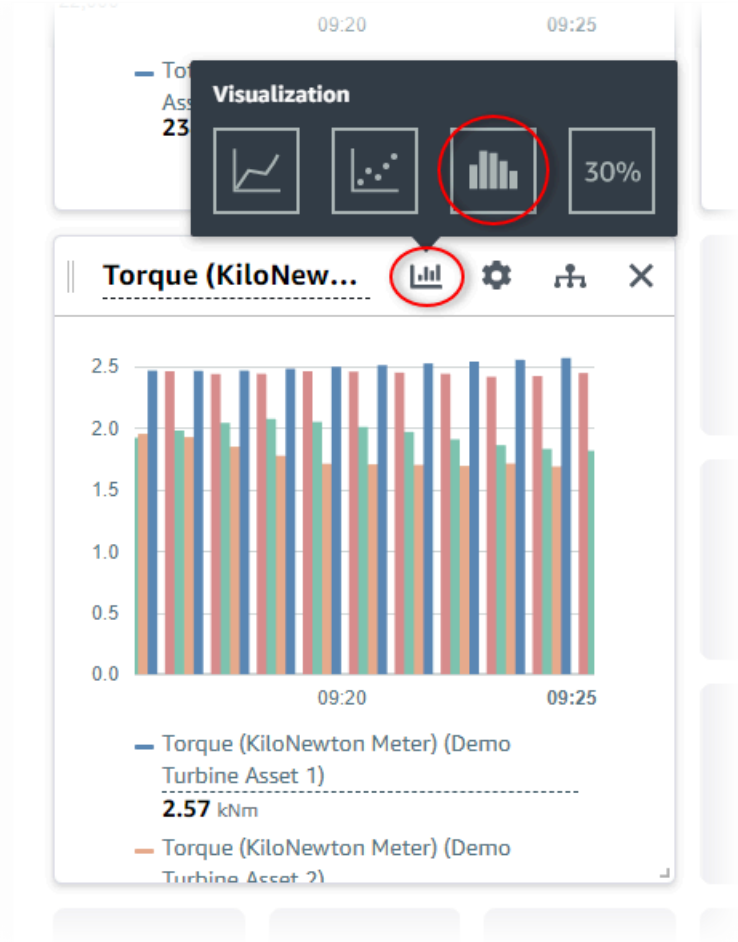


5. Aggiungere Wind Speed alla nuova visualizzazione della velocità del vento per ogni Demo Turbine Asset 2, 3 e 4 (in questo ordine).

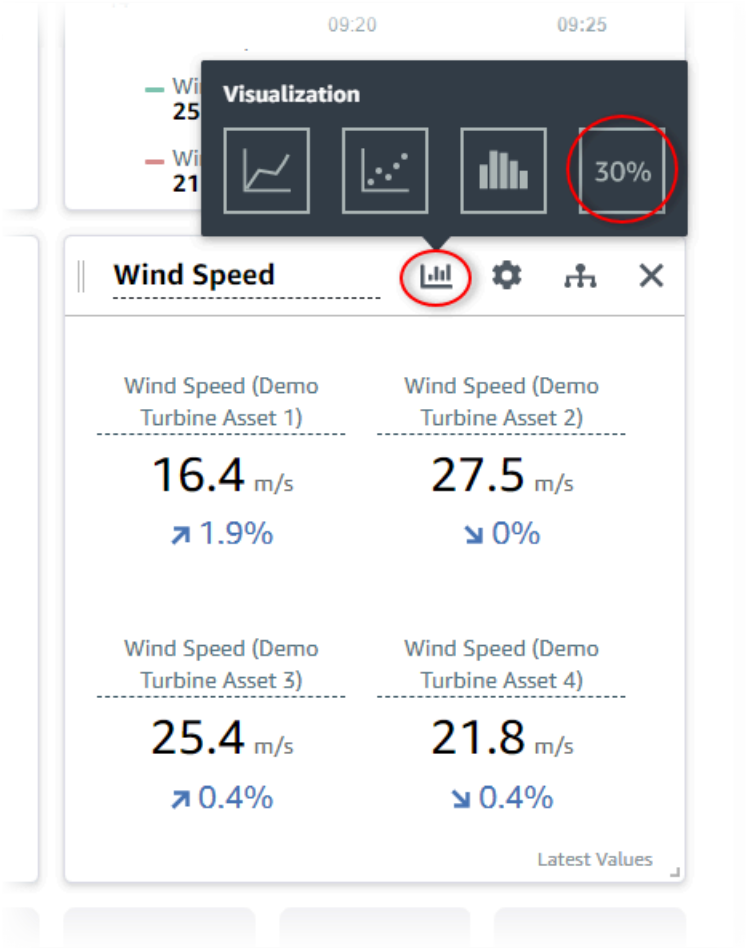
   La visualizzazione Wind Speed è simile allo screenshot seguente.



6. Ripeti i passaggi 4 e 5 per le Torque (KiloNewton Meter)proprietà delle turbine eoliche per creare una visualizzazione della coppia delle turbine eoliche.
7. Scegliere l'icona del tipo di visualizzazione per la visualizzazione Torque (KiloNewton Meter), quindi scegliere l'icona del grafico a barre.

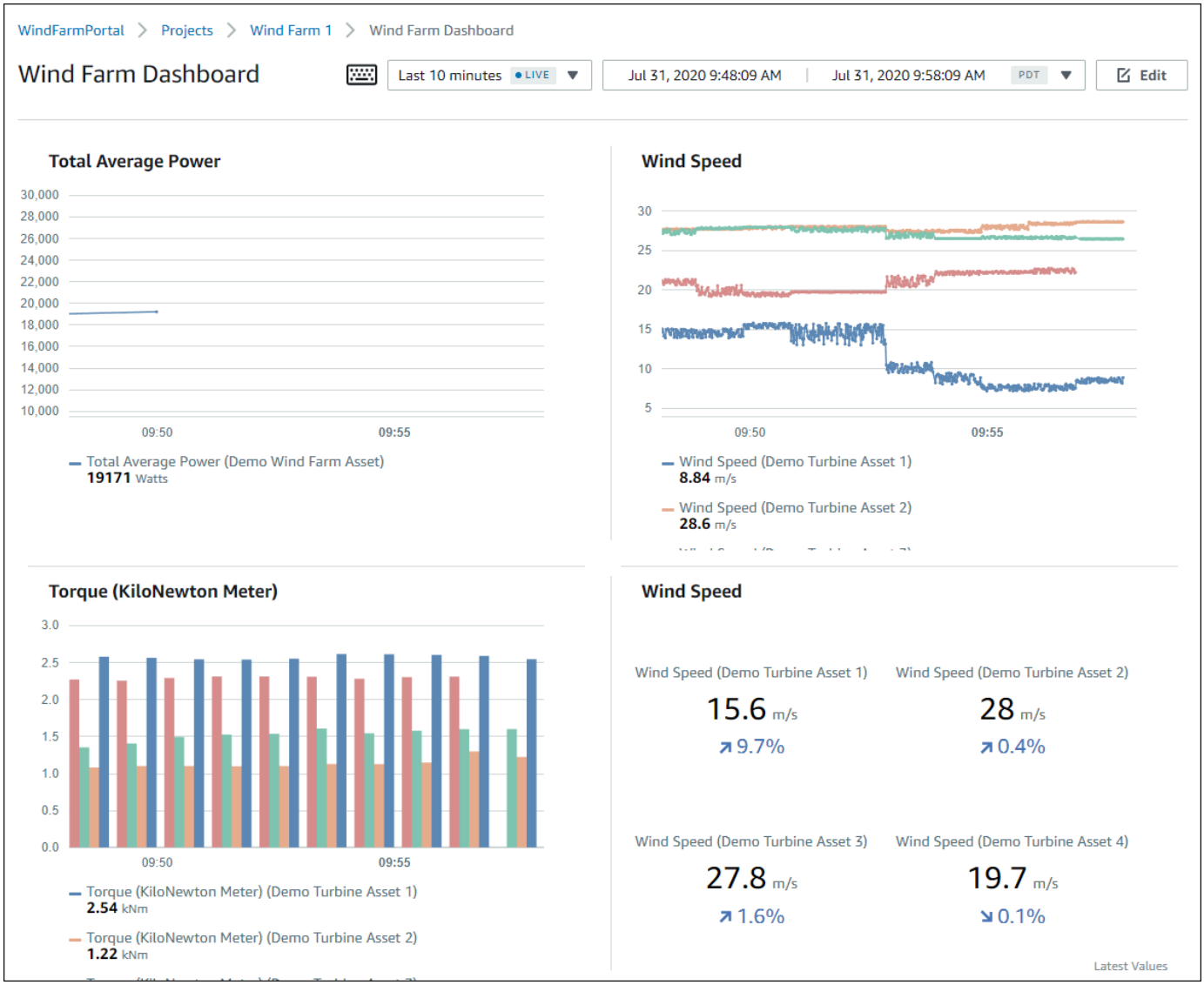


8. Ripeti i passaggi 4 e 5 per le Wind Directionproprietà delle turbine eoliche per creare una visualizzazione della direzione del vento.
9. Scegliere l'icona del tipo di visualizzazione per la visualizzazione Wind Direction, quindi scegliere l'icona del grafico KPI (30%).



10. (Facoltativo) Apportare altre modifiche al titolo della visualizzazione, ai titoli della legenda, al tipo, alle dimensioni e alla posizione per ogni visualizzazione in base alle esigenze.
11. Scegli Salva dashboard in alto a destra per salvare la dashboard.

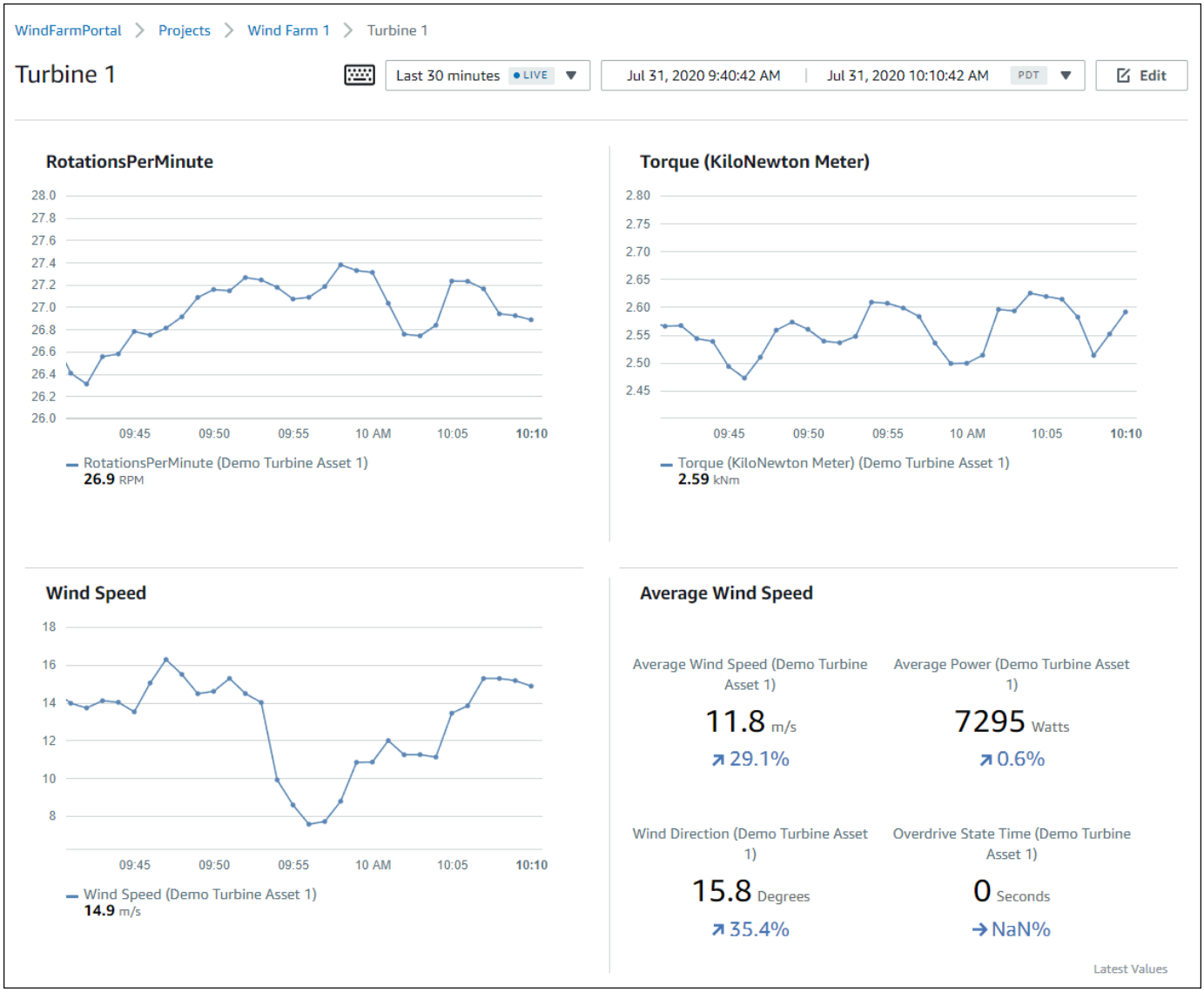
    Il pannello di controllo è simile allo screenshot seguente.



12. (Facoltativo) Creare un pannello di controllo aggiuntivo per ogni asset turbina eolica.

    Come procedura consigliata, consigliamo di creare un pannello di controllo per ogni asset in modo che i visualizzatori dei progetti possano esaminare eventuali problemi relativi a ogni singolo asset. È possibile aggiungere solo fino a 5 asset per ogni visualizzazione, pertanto è necessario creare più pannelli di controllo per gli asset gerarchici in molti scenari.

    Un pannello di controllo per una turbina eolica demo è simile allo screenshot seguente.



13. (Facoltativo) Modificare la timeline o selezionare i punti dati in una visualizzazione per esplorare i dati nel pannello di controllo. Per ulteriori informazioni, consulta Visualizzazione dei dashboard nella Guida all'AWS IoT SiteWise Monitor applicazione.

Fase 5: Esplora il portale

In questa procedura, è possibile esplorare il portale come utente con meno autorizzazioni rispetto a un amministratore del AWS IoT SiteWise portale.

Per esplorare il portale e completare il tutorial

- (Facoltativo) Se hai aggiunto altri utenti al progetto come proprietari o visualizzatori, puoi accedere al portale come tali utenti. Ciò consente di esplorare il portale come utente con meno autorizzazioni rispetto a un amministratore del portale.

  > **Important**
  >
  > Ti viene addebitato un costo per ogni utente che accede a un portale. Per ulteriori informazioni, consulta la sezione Prezzi di AWS IoT SiteWise.

  Per esplorare il portale con altri utenti, procedi come segue:

  a. Scegli Esci nella parte inferiore sinistra del portale per uscire dall'applicazione web.
  b. Scegli Esci in alto a destra nel portale applicativo IAM Identity Center per disconnetterti dal tuo utente IAM Identity Center.
  c. Accedi al portale come utente IAM Identity Center che hai assegnato come proprietario del progetto o visualizzatore del progetto. Per ulteriori informazioni, consulta Passaggio 2: accedi a un portale.

Hai completato il tutorial. Una volta terminata l'esplorazione del parco eolico dimostrativo in SiteWise Monitor, segui la procedura successiva per ripulire le risorse.

Passaggio 6: Pulisci le risorse dopo il tutorial

Una volta completato il tutorial puoi ripulire le risorse. Non viene addebitato alcun costo per AWS IoT SiteWise se gli utenti non accedono al portale, ma puoi eliminare il portale e gli utenti Elenco AWS IAM Identity Center . Gli asset della centrale eolica demo vengono eliminati alla fine della durata scelta al momento della creazione della demo oppure è possibile eliminare la demo manualmente. Per ulteriori informazioni, consulta Eliminazione della demo AWS IoT SiteWise.

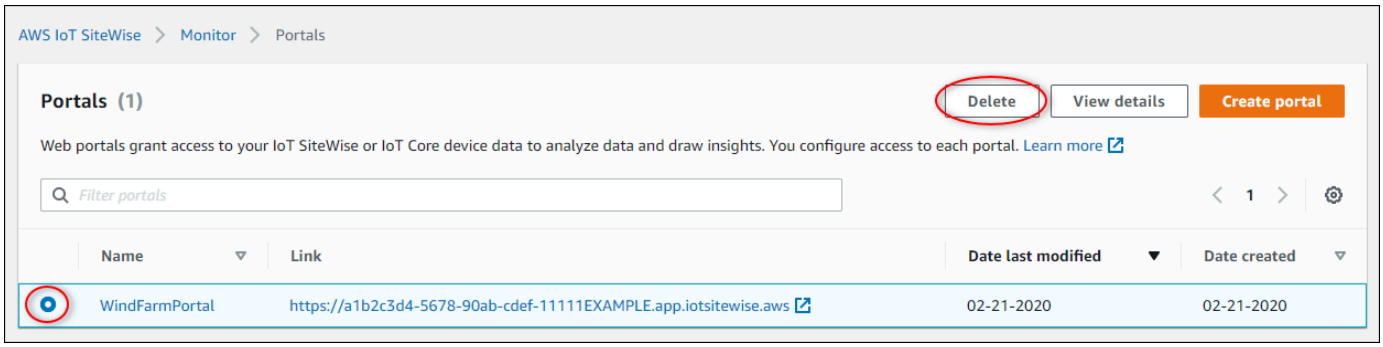
Utilizza le seguenti procedure per eliminare gli utenti del portale e di IAM Identity Center.

Per eliminare un portale

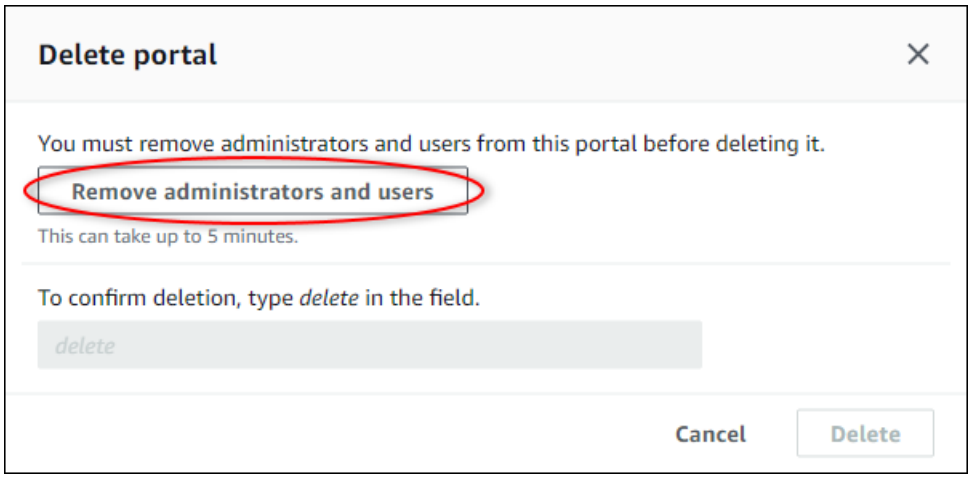
1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione a sinistra scegliere Portals (Portali).

3. Scegli il tuo portale WindFarmPortal, quindi scegli Elimina.

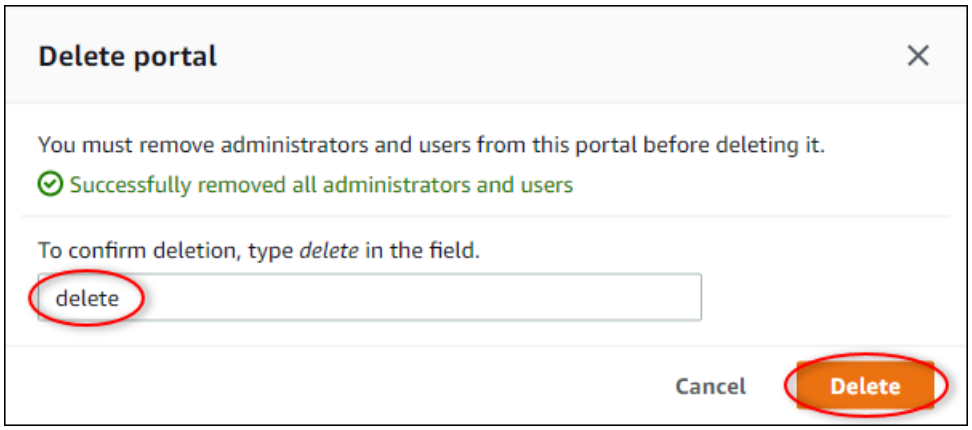
   Quando si elimina un portale o un progetto, gli asset associati ai progetti eliminati non sono interessati.



4. Nella finestra di dialogo Elimina portale, scegli Rimuovi amministratori e utenti.

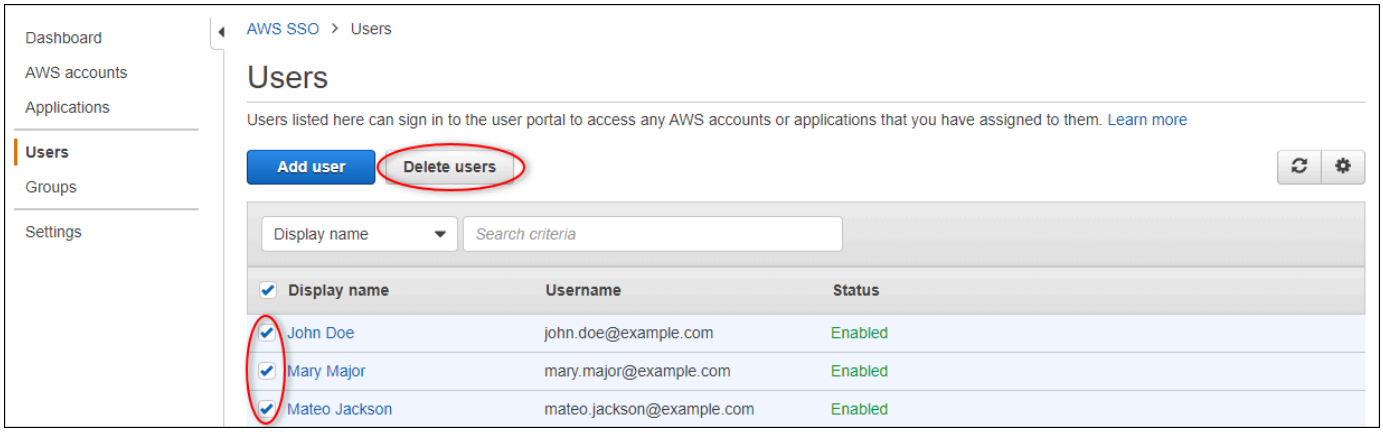


5. Immettere **`delete`** per confermare l'eliminazione, quindi scegliere Delete (Elimina).

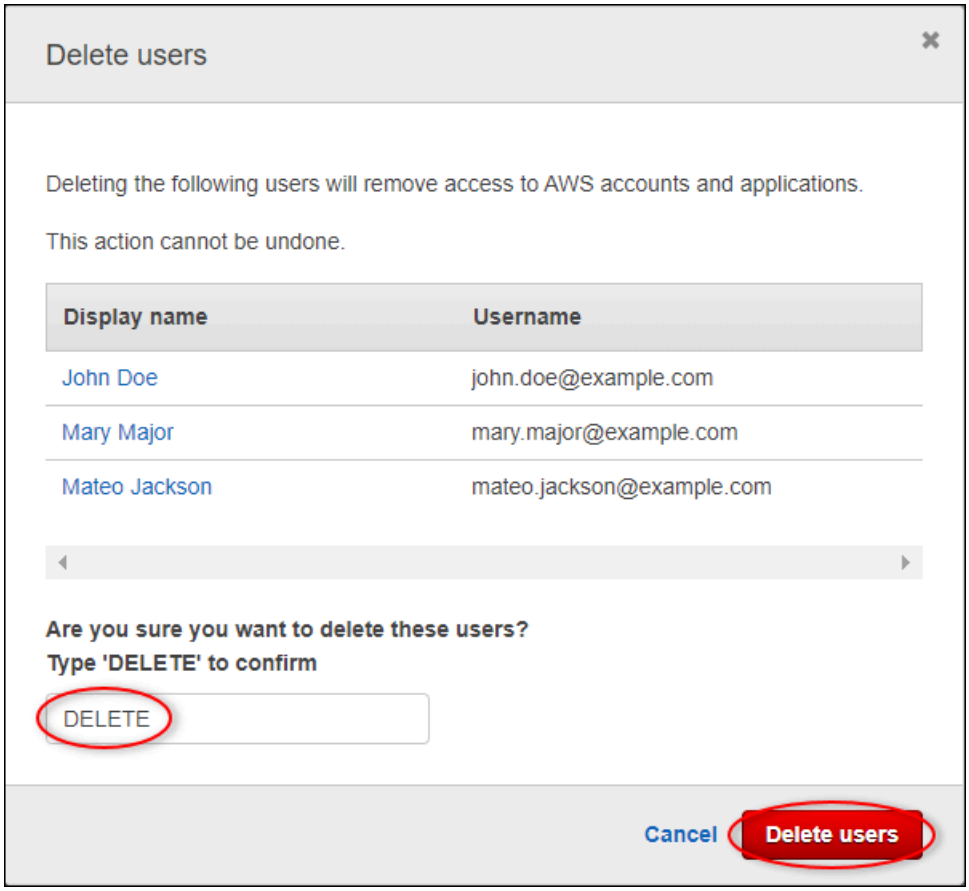


Per eliminare gli utenti di IAM Identity Center

1. Accedi alla console IAM Identity Center.
2. Nel riquadro di navigazione a sinistra, seleziona Users (Utenti).
3. Selezionare la casella di controllo per ogni utente da eliminare, quindi scegliere Delete users (Elimina utenti).



4. Nella finestra di dialogo Elimina utenti, inserisci**DELETE**, quindi scegli Elimina utenti.



Pubblicazione degli aggiornamenti dei valori delle proprietà su Amazon DynamoDB

Questo tutorial introduce un modo pratico per archiviare i dati utilizzando Amazon DynamoDB, semplificando l'accesso ai dati storici degli asset senza dover interrogare ripetutamente l'API. AWS IoT SiteWise Dopo aver completato questo tutorial, puoi creare un software personalizzato che utilizza i dati degli asset, ad esempio una mappa in tempo reale della velocità e della direzione del vento su un intero parco eolico. Se desideri monitorare e visualizzare i tuoi dati senza implementare una soluzione software personalizzata, consulta. Monitoraggio dei dati con AWS IoT SiteWise Monitor

In questo tutorial, ti baserai sulla AWS IoT SiteWise demo che fornisce un set di dati di esempio per un parco eolico. Puoi configurare gli aggiornamenti dei valori delle proprietà dalla demo del parco eolico per inviare dati, tramite le regole AWS IoT Core, a una tabella DynamoDB che crei. Quando abiliti gli aggiornamenti dei valori delle proprietà, AWS IoT SiteWise invia i dati AWS IoT Core nei messaggi MQTT. Quindi, definisci le regole di AWS IoT base che eseguono azioni, come l'azione DynamoDB, a seconda del contenuto di tali messaggi. Per ulteriori informazioni, consulta Interazione con altri servizi AWS.

Argomenti

Prerequisiti

Per completare questo tutorial, è necessario quanto segue:

- Un AWS account. Se non lo hai, consultare Configurare un Account AWS.

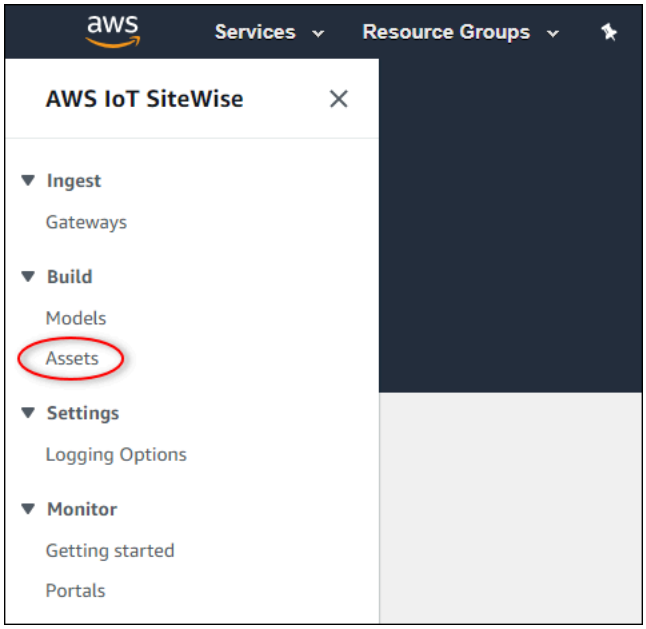
- Un computer di sviluppo che esegue Windows, macOS, Linux o Unix per accedere a. AWS Management Console Per ulteriori informazioni, consulta Nozioni di base su AWS Management Console.
- Un utente IAM con autorizzazioni da amministratore.
- Una demo di un parco AWS IoT SiteWise eolico funzionante. Quando configuri la demo, definisce i modelli e gli asset AWS IoT SiteWise e trasmette loro i dati per rappresentare un parco eolico. Per ulteriori informazioni, consulta Utilizzo della AWS IoT SiteWise demo.

Fase 1: Configurazione AWS IoT SiteWise per la pubblicazione degli aggiornamenti dei valori delle proprietà

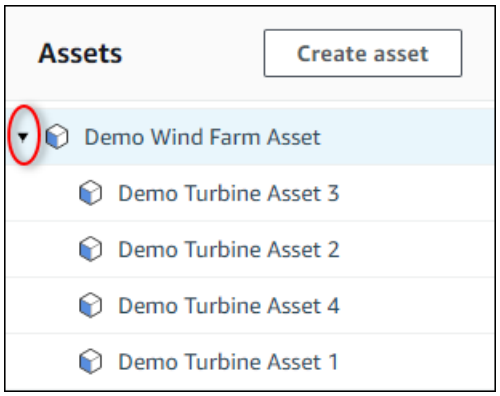
In questa procedura, è possibile abilitare le notifiche del valore della proprietà per le proprietà Wind Speed degli asset turbine della demo. Dopo aver abilitato le notifiche sui valori delle proprietà, AWS IoT SiteWise pubblica ogni aggiornamento dei valori in un messaggio MQTT su AWS IoT Core.

Per abilitare le notifiche di aggiornamento del valore della proprietà sulle proprietà degli asset

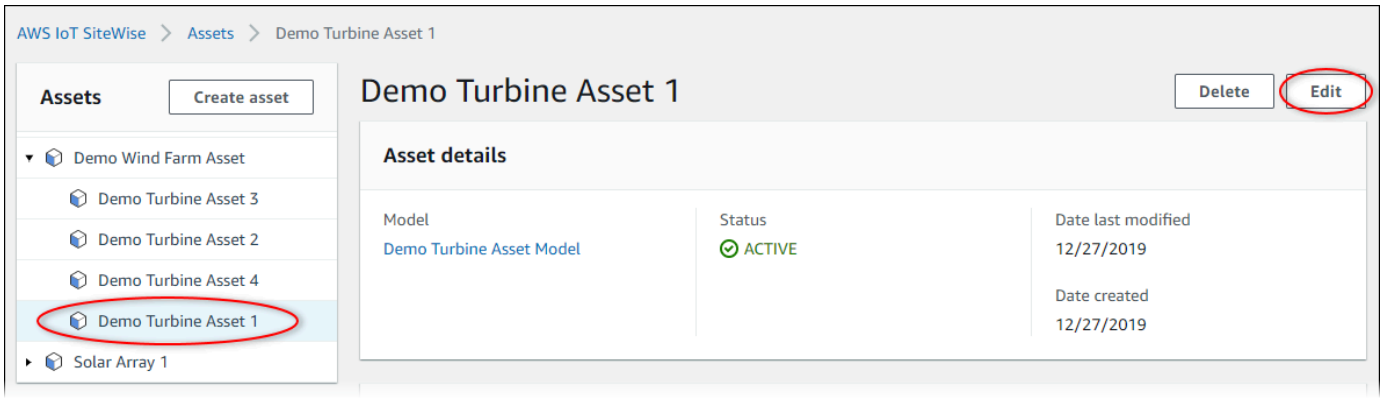
1. Accedi alla console AWS IoT SiteWise.
2. Controlla gli AWS IoT SiteWise endpoint e le quote dove AWS IoT SiteWise è supportato e cambia AWS regione, se necessario. Passa a una regione in cui stai eseguendo la AWS IoT SiteWise demo.
3. Nel riquadro di navigazione a sinistra, scegli Asset.



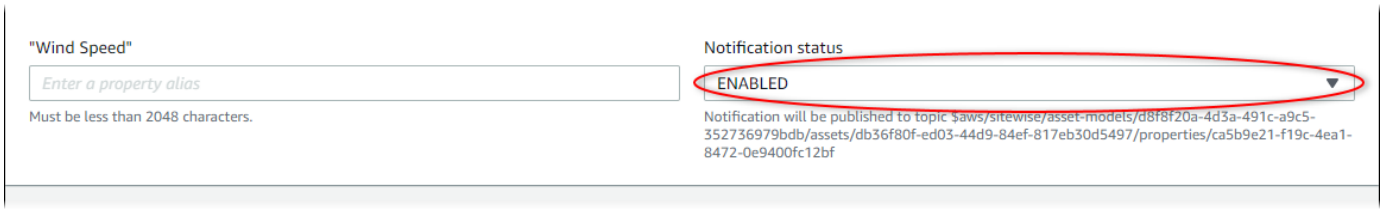
4. Scegliere la freccia accanto a Demo Wind Farm Asset per espandere la gerarchia dell'asset della centrale eolica.



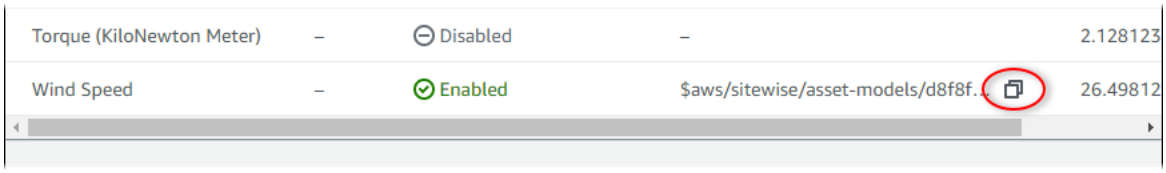
5. Scegli una turbina demo e seleziona Modifica.



6. Aggiorna lo stato di notifica della Wind Speedproprietà su ENABLED.



7. Scegli Salva risorsa nella parte inferiore della pagina.
8. Ripetere i passaggi da 5 a 7 per ogni risorsa della turbina demo.
9. Scegliere una turbina demo (ad esempio, Demo Turbine Asset 1).
10. Scegliere Measurements (Misurazioni).
11. Scegliere l'icona di copia accanto alla proprietà Wind Speed per copiare l'argomento di notifica negli Appunti. Salvare l'argomento di notifica da utilizzare più avanti in questo tutorial. È sufficiente registrare l'argomento di notifica da una turbina.



L'argomento di notifica dovrebbe essere simile all'esempio seguente.

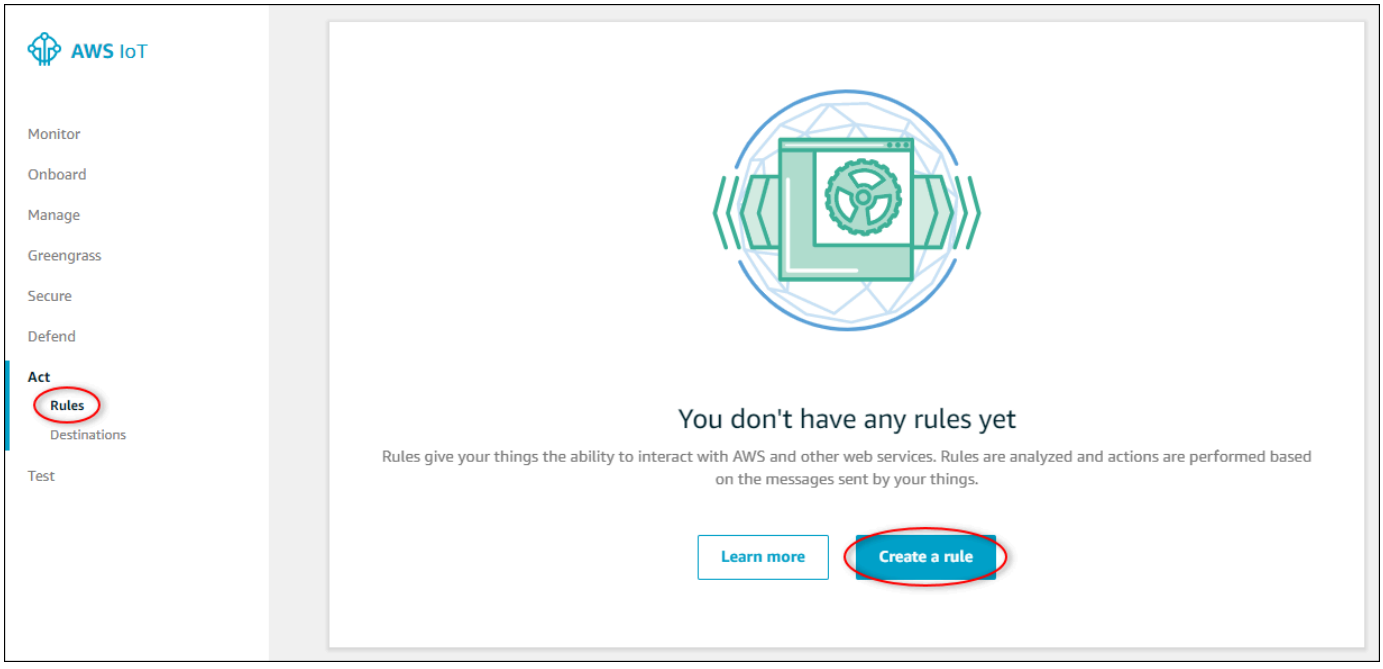
```
$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/
assets/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE/properties/a1b2c3d4-5678-90ab-
cdef-33333EXAMPLE
```

Passaggio 2: crea una regola in Core AWS IoT

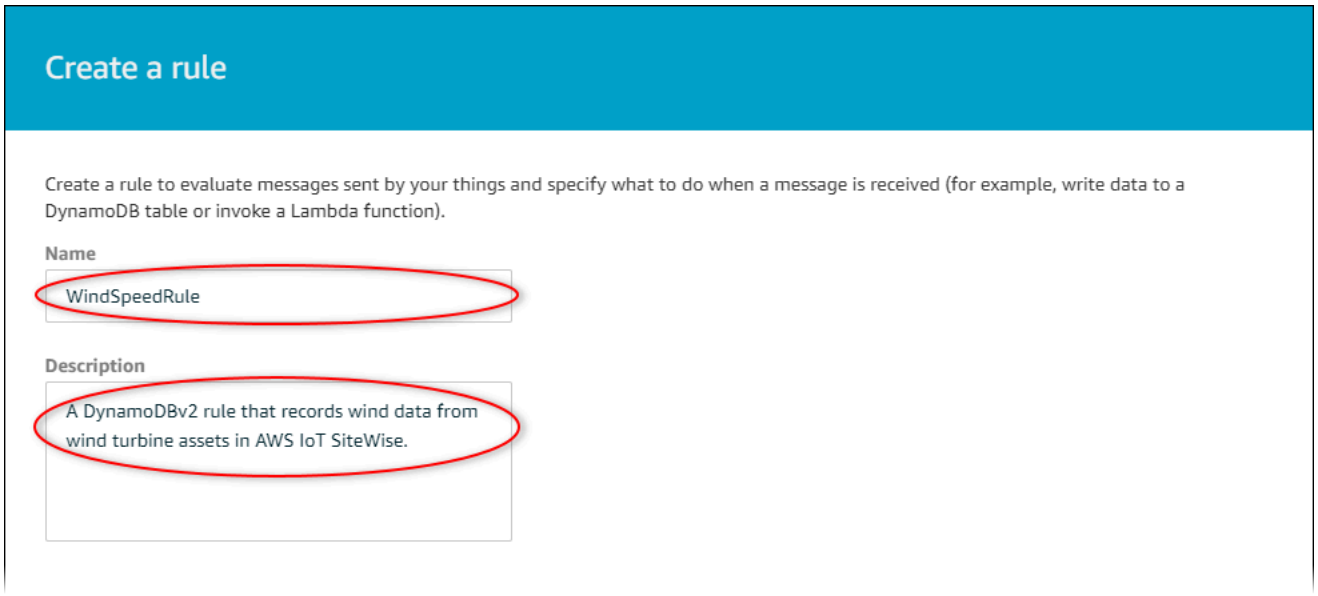
In questa procedura, crei una regola in AWS IoT Core che analizza i messaggi di notifica del valore della proprietà e inserisce i dati in una tabella Amazon DynamoDB. AWS IoT Le regole di base analizzano i messaggi MQTT ed eseguono azioni in base al contenuto e all'argomento di ciascun messaggio. Quindi, crei una regola con un'azione DynamoDB per inserire dati in una tabella DynamoDB che crei come parte di questo tutorial.

Per creare una regola con un'azione DynamoDB

1. Passare alla console AWS IoT. Se viene visualizzato il pulsante Get started (Inizia), sceglierlo.
2. Nel riquadro di navigazione sinistro scegliere Atti e quindi Regole.



3. Se viene visualizzata la finestra di dialogoYou don’t have any rules yet (Non hai ancora regole), selezionare Create a rule (Crea una regola). In caso contrario, scegliere Create (Crea).
4. Inserire un nome e una descrizione per la regola.



5. Individuare l'argomento di notifica salvato in precedenza in questo tutorial.

```
$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/
assets/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE/properties/a1b2c3d4-5678-90ab-
cdef-33333EXAMPLE
```

   Sostituisci l'ID della risorsa (l'ID dopo`assets/`) nell'argomento con un`+`. Questo seleziona la proprietà della velocità del vento per tutte le turbine eoliche dimostrative. Il filtro dell’argomento `+` accetta tutti i nodi da un singolo livello in un argomento. L'argomento dovrebbe essere simile all'esempio seguente.

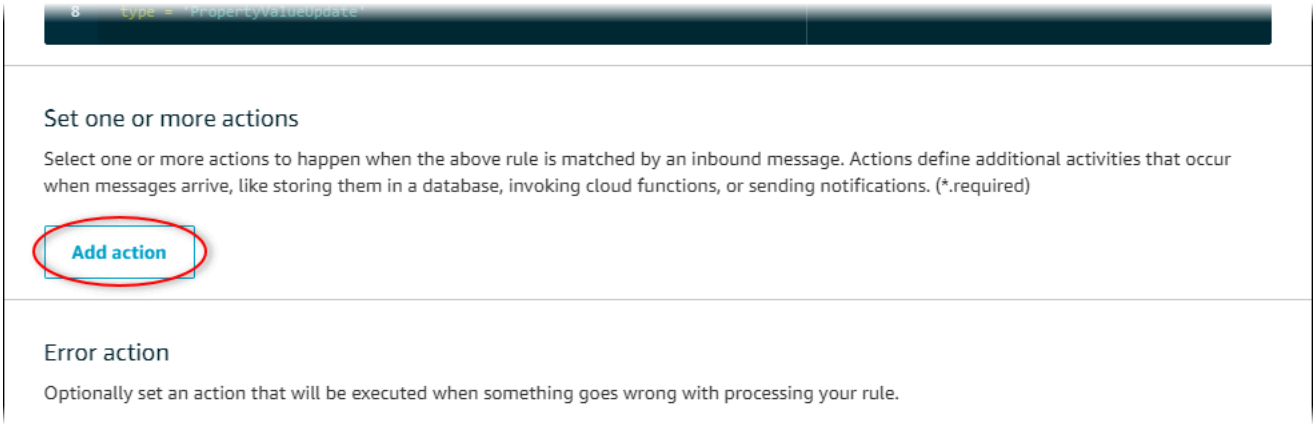
```
$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/assets/+/
properties/a1b2c3d4-5678-90ab-cdef-33333EXAMPLE
```

6. Immettere la seguente istruzione di query per la regola. Sostituire l'argomento nella sezione `FROM` con l'argomento di notifica.

```
SELECT
  payload.assetId AS asset,
  (SELECT VALUE (value.doubleValue) FROM payload.values) AS windspeed,
  timestamp() AS timestamp
FROM
```

```
  '$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/assets/+/
properties/a1b2c3d4-5678-90ab-cdef-33333EXAMPLE'
WHERE
  type = 'PropertyValueUpdate'
```

7. In Set one or more actions (Imposta una o più operazioni), scegliere Add action (Aggiungi operazione).



8. Nella pagina Seleziona un'azione, scegli Dividi messaggio in più colonne di una tabella DynamoDB (DynamoDBV2).

9. Scegliere Configura azione nella parte inferiore della pagina.
10. Nella pagina Configure action (Configura operazione), scegli Create a new resource (Crea una nuova risorsa).

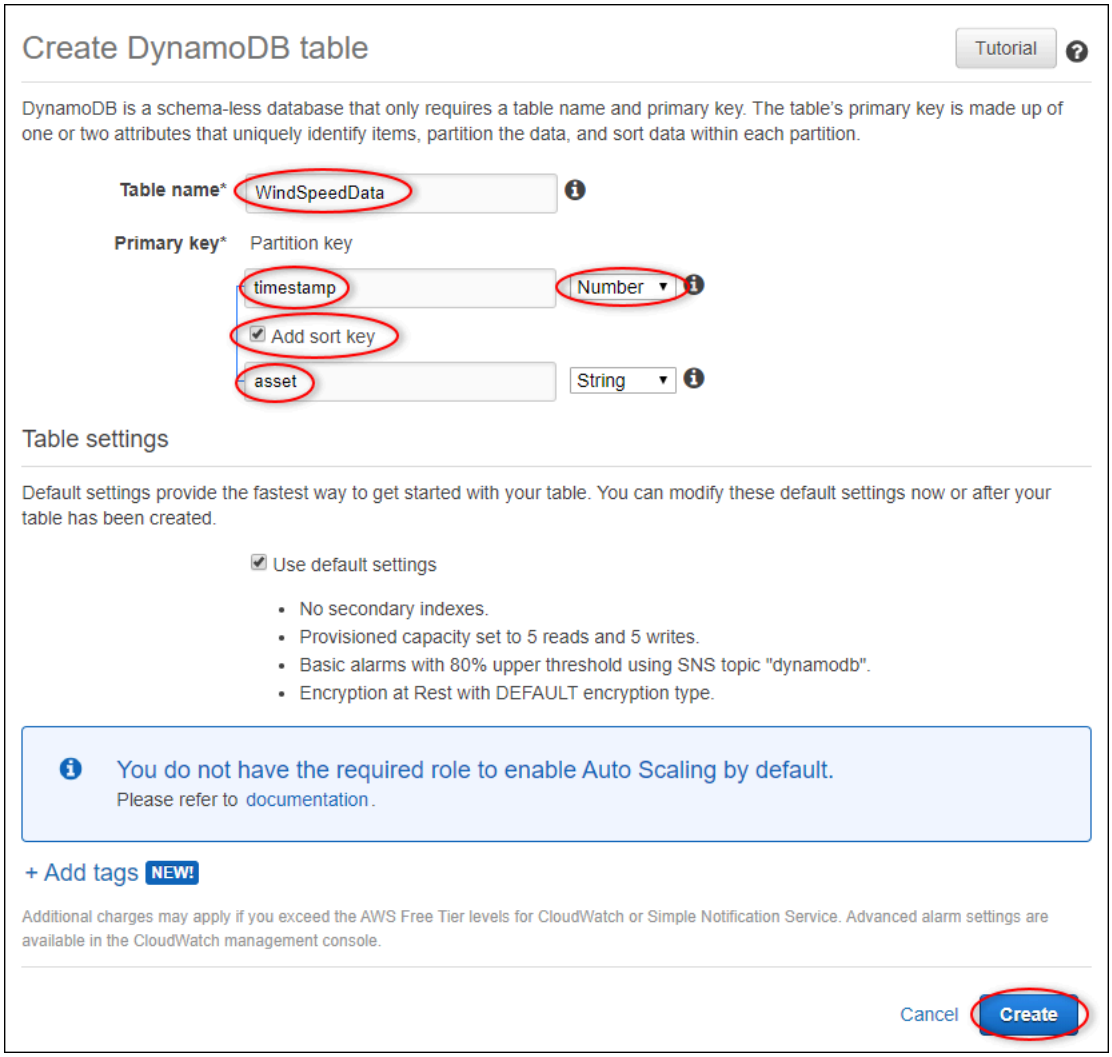
    La console DynamoDB si apre in una nuova scheda. Tenere aperta la scheda Azione regola mentre si completano le procedure riportate di seguito.

Fase 3: Creare una tabella DynamoDB

In questa procedura, crei una tabella Amazon DynamoDB per ricevere i dati sulla velocità del vento dall'azione della regola.

Per creare una tabella DynamoDB

1. Nella dashboard della console DynamoDB, scegli Crea tabella.
2. Immettere un nome per la tabella.



3. Per Chiave primaria esegui queste operazioni:
   a. Inserisci **`timestamp`** come chiave di partizione.
   b. Scegli il tipo Numero.
   c. Selezionare la casella di controlloAggiungi chiave di ordinamento).

d. Immettere **`asset`** come chiave di ordinamento e lasciare il tipo di chiave di ordinamento predefinito String.

4. Scegli Crea.

   Quando l'avviso tabella in fase di creazione scompare, la tabella è pronta.

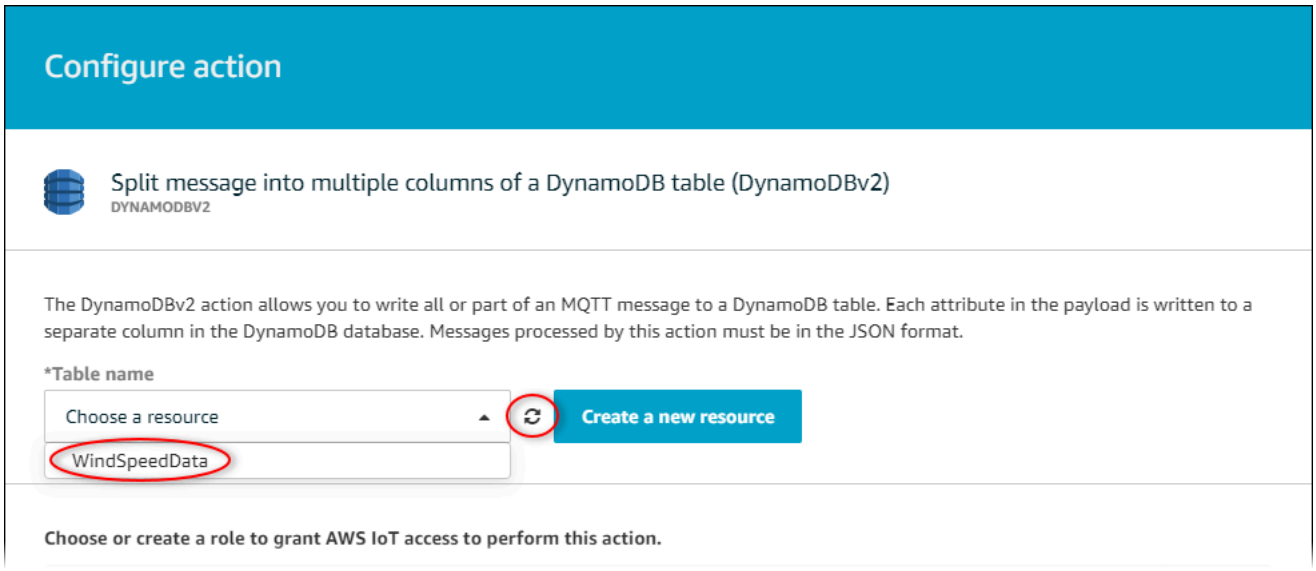
5. Tornare alla scheda con la pagina Configura azione. Tieni aperta la scheda DynamoDB mentre completi le seguenti procedure.

Fase 4: Configurare l'azione della regola DynamoDB

In questa procedura, configuri l'azione della regola di Amazon DynamoDB per inserire i dati dagli aggiornamenti dei valori delle proprietà nella tua nuova tabella DynamoDB.

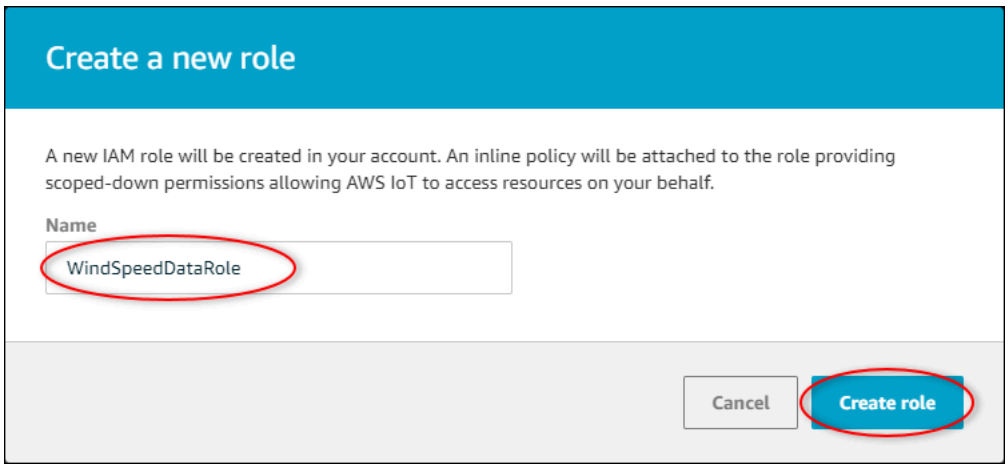
Per configurare l'azione della regola DynamoDB

1. Nella pagina Configura azione, aggiorna l'elenco dei nomi delle tabelle e scegli la nuova tabella DynamoDB.



2. Scegli Crea ruolo per creare un ruolo IAM che conceda l'accesso AWS IoT Core per eseguire l'azione della regola.

3. Fornire un nome ruolo e selezionare Crea ruolo.



4. Selezionare Add action (Aggiungi operazione).
5. Scegliere Crea regola nella parte inferiore della pagina per completare la creazione della regola.

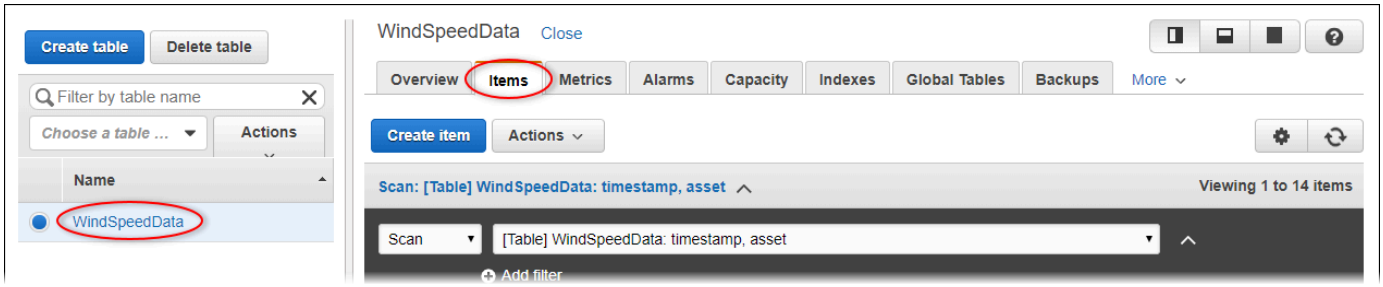
   I dati degli asset dimostrativi dovrebbero iniziare a comparire nella tabella DynamoDB.

Fase 5: Esplora i dati in DynamoDB

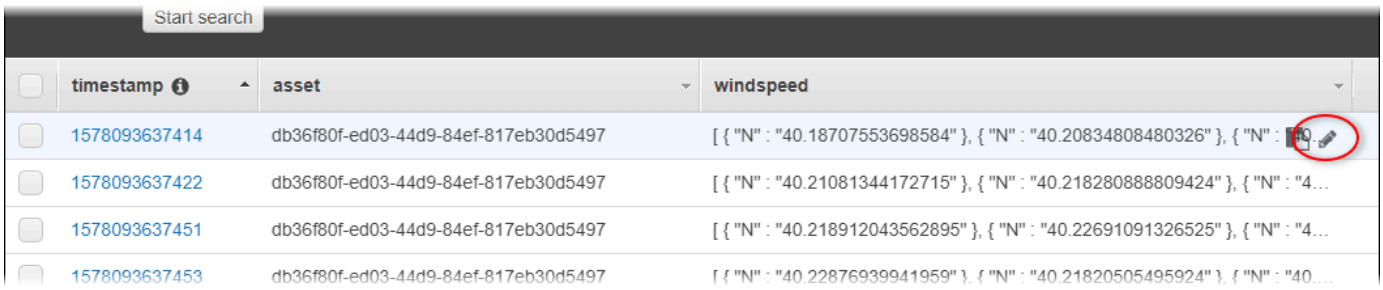
In questa procedura, esplori i dati sulla velocità del vento degli asset dimostrativi nella tua nuova tabella Amazon DynamoDB.

Per esplorare i dati degli asset in DynamoDB

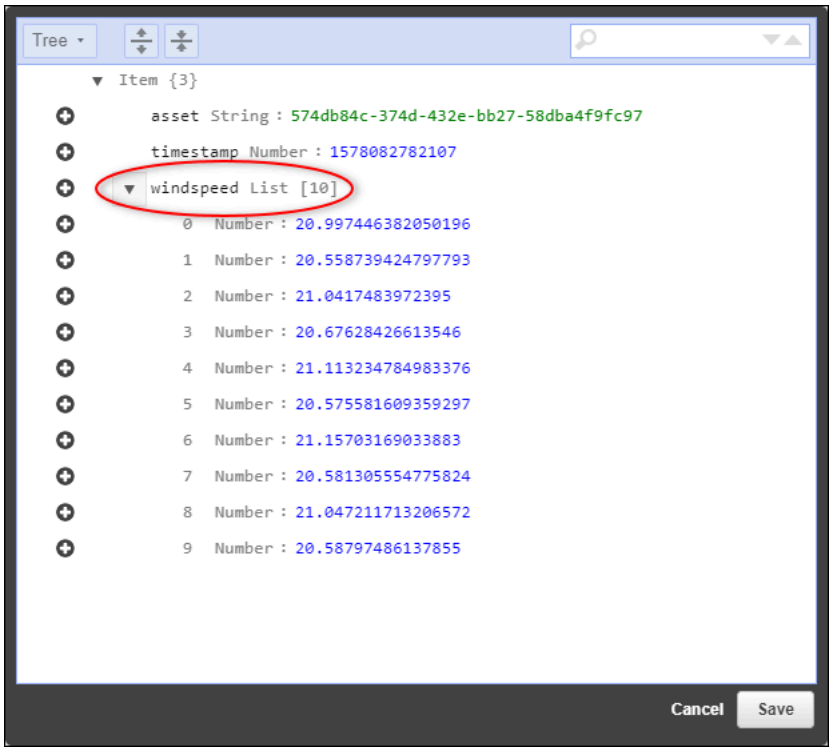
1. Tornate alla scheda con la tabella DynamoDB aperta.
2. Nella tabella creata in precedenza, scegliere la scheda Elementi per visualizzare i dati nella tabella. Aggiorna la pagina se non vedi righe nella tabella. Se le righe non vengono visualizzate dopo alcuni minuti, consulta Risoluzione dei problemi relativi a una regola.



3. In una riga nella tabella, scegliere l'icona di modifica per espandere i dati.



4. Scegliere la freccia accanto alla struttura della windspeed per espandere l'elenco dei punti dati della velocità del vento. Ogni elenco riporta una serie di punti dati sulla velocità del vento inviati AWS IoT SiteWise dalla demo del parco eolico. Se si imposta un'azione regola per uso personale, è possibile che si desideri un formato di dati diverso. Per ulteriori informazioni, consulta Esecuzione di query sui messaggi di notifica delle proprietà degli asset.



Ora che hai completato il tutorial, disabilita o elimina la regola ed elimina la tabella DynamoDB per evitare di incorrere in costi aggiuntivi. Per ripulire le risorse, consulta. Passaggio 6: Pulisci le risorse dopo il tutorial

Passaggio 6: Pulisci le risorse dopo il tutorial

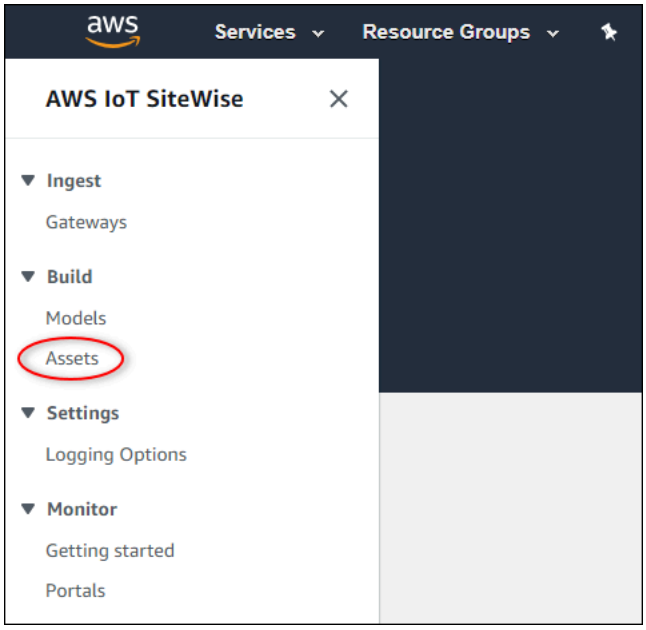
Dopo aver completato questo tutorial, puoi pulire le risorse per evitare di incorrere in costi aggiuntivi. Gli asset del parco eolico dimostrativo vengono eliminati al termine della durata scelta al momento

della creazione della demo. Puoi anche eliminare la demo manualmente. Per ulteriori informazioni, consulta Eliminazione della demo AWS IoT SiteWise.

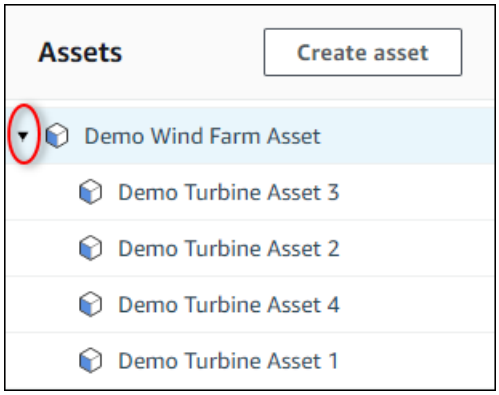
Utilizza le seguenti procedure per disabilitare le notifiche di aggiornamento dei valori delle proprietà (se non hai eliminato la demo), disabilitare o eliminare la AWS IoT regola ed eliminare la tabella DynamoDB.

Per disabilitare le notifiche di aggiornamento del valore della proprietà sulle proprietà degli asset

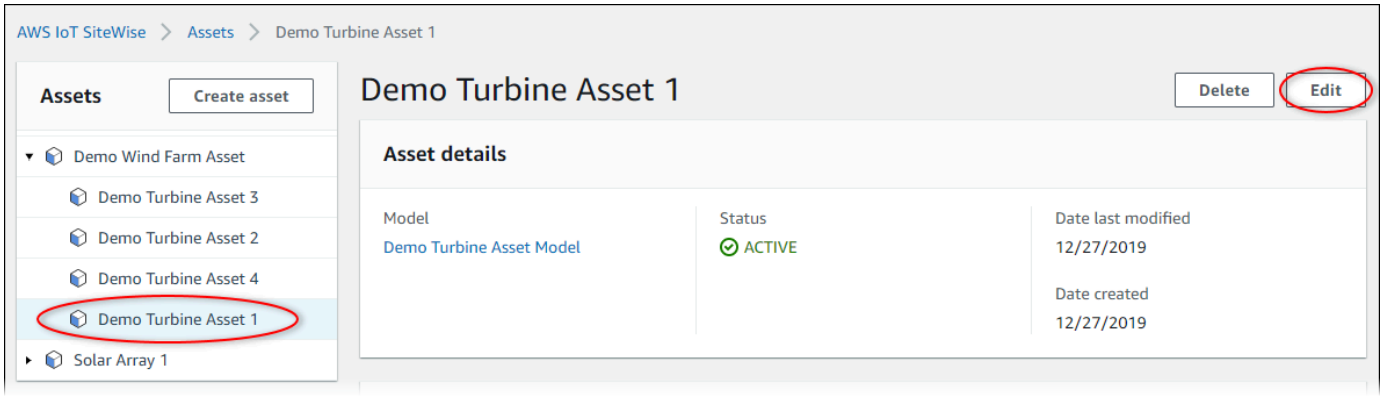
1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione a sinistra, scegli Asset.



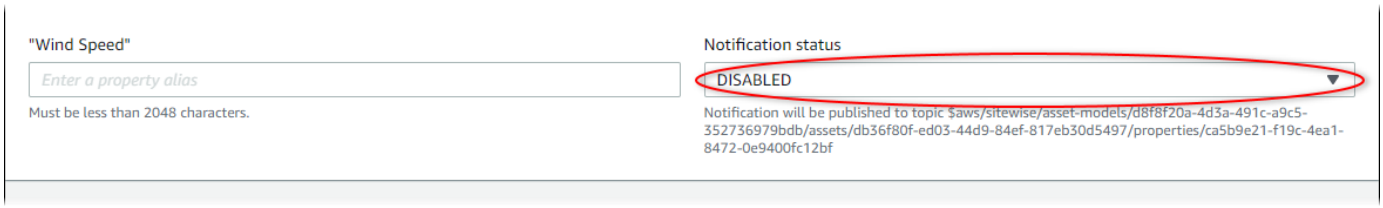
3. Scegliere la freccia accanto a Demo Wind Farm Asset per espandere la gerarchia dell'asset della centrale eolica.



4. Scegli una turbina demo e seleziona Modifica.



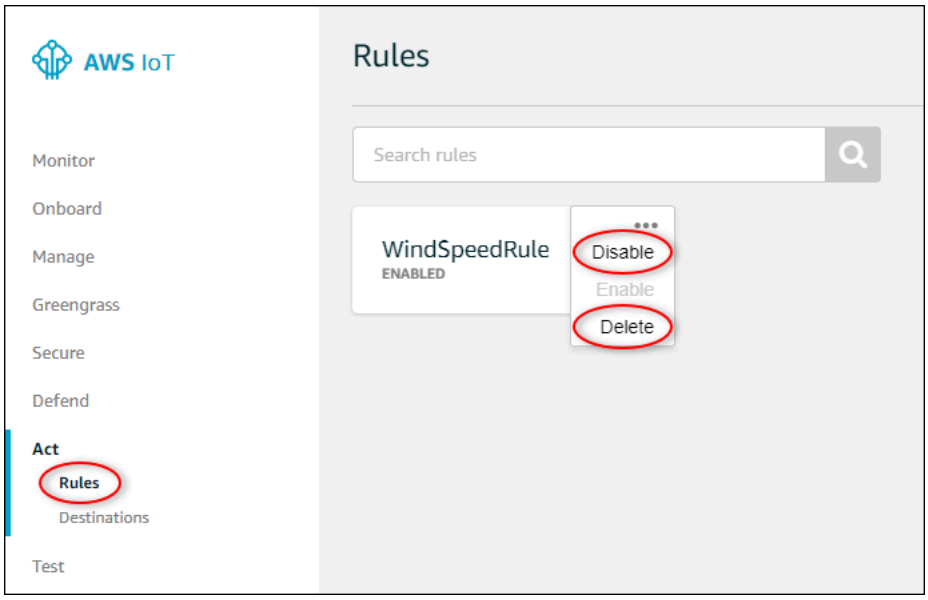
5. Aggiorna lo stato di notifica della Wind Speedproprietà su DISABILITATO.



6. Scegli Salva risorsa nella parte inferiore della pagina.
7. Ripetere i passaggi da 4 a 6 per ogni asset turbina demo.

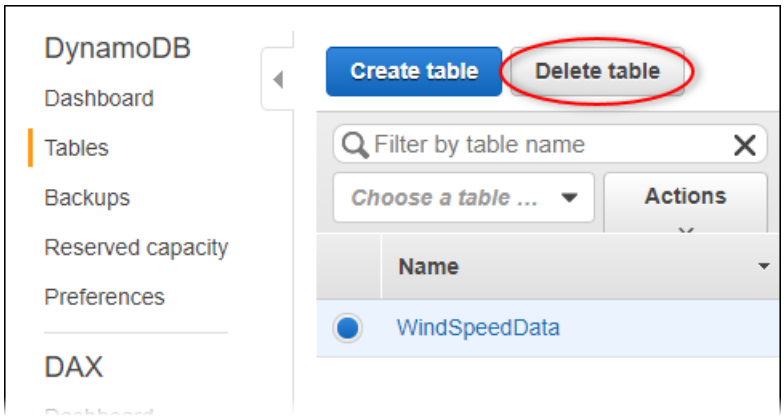
Per disabilitare o eliminare una regola in AWS IoT Core

1. Passare alla console AWS IoT.
2. Nel riquadro di navigazione sinistro scegliere Atti e quindi Regole.
3. Scegli il menu della regola e seleziona Disattiva o Elimina.

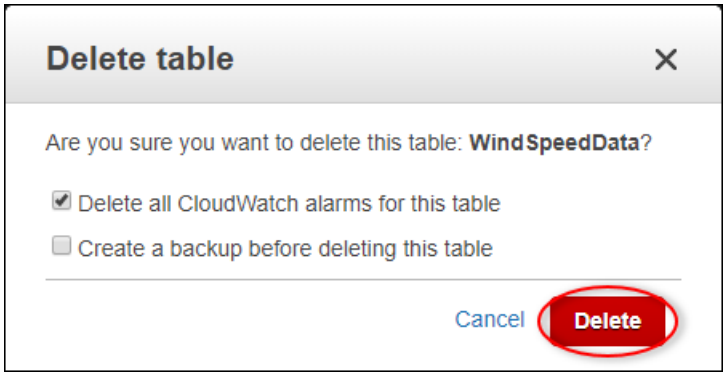


Per eliminare una tabella DynamoDB

1. Accedere alla console DynamoDB.
2. Nel riquadro di navigazione a sinistra, selezionare Tables (Tabelle).
3. Scegliere la tabella creata in precedenza WindSpeedData.
4. Seleziona Delete Table (Elimina tabella).



5. Nella finestra di dialogo Delete table (Elimina tabella) scegliere Delete (Elimina).



Inserimento di dati in AWS IoT SiteWise

AWS IoT SiteWise è progettato per raccogliere e correlare in modo efficiente i dati industriali con gli asset corrispondenti, che rappresentano vari aspetti delle operazioni industriali. Questa documentazione si concentra sugli aspetti pratici dell'acquisizione dei dati e offre diversi metodi adattati a diversi casi d'uso industriali. AWS IoT SiteWise Per le istruzioni sulla creazione di un'operazione industriale virtuale, consulta Modellazione degli asset industriali.

È possibile inviare dati industriali a AWS IoT SiteWise utilizzando una delle seguenti opzioni:

- AWS IoT SiteWise Edge: utilizza il gateway SiteWise Edge come intermediario tra AWS IoT SiteWise e i tuoi server di dati. AWS IoT SiteWise fornisce AWS IoT Greengrass componenti che è possibile implementare su qualsiasi piattaforma in grado di eseguire la configurazione AWS IoT Greengrass di un SiteWise gateway Edge. Questa opzione supporta il collegamento con il protocollo server OPC-UA.
- AWS IoT Regole principali: utilizza le regole di AWS IoT base per caricare dati dai messaggi MQTT pubblicati da un oggetto o da un AWS IoT altro servizio. AWS
- AWS IoT Events azioni: utilizza le AWS IoT Events azioni attivate da eventi specifici in. AWS IoT Events Questo metodo è adatto per scenari in cui il caricamento dei dati è legato al verificarsi di eventi.
- AWS IoT Greengrass stream manager: utilizza AWS IoT Greengrass stream manager per caricare dati da fonti di dati locali utilizzando un dispositivo edge. Questa opzione si adatta a situazioni in cui i dati provengono da postazioni locali o periferiche.
- AWS IoT SiteWise API: utilizza l'AWS IoT SiteWise API per caricare dati da qualsiasi altra fonte. Utilizza la nostra BatchPutAssetPropertyValueAPI di streaming per l'inserimento in pochi secondi o l'CreateBulkImportJobAPI orientata ai batch per facilitare l'ingestione economica in batch di grandi dimensioni.

Questi metodi offrono una gamma di soluzioni per la gestione dei dati provenienti da diverse fonti. Approfondisci i dettagli di ciascuna opzione per ottenere una comprensione completa delle funzionalità di acquisizione dei dati offerte. AWS IoT SiteWise

Gestione dei flussi di dati

Prima di iniziare a creare modelli di asset e asset AWS IoT SiteWise, iniziate configurando le fonti di dati per inviare informazioni direttamente dalle apparecchiature industriali alla piattaforma. AWS

IoT SiteWise è progettato per generare automaticamente flussi di dati che raccolgono i dati grezzi. Ciascuno dei flussi di dati è identificato da un alias univoco, che semplifica la registrazione dell'origine di ogni dato.

Ad esempio, si consideri un parco eolico che utilizza un gateway AWS IoT SiteWise Edge per inviare dati sulla temperatura dell'aria, sulla velocità di rotazione dell'elica e sulle serie temporali di potenza in uscita da un server OPC-UA a. AWS IoT SiteWise L'alias del flusso di `server1-windfarm/3/turbine/7/temperature` dati identifica i valori di temperatura provenienti dalla turbina #7 del parco eolico #3. `server1`è il nome della fonte di dati OPC-UA. Il `server1` prefisso viene utilizzato per tutti i flussi di dati provenienti da questo server e aiuta a organizzare i dati in base alla fonte.

Dopo aver creato i modelli e gli asset degli asset, organizzate il flusso di dati associando ogni flusso di dati a proprietà specifiche degli asset. Questa associazione AWS IoT SiteWise consente non solo di raccogliere, ma anche di elaborare i dati in base alla struttura delle risorse. Se necessario, potete anche rimuovere il collegamento tra i flussi di dati e le proprietà degli asset.

Attualmente, è possibile associare solo i flussi di dati alle misurazioni. Le misurazioni sono un tipo di proprietà degli asset che rappresentano i flussi di dati grezzi dei sensori dei dispositivi, come i valori di temperatura con data e ora o i valori di rotazione al minuto (RPM).

Quando queste misurazioni definiscono metriche o trasformazioni, i dati in entrata attivano calcoli specifici. È importante notare che una proprietà di un asset può essere collegata solo a un flusso di dati alla volta.

> **Note**
>
> Una proprietà di un asset non può essere associata a più flussi di dati contemporaneamente.

AWS IoT SiteWise utilizza `TimeSeries` la risorsa Amazon Resource Name (ARN) per determinare i costi di storage. Per ulteriori informazioni, consulta la sezione Prezzi di AWS IoT SiteWise.

Le seguenti sezioni mostrano come utilizzare la AWS IoT SiteWise console o l'API per gestire i flussi di dati.

Argomenti

- Gestione dei flussi di dati

Gestione dei flussi di dati

Per iniziare a gestire i flussi di dati, completa quanto segue.

> **Note**
>
> Se sei alle prime armi AWS IoT SiteWise dopo il 24 novembre 2021, puoi saltare questa sezione. I clienti che hanno iniziato a utilizzarlo AWS IoT SiteWise prima di questa data devono configurare le impostazioni del servizio AWS IoT SiteWise per consentire l'acquisizione di dati senza modelli e risorse.

- Assicurati che il tuo ruolo IAM disponga delle autorizzazioni mostrate nell'esempio seguente.

  Example Politica per gli utenti di IAM

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PutAssetPropertyValuesAssetPropertyOnly",
            "Effect": "Allow",
            "Action": "iotsitewise:BatchPutAssetPropertyValue",
            "Resource": "arn:aws:iotsitewise:*:*:asset/*"
        },
        {
            "Sid": "PutAssetPropertyValuesPropertyAliasAllowed",
            "Effect": "Allow",
            "Action": "iotsitewise:BatchPutAssetPropertyValue",
            "Resource": "arn:aws:iotsitewise:*:*:time-series/*"
        }
    ]
}
```

> **Important**
>
> Prima di inserire dati in un flusso di dati, procedi come segue.
>
> - La `time-series` risorsa deve essere autorizzata se si utilizza un alias di proprietà per identificare il flusso di dati.

- La `asset` risorsa deve essere autorizzata se utilizzate un ID di risorsa per identificare la risorsa che contiene la proprietà della risorsa associata.

Per ulteriori informazioni sulla configurazione delle policy IAM, consulta Managing IAM policies nella IAM User Guide.

- Configura le impostazioni di inserimento dei dati AWS IoT SiteWise per consentire l'accettazione di flussi di dati non associati alle proprietà degli asset.

Argomenti

- Configurazione delle impostazioni di inserimento dei dati
- Gestione dei flussi di dati

Configurazione delle impostazioni di inserimento dei dati

Console

Configura AWS IoT SiteWise per accettare flussi di dati non associati alle proprietà delle risorse utilizzando la console. AWS IoT SiteWise

Per configurare le impostazioni di acquisizione dei dati (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, in Impostazioni, scegli Inserimento dati.
3. Nella pagina di ingestione dei dati, scegli Modifica.
4. Nella sezione Inserimento di dati non associati, scegli Abilita l'inserimento di dati per flussi di dati non associati alle proprietà delle risorse.

   Important

   Dopo aver configurato AWS IoT SiteWise per accettare flussi di dati non associati alle proprietà delle risorse, non puoi disattivare questa impostazione.

5. Selezionare Salva.

6. In Abilita l'inserimento di dati disassociati, scegliete Aggiorna. Lo stato per l'inserimento di dati non associati diventa Attivo. Il completamento di questo processo può richiedere alcuni minuti.

AWS CLI

Configura AWS IoT SiteWise per accettare flussi di dati non associati alle proprietà degli asset utilizzando l'operazione PutStorageConfigurationAPI. La sezione seguente utilizza il. AWS CLI

Per configurare le impostazioni di acquisizione dei dati ()AWS CLI

1. AWS IoT SiteWise Per configurare la ricezione di flussi di dati non associati alle proprietà degli asset, eseguite il comando seguente.

> **Important**
>
> Dopo aver configurato AWS IoT SiteWise per accettare flussi di dati non associati alle proprietà delle risorse, non puoi disattivare questa impostazione.

```
aws iotsitewise put-storage-configuration \
                                -\-storage-type SITEWISE_DEFAULT_STORAGE \
                                -\-disassociated-data-storage ENABLED
```

Puoi configurare il`storageType`. `MULTI_LAYER_STORAGE` Per ulteriori informazioni, consulta Gestione dell'archiviazione dei dati.

Example response

```
{
            "storageType": "SITEWISE_DEFAULT_STORAGE",
            "disassociatedDataStorage": "ENABLED",
            "configurationStatus": {
                "state": "UPDATE_IN_PROGRESS"
            }
        }
```

Il completamento di questo processo può richiedere alcuni minuti.

2. Per recuperare le informazioni sulla configurazione dello storage, esegui il comando seguente.

```
aws iotsitewise describe-storage-configuration
```

Example response

```
{
            "storageType": "SITEWISE_DEFAULT_STORAGE",
            "disassociatedDataStorage": "ENABLED",
            "configurationStatus": {
                "state": "ACTIVE"
            },
            "lastUpdateDate": "2021-11-16T15:54:14-07:00"
        }
```

Gestione dei flussi di dati

Gestisci i tuoi flussi di dati utilizzando o. Console AWS IoT SiteWise AWS CLI

Console

Usa la AWS IoT SiteWise console per gestire i tuoi flussi di dati.

Per gestire i flussi di dati (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Flussi di dati.
3. (Facoltativo) Per aggiungere o aggiornare i tag, seleziona il flusso di dati da modificare, quindi scegli Gestisci tag.

   Nella pagina Modifica tag, scegli Aggiungi tag. Nel campo Chiave, digita il nome del tag da usare.

   Selezionare Salva.
4. (Facoltativo) Nella tabella Flusso di dati, puoi filtrare i flussi di dati nei seguenti modi.

   - Nel primo menu a discesa, seleziona Prefisso Alias o Asset ID.

- Prefisso alias: il prefisso alias del flusso di dati. Puoi scegliere questa opzione se i tuoi flussi di dati di destinazione hanno un prefisso alias.
- ID risorsa: l'ID della risorsa in cui è stata creata la proprietà dell'asset. Potete scegliere questa opzione se i flussi di dati di destinazione sono associati a una proprietà dell'asset.

- Nel secondo menu a discesa, seleziona Tutti i flussi di dati, Flussi di dati associati o Flussi di dati non associati.
  - Tutti i flussi di dati: flussi di dati associati o non associati a una proprietà di un asset.
  - Flussi di dati associati: flussi di dati associati a una proprietà di un asset.
  - Flussi di dati non associati: flussi di dati non associati a una proprietà di un asset.

5. Seleziona i flussi di dati che stai gestendo. AWS IoT SiteWise visualizza i flussi di dati che hai scelto in un grafico nella parte inferiore della pagina. Se ne selezioni più di 10, il grafico mostrerà solo i primi 10.
6. (Facoltativo) Configurate il grafico nei seguenti modi.

   a. Per la funzione di aggregazione, selezionate una delle seguenti opzioni.

      - Conteggio dei punti dati: il numero totale di punti dati per le variabili specificate nell'intervallo di tempo corrente.
      - Media: la media dei valori delle variabili specificate nell'intervallo di tempo corrente.
      - Somma: la somma dei valori delle variabili specificate nell'intervallo di tempo corrente.
      - Minimo: il minimo dei valori delle variabili specificate nell'intervallo di tempo corrente.
      - Massimo: il massimo dei valori delle variabili specificate nell'intervallo di tempo corrente.

      Per ulteriori informazioni, consulta Utilizzo delle funzioni di aggregazione nelle espressioni di formule.

   b. Per Intervalli di tempo, selezionare una delle seguenti opzioni.

      - Ultima ora: il grafico mostra i dati aggregati dell'ultima ora.
      - Ultime 2 ore: il grafico mostra i dati aggregati delle ultime due ore.
      - Ultime 3 ore: il grafico mostra i dati aggregati delle ultime tre ore.
      - Ultime 4 ore: il grafico mostra i dati aggregati delle ultime quattro ore.

   c. Per Intervallo di tempo, seleziona una delle seguenti opzioni.

- 1 minuto: aggrega i dati ogni minuto nell'intervallo di tempo specificato.
- 1 ora: aggrega i dati ogni ora nell'intervallo di tempo specificato.

7. Scegli Gestisci flussi di dati.
8. Nella sezione Aggiorna le associazioni dei flussi di dati, nella colonna Nome della misurazione, esegui una delle seguenti operazioni.
   - Se il flusso di dati è associato a una misurazione, elimina l'associazione scegliendo l'icona di chiusura.
   - Se il flusso di dati non è associato a una misurazione, scegli Scegli misurazione.
9. Nella tabella Scegli una misurazione, accedi alla risorsa di destinazione, quindi scegli la misurazione che stai associando.
10. (Facoltativo) Nella sezione Aggiorna gli alias delle proprietà degli asset, inserite un alias univoco per ogni misurazione.
11. Scegli Aggiorna.

La colonna Status può visualizzare uno dei seguenti valori.

- In sospeso: stai aggiornando l'associazione del flusso di dati o l'alias della proprietà dell'asset.
- Invia: la modifica all'alias dell'associazione o della proprietà della risorsa viene salvata.
- Errore: AWS IoT SiteWise impossibile elaborare la richiesta di aggiornamento dell'associazione del flusso di dati o dell'alias per la misurazione.
- Operazione riuscita: hai aggiornato correttamente l'associazione del flusso di dati o l'alias per la misurazione.

AWS CLI

Utilizza le seguenti operazioni API per gestire i flussi di dati. Gli esempi di codice utilizzano il. AWS CLI

- AssociateTimeSeriesToAssetProperty— Associa un flusso di dati (serie temporali) a una proprietà di asset.
- DisassociateTimeSeriesFromAssetProperty— Dissocia un flusso di dati dalla proprietà di un asset.
- DeleteTimeSeries— Elimina un flusso di dati.

- DescribeTimeSeries— Recupera informazioni su un flusso di dati.
- ListTimeSeries— Recupera un elenco impaginato di flussi di dati.

AssociateTimeSeriesToAssetProperty

Per associare un flusso di dati a una proprietà dell'asset, esegui il comando seguente.

> **Important**
>
> La proprietà dell'asset specificata non deve essere attualmente associata a nessun flusso di dati.

- Sostituisci *data-stream-alias* con l'alias del flusso di dati che stai associando.
- Sostituisci *Asset-ID* con l'ID della risorsa in cui è stata creata la proprietà dell'asset.
- Sostituisci *property-ID* con l'ID della proprietà dell'asset.

```
aws iotsitewise associate-time-series-to-asset-property \
                        --alias data-stream-alias \
                        --assetId asset-ID \
                        --propertyId property-ID
```

DisassociateTimeSeriesFromAssetProperty

Per dissociare un flusso di dati da una proprietà dell'asset, esegui il comando seguente.

- Sostituiscilo *data-stream-alias* con l'alias del flusso di dati che stai dissociando.
- Sostituisci *Asset-ID* con l'ID della risorsa in cui è stata creata la proprietà dell'asset.
- Sostituisci *property-ID* con l'ID della proprietà dell'asset.

```
aws iotsitewise disassociate-time-series-from-asset-property \
                        --alias data-stream-alias \
                        --assetId asset-ID \
                        --propertyId property-ID
```

DeleteTimeSeries

Per eliminare un flusso di dati, esegui il comando seguente.

Sostituiscilo *data-stream-alias*con l'alias del flusso di dati che stai eliminando.

```
aws iotsitewise delete-time-series --alias data-stream-alias
```

Per identificare un flusso di dati, esegui una delle seguenti operazioni:

- Se il flusso di dati non è associato a una proprietà della risorsa, specificate la proprietà `alias` del flusso di dati.
- Se il flusso di dati è associato a una proprietà della risorsa, specificate una delle seguenti opzioni:
  - Il flusso `alias` di dati.
  - La `assetId` e `propertyId` che identifica la proprietà dell'asset.

DescribeTimeSeries

Utilizza l'operazione `DescribeTimeSeries` API per verificare se hai associato o dissociato correttamente un flusso di dati.

Per recuperare informazioni su un flusso di dati, esegui il comando seguente.

```
aws iotsitewise describe-time-series --alias data-stream-alias
```

Per identificare un flusso di dati, effettuate una delle seguenti operazioni:

- Se il flusso di dati non è associato a una proprietà della risorsa, specificate la proprietà `alias` del flusso di dati.
- Se il flusso di dati è associato a una proprietà della risorsa, specificate una delle seguenti opzioni:
  - Il flusso `alias` di dati.
  - La `assetId` e `propertyId` che identifica la proprietà dell'asset.

ListTimeSeries

Utilizza l'operazione `ListTimeSeries` API per verificare se hai eliminato correttamente un flusso di dati.

Per recuperare un elenco impaginato di flussi di dati, esegui il comando seguente.

```
aws iotsitewise list-time-series
```

Acquisizione di dati tramite regole AWS IoT Core

Invia dati AWS IoT SiteWise a AWS IoT oggetti e altri AWS servizi utilizzando le regole in AWS IoT Core. Le regole trasformano i messaggi MQTT ed eseguono azioni per interagire con AWS i servizi. L'azione della AWS IoT SiteWise regola inoltra i dati dei messaggi all'BatchPutAssetPropertyValueoperazione dall' AWS IoT SiteWise API. Per ulteriori informazioni, consulta Regole e AWS IoT SiteWise azioni nella Guida per gli AWS IoT sviluppatori.

Per seguire un tutorial che illustra i passaggi necessari per configurare una regola che inserisce i dati attraverso le ombre dei dispositivi, consulta. Acquisizione di dati dagli oggetti AWS IoT

Puoi anche inviare dati da altri AWS IoT SiteWise AWS servizi. Per ulteriori informazioni, consulta Interazione con altri servizi AWS.

Argomenti

- Concessione AWS IoT dell'accesso richiesto
- Configurazione dell'azione della AWS IoT SiteWise regola
- Riduzione dei costi con Basic Ingest

Concessione AWS IoT dell'accesso richiesto

Utilizzi i ruoli IAM per controllare le AWS risorse a cui ogni regola ha accesso. Prima di creare una regola, devi creare un ruolo IAM con una policy che consenta alla regola di eseguire azioni sulla AWS risorsa richiesta. AWS IoT assume questo ruolo quando esegue una regola.

Se create l'azione della regola nella AWS IoT console, potete scegliere una risorsa principale per creare un ruolo che abbia accesso a una gerarchia di risorse selezionata. Per ulteriori informazioni su come definire manualmente un ruolo per una regola, consulta Concessione AWS IoT delle autorizzazioni di accesso richieste e Pass role nella Developer Guide.AWS IoT

Per l'azione della AWS IoT SiteWise regola, è necessario definire un ruolo che consenta `iotsitewise:BatchPutAssetPropertyValue` l'accesso alle proprietà degli asset a cui la regola

invia i dati. Per migliorare la sicurezza, è possibile specificare un percorso di gerarchia AWS IoT SiteWise degli asset nella `Condition` proprietà.

La policy di attendibilità di esempio riportata di seguito consente l'accesso a un asset specifico e ai relativi asset figlio.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iotsitewise:BatchPutAssetPropertyValue",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "iotsitewise:assetHierarchyPath": [
            "/root node asset ID",
            "/root node asset ID/*"
          ]
        }
      }
    }
  ]
}
```

Rimuovilo `Condition` dalla policy per consentire l'accesso a tutte le tue risorse. La policy di attendibilità di esempio riportata di seguito consente l'accesso a tutti gli asset nella regione corrente.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iotsitewise:BatchPutAssetPropertyValue",
      "Resource": "*"
    }
  ]
}
```

Configurazione dell'azione della AWS IoT SiteWise regola

L'azione della AWS IoT SiteWise regola invia i dati dal messaggio MQTT che ha avviato la regola alle proprietà dell'asset in. AWS IoT SiteWiseÈ possibile caricare più immissioni di dati in diverse proprietà degli asset contemporaneamente, per inviare aggiornamenti per tutti i sensori di un dispositivo in un unico messaggio. Inoltre puoi caricare più punti dati contemporaneamente per ogni inserimento di dati.

> **Note**
>
> Quando invii dati a AWS IoT SiteWise con l'azione della regola, i dati devono soddisfare tutti i requisiti dell'`BatchPutAssetPropertyValue`operazione. Ad esempio, i dati non possono avere un timestamp precedente a 7 giorni dall'epoca Unix corrente. Per ulteriori informazioni, consulta Inserimento di dati con l'API AWS IoT SiteWise.

Per ogni inserimento di dati nell'azione di regola, puoi identificare una proprietà dell'asset e specificare il timestamp, la qualità e il valore di ciascun punto dati per la proprietà dell'asset. L'azione di regola prevede stringhe per tutti i parametri.

Per identificare una proprietà dell'asset, specifica uno dei seguenti valori:

- Asset ID (ID asset) (`assetId`) e Property ID (ID proprietà) (`propertyId`) della proprietà dell'asset a cui invii i dati. Puoi trovare l'Asset ID e l'ID della proprietà utilizzando. Console AWS IoT SiteWise Se conosci l'Asset ID, puoi utilizzare la chiamata AWS CLI to DescribeAssetper trovare l'ID della proprietà.
- Property alias (Alias proprietà) (`propertyAlias`), che è un alias del flusso di dati (ad esempio, `/company/windfarm/3/turbine/7/temperature`). Per utilizzare questa opzione, è necessario prima impostare l'alias della proprietà dell'asset. Per informazioni relative all'impostazione degli alias delle proprietà, consultare Mappatura dei flussi di dati industriali alle proprietà degli asset.

Per il timestamp di ogni voce, utilizzate il timestamp riportato dall'apparecchiatura o il timestamp fornito da. AWS IoT Core Il timestamp ha due parametri:

- Tempo in secondi (`timeInSeconds`) — L'ora dell'epoca Unix, in secondi, in cui il sensore o l'apparecchiatura ha riportato i dati.
- Offset in nanos (`offsetInNanos`) — (Facoltativo) L'offset in nanosecondi dal tempo in secondi.

> **Important**
>
> Se il timestamp è una stringa, ha una parte decimale o non è espresso in secondi, rifiuta la richiesta. AWS IoT SiteWise È necessario convertire il timestamp in secondi e offset in nanosecondi. Utilizza le funzionalità del motore delle AWS IoT regole per convertire il timestamp. Per ulteriori informazioni, consulta gli argomenti seguenti:
>
> - Ottenere timestamp per dispositivi che non riportano l'ora esatta
> - Conversione di timestamp in formato stringa

È possibile utilizzare modelli sostitutivi per diversi parametri dell'azione per eseguire calcoli, richiamare funzioni e recuperare valori dal payload dei messaggi. Per ulteriori informazioni, consulta Modelli sostitutivi nella Guida per gli sviluppatori.AWS IoT

> **Note**
>
> Poiché un'espressione in un modello di sostituzione viene valutata separatamente dall'istruzione `SELECT`, non puoi utilizzare un modello di sostituzione per fare riferimento a un alias creato utilizzando una clausola `AS`. È possibile fare riferimento solo alle informazioni presenti nel payload originale, oltre alle funzioni e agli operatori supportati.

Argomenti

Ottenere timestamp per dispositivi che non riportano l'ora esatta

Se il sensore o l'apparecchiatura non riporta dati temporali accurati, recupera l'ora attuale di Unix dal motore delle AWS IoT regole con timestamp (). Questa funzione restituisce il tempo in millisecondi, quindi è necessario convertire il valore in tempo in secondi e l'offset in nanosecondi. A tale scopo, utilizzate le seguenti conversioni:

- Per Time in seconds (Ora in secondi) (`timeInSeconds`), utilizza **`${floor(timestamp() / 1E3)}`** per convertire l'ora da millisecondi in secondi.
- Per Offset in nanos (Offset in nanosecondi) (`offsetInNanos`), utilizza **`${(timestamp() % 1E3) * 1E6}`** per calcolare l'offset del timestamp in nanosecondi.

Conversione di timestamp in formato stringa

Se il sensore o l'apparecchiatura riporta i dati temporali in formato stringa (ad esempio,`2020-03-03T14:57:14.699Z`), usa time_to_epoch (String, String). Questa funzione inserisce il timestamp e lo schema di formato come parametri e restituisce l'ora in millisecondi. Quindi, è necessario convertire il tempo in tempo in secondi e l'offset in nanosecondi. A tale scopo, utilizzate le seguenti conversioni:

- Per Tempo in secondi (`timeInSeconds`), utilizzare **`${floor(time_to_epoch("2020-03-03T14:57:14.699Z", "yyyy-MM-dd'T'HH:mm:ss'Z'") / 1E3)}`** per convertire la stringa del timestamp in millisecondi e quindi in secondi.
- Per Offset in nanos (`offsetInNanos`), usa per calcolare l'offset in nanosecondi della stringa del **`${(time_to_epoch("2020-03-03T14:57:14.699Z", "yyyy-MM-dd'T'HH:mm:ss'Z'") % 1E3) * 1E6}`** timestamp.

> **Note**
>
> La `time_to_epoch` funzione supporta stringhe di timestamp con precisione fino a un millisecondo. Per convertire stringhe con precisione in microsecondi o nanosecondi, configura una AWS Lambda funzione richiamata dalla regola per convertire il timestamp in valori numerici. Per ulteriori informazioni, consulta Conversione di stringhe di timestamp con precisione in nanosecondi.

Conversione di stringhe di timestamp con precisione in nanosecondi

Se il dispositivo invia informazioni sul timestamp in formato stringa con precisione in nanosecondi (ad esempio,), `2020-03-03T14:57:14.699728491Z` utilizza la procedura seguente per configurare l'azione della regola. Potete creare una AWS Lambda funzione che converta il timestamp da una stringa in Time in seconds (**`timeInSeconds`**) e Offset in nanos (). `offsetInNanos` Quindi, usa

aws_lambda (functionArn, inputJSON) nei parametri di azione della regola per richiamare quella funzione Lambda e utilizzare l'output nella regola.

> **Note**
>
> Questa sezione contiene istruzioni avanzate che presuppongono che si abbia familiarità con la creazione delle risorse seguenti:
>
> - Funzioni Lambda. Per ulteriori informazioni, consulta Creare una funzione Lambda con la console o Using Lambda con la AWS CLI nella Developer Guide.AWS Lambda
> - AWS IoT regole con la AWS IoT SiteWise regola d'azione. Per ulteriori informazioni, consulta Acquisizione di dati tramite regole AWS IoT Core.

Per creare un'azione di AWS IoT SiteWise regola che analizzi le stringhe del timestamp

1. Crea una funzione Lambda con le seguenti proprietà:

   - Nome della funzione: utilizza un nome di funzione descrittivo (ad esempio,**`ConvertNanosecondTimestampFromString`**).
   - Runtime — Usa un runtime Python 3, come Python 3.11 (). `python3.11`
   - Autorizzazioni: crea un ruolo con AWS LambdaBasicExecutionRoleautorizzazioni Lambda di base ().
   - Livelli: aggiungi il livello AWS SdkPandas-Python311 per l'utilizzo della funzione Lambda. `numpy`
   - Codice funzionale: utilizzate il seguente codice di funzione, che utilizza un argomento di stringa denominato e restituisce e valori per quel timestamp. `timestamp` `timeInSeconds` `offsetInNanos`

     ```
     import json
     import math
     import numpy

     # Converts a timestamp string into timeInSeconds and offsetInNanos in Unix epoch
      time.
     # The input timestamp string can have up to nanosecond precision.
     def lambda_handler(event, context):
         timestamp_str = event['timestamp']
         # Parse the timestamp string as nanoseconds since Unix epoch.
     ```

```
    nanoseconds = numpy.datetime64(timestamp_str, 'ns').item()
    time_in_seconds = math.floor(nanoseconds / 1E9)
    # Slice to avoid precision issues.
    offset_in_nanos = int(str(nanoseconds)[-9:])
    return {
        'timeInSeconds': time_in_seconds,
        'offsetInNanos': offset_in_nanos
    }
```

Questa funzione Lambda inserisce stringhe di timestamp in formato ISO 8601 utilizzando datetime64 from. NumPy

> **Note**
>
> Se le stringhe del timestamp non sono in formato ISO 8601, puoi implementare una soluzione che definisca il formato del timestamp. pandas Per ulteriori informazioni, consulta pandas.to_datetime.

2. Quando configuri l' AWS IoT SiteWise azione per la tua regola, usa i seguenti modelli sostitutivi per Time in seconds () e Offset in nanos (). **`timeInSeconds`** `offsetInNanos` Questi modelli di sostituzione presuppongono che il payload del messaggio contenga la stringa timestamp in `timestamp`. La funzione `aws_lambda` utilizza una struttura JSON per il suo secondo parametro, quindi è possibile modificare i modelli di sostituzione sottostanti, se necessario.

   - Per Time in seconds (Tempo in secondi) (`timeInSeconds`), utilizzare il seguente modello di sostituzione.

     ```
     ${aws_lambda('arn:aws:lambda:region:account-
     id:function:ConvertNanosecondTimestampFromString', {'timestamp':
      timestamp}).timeInSeconds}
     ```

   - Per Offset in nanos (Offset in nanosecondi) (`offsetInNanos`), utilizzare il seguente modello di sostituzione.

     ```
     ${aws_lambda('arn:aws:lambda:region:account-
     id:function:ConvertNanosecondTimestampFromString', {'timestamp':
      timestamp}).offsetInNanos}
     ```

Per ogni parametro, sostituisci *`region e account-id con la tua regione e l'ID dell'`*account. AWS Se hai usato un nome diverso per la tua funzione Lambda, cambia anche quello.

3. Concedi AWS IoT le autorizzazioni per richiamare la tua funzione con l'autorizzazione. `lambda:InvokeFunction` Per ulteriori informazioni, consultare aws_lambda(functionArn, inputJson).
4. Verifica la tua regola (ad esempio, usa il client di test AWS IoT MQTT) e verifica che AWS IoT SiteWise riceva i dati che invii.

   Se la regola non funziona come previsto, consultare Risoluzione dei problemi e azioni AWS IoT SiteWise relative alle regole.

> **Note**
>
> Questa soluzione richiama la funzione Lambda due volte per ogni stringa di timestamp. Puoi creare un'altra regola per ridurre il numero di chiamate alla funzione Lambda se la regola gestisce più punti dati con lo stesso timestamp in ogni payload.
> A tale scopo, create una regola con un'azione di ripubblicazione che richiami la Lambda e pubblichi il payload originale con la stringa del timestamp convertita in and. `timeInSeconds` `offsetInNanos` Quindi, create una regola con un'azione di regola per consumare il payload convertito AWS IoT SiteWise . Con questo approccio, riduci il numero di volte in cui la regola richiama la Lambda ma aumenti il numero di azioni della AWS IoT regola eseguite. Considerare il prezzo di ciascun servizio se si applica questa soluzione al caso d'uso.

Esempi di configurazioni di regole

Questa sezione contiene esempi di configurazioni di regole per creare una regola con un' AWS IoT SiteWise azione.

Example Azione di regola di esempio che utilizza alias di proprietà come argomenti dei messaggi

L'esempio seguente crea una regola con un' AWS IoT SiteWise azione che utilizza l'argomento (tramite topic ()) come alias di proprietà per identificare le proprietà degli asset. Utilizzate questo esempio per definire una regola per l'importazione di dati di doppio tipo in tutte le turbine eoliche di tutti i parchi eolici. Questo esempio richiede la definizione di alias di proprietà su tutte le proprietà

degli asset delle turbine. È necessario definire una seconda regola simile per importare dati di tipo intero.

```
aws iot create-topic-rule \
  --rule-name SiteWiseWindFarmRule \
  --topic-rule-payload file://sitewise-rule-payload.json
```

Il payload di esempio in `sitewise-rule-payload.json` contiene quanto segue.

```
{
  "sql": "SELECT * FROM '/company/windfarm/+/turbine/+/+' WHERE type = 'double'",
  "description": "Sends data to the wind turbine asset property with the same alias as
 the topic",
  "ruleDisabled": false,
  "awsIotSqlVersion": "2016-03-23",
  "actions": [
    {
      "iotSiteWise": {
        "putAssetPropertyValueEntries": [
          {
            "propertyAlias": "${topic()}",
            "propertyValues": [
              {
                "timestamp": {
                  "timeInSeconds": "${timeInSeconds}"
                },
                "value": {
                  "doubleValue": "${value}"
                }
              }
            ]
          }
        ],
        "roleArn": "arn:aws:iam::account-id:role/MySiteWiseActionRole"
      }
    }
  ]
}
```

Con questa azione di regola, inviate il seguente messaggio a un alias di proprietà di una turbina eolica (ad esempio,`/company/windfarm/3/turbine/7/temperature`) come argomento per l'inserimento dei dati.

```
{
  "type": "double",
  "value": "38.3",
  "timeInSeconds": "1581368533"
}
```

Example Azione di regola di esempio che utilizza timestamp() per determinare l'ora

L'esempio seguente crea una regola con un' AWS IoT SiteWise azione che identifica la proprietà di un asset tramite ID e utilizza timestamp () per determinare l'ora corrente.

```
aws iot create-topic-rule \
  --rule-name SiteWiseAssetPropertyRule \
  --topic-rule-payload file://sitewise-rule-payload.json
```

Il payload di esempio in `sitewise-rule-payload.json` contiene quanto segue.

```
{
  "sql": "SELECT * FROM 'my/asset/property/topic'",
  "description": "Sends device data to an asset property",
  "ruleDisabled": false,
  "awsIotSqlVersion": "2016-03-23",
  "actions": [
    {
      "iotSiteWise": {
        "putAssetPropertyValueEntries": [
          {
            "assetId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
            "propertyId": "a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
            "propertyValues": [
              {
                "timestamp": {
                  "timeInSeconds": "${floor(timestamp() / 1E3)}",
                  "offsetInNanos": "${(timestamp() % 1E3) * 1E6}"
                },
                "value": {
                  "doubleValue": "${value}"
                }
              }
            ]
          }
        ],
```

```
        "roleArn": "arn:aws:iam::account-id:role/MySiteWiseActionRole"
      }
    }
  ]
}
```

Con questa azione della regola, inviate il seguente messaggio a per `my/asset/property/topic` importare i dati.

```
{
  "type": "double",
  "value": "38.3"
}
```

Risoluzione dei problemi dell'azione di regola

Per risolvere l'azione della AWS IoT SiteWise regola in AWS IoT Core, configura i CloudWatch registri o configura un'azione di errore di ripubblicazione per la regola. Per ulteriori informazioni, consulta Risoluzione dei problemi e azioni AWS IoT SiteWise relative alle regole.

Riduzione dei costi con Basic Ingest

AWS IoT Core offre una funzionalità denominata Basic Ingest che è possibile utilizzare per inviare dati AWS IoT Core senza incorrere in costi di messaggistica.AWS IoT Basic Ingest ottimizza il flusso di dati per i carichi di lavoro di inserimento con elevati volumi di dati rimuovendo il broker dei messaggi di pubblicazione/sottoscrizione dal percorso di inserimento. Puoi utilizzare Basic Ingest se conosci le regole a cui devono essere instradati i messaggi.

Per utilizzare Basic Ingest, invii i messaggi direttamente a una regola specifica utilizzando l'argomento speciale `$aws/rules/rule-name`. Ad esempio, per inviare un messaggio a una regola denominata `SiteWiseWindFarmRule`, invii un messaggio all'argomento `$aws/rules/SiteWiseWindFarmRule`.

Se l'azione di regola utilizza modelli di sostituzione contenenti topic(Decimal), puoi passare l'argomento originale alla fine dell'argomento speciale di Basic Ingest, ad esempio `$aws/rules/rule-name/original-topic`. Ad esempio, per utilizzare Basic Ingest con l'alias di proprietà della centrale eolica di esempio della sezione precedente, puoi inviare messaggi al seguente argomento.

```
$aws/rules/SiteWiseWindFarmRule//company/windfarm/3/turbine/7/temperature
```

> **Note**
>
> L'esempio precedente include una seconda barra (`//`) perché AWS IoT rimuove il prefisso Basic Ingest (`$aws/rules/rule-name/`) dall'argomento visibile all'azione della regola. In questo esempio, la regola riceve l'argomento `/company/windfarm/3/turbine/7/temperature`.

Per ulteriori informazioni, consulta Ridurre i costi di messaggistica con Basic Ingest nella Guida per gli sviluppatori.AWS IoT

Acquisizione di dati da AWS IoT Events

Con AWS IoT Events, puoi creare applicazioni complesse di monitoraggio degli eventi per la tua flotta IoT nel AWS Cloud. Utilizza l' SiteWise azione IoT in AWS IoT Events per inviare dati alle proprietà degli asset AWS IoT SiteWise quando si verifica un evento.

AWS IoT Events è progettato per semplificare lo sviluppo di applicazioni di monitoraggio degli eventi per dispositivi e sistemi IoT all'interno del AWS Cloud. Utilizzando AWS IoT Events, puoi:

- Rileva e rispondi a cambiamenti, anomalie o condizioni specifiche nella tua flotta IoT.
- Migliora l'efficienza operativa e abilita la gestione proattiva del tuo ecosistema IoT.

Grazie all'integrazione con AWS IoT SiteWise through the AWS IoT SiteWise action, ne AWS IoT Events estende le funzionalità, consentendoti di aggiornare automaticamente le proprietà degli asset AWS IoT SiteWise in risposta a eventi specifici. Questa interazione può semplificare l'inserimento e la gestione dei dati. Può anche fornirti informazioni utili.

Per ulteriori informazioni, consulta i seguenti argomenti nella Guida per gli AWS IoT Events sviluppatori:

- Che cos'è AWS IoT Events?
- Operazioni AWS IoT Events
- SiteWise Azione IoT

Utilizzo AWS IoT Greengrass dello stream manager

AWS IoT Greengrass stream manager è una funzionalità di integrazione che facilita il trasferimento di flussi di dati da fonti locali al AWS cloud. Funge da livello intermedio che gestisce i flussi di dati, consentendo ai dispositivi che operano all'edge di raccogliere e archiviare i dati prima che vengano inviati AWS IoT SiteWise, per ulteriori analisi ed elaborazioni.

Aggiungi una destinazione di dati configurando una fonte locale sulla AWS IoT SiteWise console. Puoi anche utilizzare stream manager nella tua AWS IoT Greengrass soluzione personalizzata per importare dati. AWS IoT SiteWise

> **Note**
>
> Per importare dati da fonti OPC-UA, configura un gateway AWS IoT SiteWise Edge che funzioni su. AWS IoT Greengrass Per ulteriori informazioni, consulta Utilizzo dei gateway SiteWise Edge.

Per ulteriori informazioni su come configurare una destinazione per i dati di origine locale, consulta. Configurazione delle origini dati

Per ulteriori informazioni su come importare dati utilizzando stream manager in una AWS IoT Greengrass soluzione personalizzata, consulta i seguenti argomenti nella Guida per gli AWS IoT Greengrass Version 2 sviluppatori:

- Che cos'è AWS IoT Greengrass?
- Gestisci i flussi di dati sul core AWS IoT Greengrass
- Esportazione dei dati nelle proprietà degli asset AWS IoT SiteWise

Acquisizione di dati tramite l'API AWS IoT SiteWise

Utilizza l' AWS IoT SiteWise API per inviare dati industriali con data e ora alle proprietà degli attributi e di misurazione degli asset. L'API accetta un payload che contiene strutture (TQV). timestamp-quality-value

Usa l'BatchPutAssetPropertyValueoperazione per caricare i tuoi dati. Con questa operazione, puoi caricare più immissioni di dati alla volta per raccogliere dati da più dispositivi e inviarli tutti in un'unica richiesta.

> **Important**
>
> L'BatchPutAssetPropertyValueoperazione è soggetta alle seguenti quote:
>
> - Fino a 10 iscrizioni per richiesta.
> - Fino a 10 valori di proprietà (punti dati TQV) per ingresso.
> - AWS IoT SiteWise rifiuta tutti i dati con un timestamp datato a più di 7 giorni nel passato o a più di 10 minuti nel futuro.
>
> Per ulteriori informazioni su queste quote, consulta l'API Reference BatchPutAssetPropertyValue.AWS IoT SiteWise

Per identificare la proprietà di una risorsa, specificate una delle seguenti opzioni:

- La proprietà `assetId` e `propertyId` della risorsa a cui vengono inviati i dati.
- Il`propertyAlias`, che è un alias del flusso di dati (ad esempio,`/company/windfarm/3/turbine/7/temperature`). Per utilizzare questa opzione, è necessario prima impostare l'alias della proprietà dell'asset. Per impostare gli alias delle proprietà, vedere. Mappatura dei flussi di dati industriali alle proprietà degli asset

L'esempio seguente illustra come inviare le letture della temperatura e delle rotazioni al minuto (RPM) di una turbina eolica da un payload archiviato in un file JSON.

```
aws iotsitewise batch-put-asset-property-value --cli-input-json file://batch-put-
payload.json
```

Il payload di esempio in `batch-put-payload.json` contiene quanto segue.

```
{
  "entries": [
    {
      "entryId": "unique entry ID",
      "propertyAlias": "/company/windfarm/3/turbine/7/temperature",
      "propertyValues": [
        {
          "value": {
            "integerValue": 38
```

```
          },
          "timestamp": {
            "timeInSeconds": 1575691200
          }
        }
      ]
    },
    {
      "entryId": "unique entry ID",
      "propertyAlias": "/company/windfarm/3/turbine/7/rpm",
      "propertyValues": [
        {
          "value": {
            "doubleValue": 15.09
          },
          "timestamp": {
            "timeInSeconds": 1575691200
          },
          "quality": "GOOD"
        }
      ]
    }
  ]
}
```

Ogni voce nel payload contiene un `entryId` che è possibile definire come una qualsiasi stringa univoca. Se una richiesta non riesce, ciascun errore conterrà l'`entryId` della richiesta corrispondente in modo che sia possibile sapere quale richiesta riprovare.

Ogni struttura nell'elenco di `propertyValues` è una struttura timestamp-quality-value (TQV) che contiene `a`value, a e facoltativamente `a`timestamp. `quality`

- `value`— Una struttura che contiene uno dei seguenti campi, a seconda del tipo di proprietà impostata:
  - `booleanValue`
  - `doubleValue`
  - `integerValue`
  - `stringValue`
- `timestamp`— Una struttura che contiene l'ora attuale dell'epoca Unix in secondi,. `timeInSeconds` È inoltre possibile impostare la `offsetInNanos` chiave nella `timestamp`

struttura se si dispone di dati temporalmente precisi. AWS IoT SiteWise rifiuta tutti i punti dati con timestamp più vecchi di 7 giorni nel passato o più recenti di 10 minuti nelle future.

- `quality`— (Facoltativo) Una delle seguenti stringhe di qualità:
  - `GOOD`— (Impostazione predefinita) I dati non sono interessati da alcun problema.
  - `BAD`— I dati sono interessati da un problema, ad esempio un guasto del sensore.
  - `UNCERTAIN`— I dati sono influenzati da un problema come l'imprecisione del sensore.

  Per ulteriori informazioni su come AWS IoT SiteWise gestisce la qualità dei dati nei calcoli, vedi Qualità dei dati nelle espressioni di formule.

Acquisizione di dati tramite l'API CreateBulkImportJob

Usa l'`CreateBulkImportJob`API per importare grandi quantità di dati da Amazon S3. I tuoi dati devono essere salvati in formato CSV in Amazon S3. I file di dati possono avere le seguenti colonne.

> **Note**
>
> Per identificare la proprietà di una risorsa, specificate una delle seguenti opzioni.
>
> - La proprietà `ASSET_ID` e `PROPERTY_ID` della risorsa a cui stai inviando i dati.
> - IlALIAS, che è un alias del flusso di dati (ad esempio,`/company/windfarm/3/turbine/7/temperature`). Per utilizzare questa opzione, è necessario prima impostare l'alias della proprietà dell'asset. Per informazioni relative all'impostazione degli alias delle proprietà, consultare the section called “Mappatura dei flussi di dati industriali alle proprietà degli asset”.

- `ALIAS`— L'alias che identifica la proprietà, ad esempio il percorso del flusso di dati del server OPC-UA (ad esempio,). `/company/windfarm/3/turbine/7/temperature` Per ulteriori informazioni, consulta Mappatura dei flussi di dati industriali alle proprietà degli asset.
- `ASSET_ID`— L'ID della risorsa.
- `PROPERTY_ID`— L'ID della proprietà dell'asset.
- `DATA_TYPE`— Il tipo di dati della proprietà può essere uno dei seguenti.
  - `STRING`— Una stringa con un massimo di 1024 byte.
  - `INTEGER`— Un numero intero con segno a 32 bit con intervallo [-2.147.483.648, 2.147.483.647].

  - `DOUBLE`— Un numero in virgola mobile con intervallo [-10^100, 10^100] e precisione doppia IEEE 754.
  - `BOOLEAN`— `true` oppure. `false`
- `TIMESTAMP_SECONDS`— Il timestamp del punto dati, in Unix Epoch Time.
- `TIMESTAMP_NANO_OFFSET`— L'offset in nanosecondi coperto da. `TIMESTAMP_SECONDS`
- `QUALITY`— (Facoltativo) La qualità del valore della proprietà del bene. Il valore può essere uno dei seguenti.
  - `GOOD`— (Impostazione predefinita) I dati non sono interessati da alcun problema.
  - `BAD`— I dati sono interessati da un problema, ad esempio un guasto del sensore.
  - `UNCERTAIN`— I dati sono influenzati da un problema come l'imprecisione del sensore.

  Per ulteriori informazioni su come AWS IoT SiteWise gestisce la qualità dei dati nei calcoli, vedi Qualità dei dati nelle espressioni di formule.
- `VALUE`— Il valore della proprietà dell'asset.

Example file di dati in formato.csv

```
asset_id,property_id,DOUBLE,1635201373,0,GOOD,1.0
asset_id,property_id,DOUBLE,1635201374,0,GOOD,2.0
asset_id,property_id,DOUBLE,1635201375,0,GOOD,3.0
```

```
unmodeled_alias1,DOUBLE,1635201373,0,GOOD,1.0
unmodeled_alias1,DOUBLE,1635201374,0,GOOD,2.0
unmodeled_alias1,DOUBLE,1635201375,0,GOOD,3.0
unmodeled_alias1,DOUBLE,1635201376,0,GOOD,4.0
unmodeled_alias1,DOUBLE,1635201377,0,GOOD,5.0
unmodeled_alias1,DOUBLE,1635201378,0,GOOD,6.0
unmodeled_alias1,DOUBLE,1635201379,0,GOOD,7.0
unmodeled_alias1,DOUBLE,1635201380,0,GOOD,8.0
unmodeled_alias1,DOUBLE,1635201381,0,GOOD,9.0
unmodeled_alias1,DOUBLE,1635201382,0,GOOD,10.0
```

AWS IoT SiteWise fornisce le seguenti operazioni API per creare un processo di importazione in blocco e ottenere informazioni su un lavoro esistente.

- CreateBulkImportJob— Crea un nuovo processo di importazione in blocco.
- DescribeBulkImportJob— Recupera informazioni su un processo di importazione in blocco.

- ListBulkImportJob— Recupera un elenco impaginato di riepiloghi di tutti i lavori di importazione in blocco.

Crea un processo di importazione in blocco ()AWS CLI

Utilizza l'operazione CreateBulkImportJobAPI per trasferire dati da Amazon S3 a. AWS IoT SiteWise Utilizza l'CreateBulkImportJobAPI per importare dati in piccoli lotti in modo conveniente. Nell'esempio seguente viene utilizzato AWS CLI.

> **Important**
>
> Prima di creare un processo di importazione in blocco, devi abilitare il livello AWS IoT SiteWise caldo o AWS IoT SiteWise il livello freddo. Per ulteriori informazioni, consulta Configurare le impostazioni di archiviazione.
> L'importazione in blocco è progettata per archiviare dati storici in. AWS IoT SiteWise Non avvia calcoli o notifiche sul livello AWS IoT SiteWise caldo o sul livello AWS IoT SiteWise freddo.

Esegui il comando seguente. Sostituisci *file-name* con il nome del file che contiene la configurazione del processo di importazione in blocco.

```
aws iotsitewise create-bulk-import-job --cli-input-json file://file-name.json
```

Example Configurazione del processo di importazione in blocco

Di seguito sono riportati alcuni esempi di impostazioni di configurazione:

- Sostituisci *adaptive-ingestion-flag* con `true` o `false`.
  - Se impostato su`false`, il processo di importazione in blocco inserisce i dati storici in. AWS IoT SiteWise
  - Se impostato su`true`, il processo di importazione in blocco esegue le seguenti operazioni:
    - Inserisce nuovi dati in. AWS IoT SiteWise
    - Calcola metriche e trasformazioni e supporta notifiche per i dati con un timestamp entro sette giorni.
- Sostituisci *delete-files-after-import-flag* con `true` per eliminare i dati dal bucket di dati S3 dopo averli inseriti in uno storage di livello caldo. AWS IoT SiteWise

- Sostituisci *error-bucket* con il nome del bucket Amazon S3 a cui vengono inviati gli errori associati a questo processo di importazione in blocco.
- Sostituisci *error-bucket-prefix*con il prefisso del bucket Amazon S3 a cui vengono inviati gli errori associati a questo processo di importazione in blocco.

  Amazon S3 utilizza il prefisso come nome di cartella per organizzare i dati nel bucket. Ogni oggetto Amazon S3 ha una chiave che è il suo identificatore univoco nel bucket. Per ogni oggetto in un bucket è presente esattamente una chiave. Il prefisso deve terminare con una barra (/). Per ulteriori informazioni, consulta Organization object using prefixes nella Amazon Simple Storage Service User Guide.
- Sostituisci *data-bucket* con il nome del bucket Amazon S3 da cui vengono importati i dati.
- Sostituisci *data-bucket-key*con la chiave dell'oggetto Amazon S3 che contiene i tuoi dati. Ogni oggetto ha una chiave che è un identificatore univoco. Ogni oggetto ha esattamente una chiave.
- Sostituiscilo *data-bucket-version-id*con l'ID della versione per identificare una versione specifica dell'oggetto Amazon S3 che contiene i tuoi dati. Questo parametro è facoltativo.
- Sostituisci *column-name* con il nome della colonna specificato nel file.csv.
- Sostituisci *job-name con un nome* univoco che identifichi il processo di importazione in blocco.
- Sostituisci *job-role-arn*con il ruolo IAM che consente di AWS IoT SiteWise leggere i dati di Amazon S3.

> **Note**
>
> Assicurati che il tuo ruolo disponga delle autorizzazioni mostrate nell'esempio seguente. Sostituisci *data-bucket* con il nome del bucket Amazon S3 che contiene i tuoi dati. Inoltre, sostituisci *error-bucket* con il nome del bucket Amazon S3 a cui vengono inviati gli errori associati a questo processo di importazione in blocco.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:GetObject",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::data-bucket",
```

```
                "arn:aws:s3:::data-bucket/*",
            ],
            "Effect": "Allow"
        },
       {
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::error-bucket",
                "arn:aws:s3:::error-bucket/*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

```
{
   "adaptiveIngestion": adaptive-ingestion-flag,
   "deleteFilesAfterImport": delete-files-after-import-flag,
   "errorReportLocation": {
      "bucket": "error-bucket",
      "prefix": "error-bucket-prefix"
   },
   "files": [
      {
         "bucket": "data-bucket",
         "key": "data-bucket-key",
         "versionId": "data-bucket-version-id"
      }
   ],
   "jobConfiguration": {
      "fileFormat": {
         "csv": {
            "columnNames": [ "column-name" ]
         }
      }
   },
   "jobName": "job-name",
```

```
   "jobRoleArn": "job-role-arn"
}
```

Example response

```
{
   "jobId":"f8c031d0-01d1-4b94-90b1-afe8bb93b7e5",
   "jobStatus":"PENDING",
   "jobName":"myBulkImportJob"
}
```

Descrivi un processo di importazione in blocco ()AWS CLI

Utilizzate l'operazione DescribeBulkImportJobAPI per recuperare informazioni su un processo di importazione in blocco. L'esempio seguente utilizza. AWS CLI

Sostituisci *Job-ID* con l'ID del processo di importazione in blocco che desideri recuperare.

```
aws iotsitewise describe-bulk-import-job --job-id job-ID
```

Example response

```
{
   "files":[
      {
         "bucket":"test-bucket",
         "key":"100Tags12Hours.csv"
      },
      {
         "bucket":"test-bucket",
         "key":"BulkImportData1MB.csv"
      },
      {
         "bucket":"test-bucket",
         "key":"UnmodeledBulkImportData1MB.csv"
      }
   ],
   "errorReportLocation":{
      "prefix":"errors/",
      "bucket":"test-error-bucket"
   },
```

```
   "jobConfiguration":{
      "fileFormat":{
         "csv":{
            "columnNames":[
               "ALIAS",
               "DATA_TYPE",
               "TIMESTAMP_SECONDS",
               "TIMESTAMP_NANO_OFFSET",
               "QUALITY",
               "VALUE"
            ]
         }
      }
   },
   "jobCreationDate":1645745176.498,
   "jobStatus":"COMPLETED",
   "jobName":"myBulkImportJob",
   "jobLastUpdateDate":1645745279.968,
   "jobRoleArn":"arn:aws:iam::123456789012:role/DemoRole",
   "jobId":"f8c031d0-01d1-4b94-90b1-afe8bb93b7e5"
}
```

Elenca i lavori di importazione in blocco ()AWS CLI

Utilizzate l'operazione ListBulkImportJobsAPI per recuperare un elenco impaginato di riepiloghi di tutti i lavori di importazione in blocco. L'esempio seguente utilizza. AWS CLI

```
aws iotsitewise list-bulk-import-jobs --filter COMPLETED
```

Example response

```
{
   "jobSummaries":[
      {
         "id":"bdbbfa52-d775-4952-b816-13ba1c7cb9da",
         "name":"myBulkImportJob",
         "status":"COMPLETED"
      },
      {
         "id":"15ffc641-dbd8-40c6-9983-5cb3b0bc3e6b",
         "name":"myBulkImportJob2",
         "status":"RUNNING"
```

```
        }
    ]
}
```

Utilizzo dei gateway SiteWise Edge

Un gateway AWS IoT SiteWise Edge funge da intermediario tra le apparecchiature industriali e. AWS IoT SiteWise Funziona su un gateway SiteWise Edge AWS IoT Greengrass V2 che supporta la raccolta e l'elaborazione dei dati in locale. È possibile utilizzare AWS OpsHub for per AWS IoT SiteWise gestire i gateway SiteWise Edge e monitorare le operazioni in loco.

È possibile monitorare i dati localmente nella propria struttura utilizzando i portali SiteWise Monitor sui dispositivi locali. Per ulteriori informazioni, consulta Attivazione del portale all'edge.

Argomenti

SiteWise Requisiti del gateway edge

AWS IoT SiteWise I gateway edge funzionano AWS IoT Greengrass V2 come un insieme di AWS IoT Greengrass componenti che supportano la raccolta, l'elaborazione e la pubblicazione dei dati

in locale. Per configurare un gateway SiteWise Edge funzionante AWS IoT Greengrass V2, è necessario creare un gateway in Cloud AWS ed eseguire il software SiteWise Edge gateway per configurare il dispositivo locale.

Requisiti

I dispositivi locali devono soddisfare i seguenti requisiti per installare ed eseguire il software SiteWise Edge gateway.

- Supporta la versione del software AWS IoT Greengrass V2 Core v2.3.0 o successiva. Per ulteriori informazioni, consulta Requisiti nella Guida per gli AWS IoT Greengrass Version 2 sviluppatori.
- Una delle seguenti piattaforme supportate:
  - Sistema operativo: Ubuntu 20.04 o successivo

    Architettura: x86_64 (AMD64) o ARMv8 (Aarch64)
  - Sistema operativo: Red Hat Enterprise Linux (RHEL) 8

    Architettura: x86_64 (AMD64) o ARMv8 (Aarch64)
  - Sistema operativo: Amazon Linux 2

    Architettura: x86_64 (AMD64) o ARMv8 (Aarch64)
  - Sistema operativo: Debian 11

    Architettura: x86_64 (AMD64) o ARMv8 (Aarch64)
  - Sistema operativo: Windows Server 2019 e versioni successive

    Architettura: x86_64 (AMD64)

  > **Note**
  >
  > Le piattaforme ARM supportano solo i gateway SiteWise Edge con Data Collection Pack. Il Data Processing Pack non è supportato.

- Minimo 4 GB di RAM.
- Almeno 10 GB di spazio su disco disponibili per il software SiteWise Edge gateway.
- Se si prevede di elaborare i dati in modalità edge con AWS IoT SiteWise, il dispositivo locale deve inoltre soddisfare i seguenti requisiti:
  - Dispone di un processore quad-core x86 a 64 bit.

  - Ha almeno 16 GB di RAM.
  - Ha almeno 32 GB di RAM se si utilizza Windows.
  - Aveva almeno 256 GB di spazio libero su disco.
- I requisiti minimi di spazio su disco e capacità di elaborazione dipendono da una serie di fattori specifici dell'implementazione e del caso d'uso.
  - Lo spazio su disco necessario per memorizzare nella cache i dati relativi alla connettività Internet intermittente dipende dai seguenti fattori:
    - Numero di flussi di dati caricati
    - Punti dati per flusso di dati al secondo
    - Dimensione di ciascun punto dati
    - Velocità di comunicazione
    - Tempo previsto di inattività della rete
  - La capacità di elaborazione necessaria per il polling e il caricamento dei dati dipende dai seguenti fattori:
    - Numero di flussi di dati caricati
    - Punti dati per flusso di dati al secondo
- Configura il dispositivo locale per assicurarti che le seguenti porte siano accessibili:
  - Il dispositivo locale deve consentire il traffico di rete in entrata sulla porta 443.
  - Il dispositivo locale deve consentire il traffico in uscita sulle porte 443 e 8883.

    Per un elenco completo degli endpoint di servizio in uscita richiesti, consulta Endpoint di servizio richiesti per i gateway Edge. AWS IoT SiteWise
  - Le seguenti porte sono riservate all'uso da AWS IoT SiteWise: 80, 443, 3001, 4569, 4572, 8000, 8081, 8082, 8084, 8085, 8445, 8086, 9000, 9500, 11080 e 50010. L'utilizzo di una porta riservata per il traffico può comportare l'interruzione della connessione.
- Java Runtime Environment (JRE) versione 11 o successiva. Java deve essere disponibile nella variabile di `PATH` ambiente del dispositivo. Per utilizzare Java per sviluppare componenti personalizzati, è necessario installare un Java Development Kit (JDK). Ti consigliamo di utilizzare Amazon Corretto o OpenJDK.

È necessario disporre delle seguenti autorizzazioni per utilizzare i gateway Edge: SiteWise

> **Note**
>
> Se utilizzi la AWS IoT SiteWise console per creare il tuo gateway SiteWise Edge, queste autorizzazioni vengono aggiunte automaticamente.

- Il ruolo IAM per il tuo gateway SiteWise Edge deve consentirti di utilizzare un gateway SiteWise Edge su un AWS IoT Greengrass V2 dispositivo per elaborare i dati del modello di asset e i dati degli asset.

  Il ruolo consente al seguente servizio di assumere il ruolo:`credentials.iot.amazonaws.com`.

  Dettagli dell'autorizzazione

  Il ruolo deve avere le seguenti autorizzazioni:

  - `iotsitewise`— Consente ai responsabili di recuperare i dati dei modelli di asset e i dati degli asset dall'edge.
  - `iot`— Consente ai AWS IoT Greengrass V2 dispositivi di interagire con. AWS IoT
  - `logs`— Consente ai AWS IoT Greengrass V2 dispositivi di inviare log ad Amazon CloudWatch Logs.
  - `s3`— Consente ai AWS IoT Greengrass V2 dispositivi di scaricare elementi di componenti personalizzati da Amazon S3.

  ```
  {
      "Version": "2012-10-17",
      "Statement": [
          {
              "Effect": "Allow",
              "Action": [
                  "iotsitewise:BatchPutAssetPropertyValue",
                  "iotsitewise:List*",
                  "iotsitewise:Describe*",
                  "iotsitewise:Get*"
              ],
              "Resource": "*"
          },
          {
              "Effect": "Allow",
              "Action": [
                  "iot:DescribeCertificate",
  ```

```
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:DescribeLogStreams",
                "s3:GetBucketLocation",
                "s3:GetObject",
                "iot:Connect",
                "iot:Publish",
                "iot:Subscribe",
                "iot:Receive",
                "iot:DescribeEndpoint"
            ],
            "Resource": "*"
        }
    ]
}
```

Creazione di un gateway SiteWise Edge

È possibile utilizzare la AWS IoT SiteWise console per creare un gateway SiteWise Edge. Questa procedura descrive in dettaglio come creare un gateway SiteWise Edge ospitato autonomamente da installare sul proprio hardware. Per informazioni sulla creazione di un gateway SiteWise Edge che funziona su Siemens Industrial Edge, consulta. Running SiteWise Edge su Siemens Industrial Edge

Creare un gateway SiteWise Edge

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Edge gateway.
3. Selezionare Create gateway (Crea gateway).
4. Per il tipo di implementazione, scegli Gateway self-hosted.
5. Inserisci un nome per il tuo gateway SiteWise Edge o utilizza il nome generato da AWS IoT SiteWise.
6. In Greengrass Device OS, seleziona il sistema operativo del dispositivo su cui installerai questo gateway SiteWise Edge.

> **Note**
>
> Il Data Processing Pack è disponibile solo su piattaforme x86.

7. (Facoltativo) Per elaborare e organizzare i dati sull'edge, in Funzionalità Edge, seleziona Data Processing Pack.

> **Note**
>
> Per concedere ai gruppi di utenti presenti nella directory aziendale l'accesso a questo gateway SiteWise Edge, vedere Configurazione della funzionalità edge

8. (Facoltativo) In configurazione avanzata, effettuate le seguenti operazioni:

   - Per il dispositivo principale Greengrass, scegli una delle seguenti opzioni:

     - Configurazione predefinita: utilizza AWS automaticamente le impostazioni predefinite per creare un dispositivo principale Greengrass in. AWS IoT Greengrass V2

       1. Inserisci un nome per il dispositivo principale Greengrass o usa il nome generato da. AWS IoT SiteWise

     - Configurazione avanzata: scegli questa opzione se desideri utilizzare un dispositivo principale Greengrass esistente o crearne uno manualmente.

       1. Scegli un dispositivo principale Greengrass o scegli Crea dispositivo principale Greengrass per crearne uno nella console. AWS IoT Greengrass V2 Per ulteriori informazioni, consulta Configurazione dei dispositivi AWS IoT Greengrass V2 principali nella Guida per gli AWS IoT Greengrass Version 2 sviluppatori.

9. Selezionare Create gateway (Crea gateway).

10. Nella finestra di dialogo del programma di installazione del gateway Generate SiteWise Edge, scegli Genera e scarica. AWS IoT SiteWise genera automaticamente un programma di installazione che è possibile utilizzare per configurare il dispositivo locale.

> **Important**
>
> Assicurati di salvare il file di installazione in una posizione sicura. Il file verrà utilizzato in un secondo momento.

Ora che hai creato il gateway SiteWise Edge, aggiungi fonti di dati, configura il componente publisher e consenti al gateway SiteWise Edge di ricevere dati e inviarli al AWS cloud.

Installazione del software SiteWise Edge gateway sul dispositivo locale

Dopo aver creato un gateway SiteWise Edge, è necessario installare il software SiteWise Edge gateway sul dispositivo locale. SiteWise Il software Edge Gateway può essere installato su dispositivi locali su cui sono installati sistemi operativi server Linux o Windows.

> **Important**
>
> Assicurati che il dispositivo locale si connetta a Internet.

Linux

La procedura seguente utilizza SSH per connettersi al dispositivo locale. In alternativa, è possibile utilizzare un'unità flash USB o altri strumenti per trasferire il file di installazione sul dispositivo locale. Se non desideri utilizzare SSH, vai al passaggio 2: installa il software gateway SiteWise Edge riportato di seguito.

Prerequisiti SSH

Prima di connetterti al dispositivo tramite SSH, completa i seguenti prerequisiti.

- Ottieni l'indirizzo IP del tuo dispositivo.
- Ottieni il nome utente per connetterti al tuo dispositivo.
- Installa un client SSH sul tuo computer locale, se necessario.

  Il computer locale potrebbe avere un client SSH installato per impostazione predefinita. Puoi verificarlo digitando ssh nella riga di comando. Se il computer non riconosce il comando, è possibile installare un client SSH.

  - Linux e macOS: scarica e installa OpenSSH. Per ulteriori informazioni, consulta https://www.openssh.com.

Passaggio 1: copia il programma di installazione sul dispositivo gateway Edge SiteWise

Le seguenti istruzioni spiegano come connettersi al dispositivo locale utilizzando un client SSH.

1. Per connetterti al tuo dispositivo, esegui il seguente comando in una finestra di terminale sul tuo computer, sostituendo *nome utente* e *IP* con un nome utente con privilegi e indirizzo IP elevati.

```
ssh username@IP
```

2. Per trasferire il file di installazione AWS IoT SiteWise generato sul dispositivo gateway SiteWise Edge, esegui il comando seguente.

> **Note**
>
> - Sostituiscilo *path-to-saved-installer*con il percorso sul computer utilizzato per salvare il file di installazione e il nome del file di installazione.
> - Sostituisci *l'indirizzo IP* con l'indirizzo IP del dispositivo locale.
> - Sostituiscilo *directory-to-receive-installer*con il percorso sul dispositivo locale che usi per ricevere il file di installazione.

```
scp path-to-saved-installer.sh user-name@IP-address:directory-to-receive-
installer
```

Passaggio 2: installare il software SiteWise Edge gateway

Nelle seguenti procedure, esegui i comandi in una finestra di terminale sul tuo dispositivo gateway SiteWise Edge.

1. Assegna al file di installazione l'autorizzazione di esecuzione.

```
chmod +x path-to-installer.sh
```

2. Eseguire il programma di installazione.

```
sudo ./path-to-installer.sh
```

Windows server

Prerequisiti

È necessario disporre dei seguenti prerequisiti per installare il software SiteWise Edge gateway:

- Windows Server 2019 o versione successiva installato
- Privilegi di amministratore
- PowerShell versione 5.1 o successiva installata
- SiteWise Il programma di installazione di Edge Gateway è stato scaricato su Windows Server, dove verrà eseguito il provisioning

Passaggio 1: Esegui PowerShell come amministratore

1. Sul server Windows in cui desideri installare SiteWise Edge gateway, accedi come amministratore.
2. Entra PowerShellnella barra di ricerca di Windows.
3. Nei risultati della ricerca, apri il menu contestuale (fai clic con il pulsante destro del mouse) sull' PowerShell app Windows. Scegli Esegui come amministratore.

Passaggio 2: installa il software SiteWise Edge gateway

Esegui i seguenti comandi in una finestra di terminale sul tuo dispositivo SiteWise Edge Gateway.

1. Sblocca il programma di installazione del gateway SiteWise Edge.

```
unblock-file path-to-installer.ps1
```

2. Esegui il programma di installazione.

```
./path-to-installer.ps1
```

> **Note**
>
> Se l'esecuzione dello script è disabilitata sul sistema, modifica la politica di esecuzione dello script in`RemoteSigned`.

```
Set-ExecutionPolicy RemoteSigned
```

Abilitare l'elaborazione dei dati edge

È possibile utilizzare AWS IoT SiteWise Edge per raccogliere, elaborare e monitorare i dati delle apparecchiature a livello locale. È possibile utilizzare SiteWise Edge per modellare i dati industriali e SiteWise Monitor per creare dashboard in cui il personale operativo possa visualizzare i dati localmente. È possibile elaborare i dati localmente e inviarli a Cloud AWS, oppure elaborarli in locale utilizzando l'API. AWS IoT SiteWise

Con AWS IoT SiteWise Edge, puoi elaborare i dati grezzi localmente e scegliere di inviare solo dati aggregati per ottimizzare l'utilizzo della larghezza Cloud AWS di banda e i costi di archiviazione nel cloud.

> **Note**
>
> - AWS IoT SiteWise conserva i dati perimetrali sui gateway SiteWise Edge per un massimo di 30 giorni. Il periodo di conservazione dei dati dipende dallo spazio disponibile su disco del dispositivo.
> - Se il gateway SiteWise Edge è stato disconnesso da Cloud AWS per 30 giorni, il Data Processing Pack viene disattivato automaticamente.

Configurazione della funzionalità edge

AWS IoT SiteWise fornisce i seguenti pacchetti che il gateway SiteWise Edge può utilizzare per determinare come raccogliere ed elaborare i dati. Seleziona i pacchetti per abilitare le funzionalità edge per il tuo gateway SiteWise Edge.

- Data Collection Pack consente al gateway SiteWise Edge di raccogliere dati da più server OPC-UA e quindi di esportarli dall'edge al. Cloud AWS Diventa attivo dopo aver aggiunto fonti di dati al gateway SiteWise Edge.
- Data Processing Pack consente al gateway SiteWise Edge di elaborare i dati delle apparecchiature sull'edge. Ad esempio, puoi utilizzare modelli di asset per calcolare metriche e trasformazioni. Per ulteriori informazioni sui modelli di asset e sugli asset, consulta. Modellazione degli asset industriali

> **Note**
>
> Il Data Processing Pack è disponibile solo su piattaforme x86.

Per configurare le funzionalità edge

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Edge gateway.
3. Seleziona il gateway SiteWise Edge per il quale desideri attivare le funzionalità edge.
4. Nella sezione Funzionalità Edge, scegli Modifica
5. Nella sezione Funzionalità Edge, seleziona Abilita il pacchetto di elaborazione dati (comporta costi aggiuntivi).
6. (Facoltativo) Nella sezione Connessione LDAP Edge, è possibile concedere ai gruppi di utenti presenti nella directory aziendale l'accesso a questo gateway SiteWise Edge. I gruppi di utenti possono utilizzare le credenziali LDAP (Lightweight Directory Access Protocol) per accedere al SiteWise gateway Edge. Quindi possono utilizzare le AWS OpsHub AWS IoT SiteWise applicazioni, le operazioni AWS IoT SiteWise API o altri strumenti per gestire il gateway SiteWise Edge. Per ulteriori informazioni, consulta Gestione dei gateway SiteWise Edge.

   > **Note**
   >
   > È inoltre possibile utilizzare le credenziali Linux o Windows per accedere al gateway SiteWise Edge. Per ulteriori informazioni, consulta Accesso al gateway SiteWise Edge utilizzando le credenziali del sistema operativo Linux.

   a. Seleziona Attivato.
   b. Per Nome del provider, inserisci un nome per il tuo provider LDAP.
   c. Per Nome host o indirizzo IP, inserisci il nome host o l'indirizzo IP del tuo server LDAP.
   d. Per Porta, inserisci un numero di porta.
   e. Per Nome distinto di base (DN), immettere un nome distinto (DN) per la base.

Sono supportati i seguenti tipi di attributi: CommonName (CN), LocalityName (L), Name (ST), stateOrProvince OrganizationName (O), (OU), CountryName organizationalUnitName (C), StreetAddress (STREET), DomainComponent (DC) e userid (UID).

f. Per il DN del gruppo di amministratori, inserisci un DN.

g. Per il DN del gruppo di utenti, inserisci un DN.

7. Selezionare Salva.

Ora che hai attivato le funzionalità edge sul tuo gateway SiteWise Edge, devi configurare il tuo modello di asset per l'edge. La configurazione edge del modello di asset specifica dove vengono calcolate le proprietà degli asset. È possibile calcolare tutte le proprietà sull'edge oppure configurare le proprietà del modello di asset separatamente. Le proprietà del modello di asset includono metriche, trasformazioni e misurazioni.

Per ulteriori informazioni sulle proprietà degli asset, consulta. the section called “Definizione delle proprietà dei dati”

Dopo aver creato il modello di asset, puoi configurarlo per l'edge. Per ulteriori informazioni sulla configurazione del modello di asset per l'edge, consultathe section called “Creazione di un modello di asset (console)”.

> **Note**
>
> I modelli di asset e i dashboard vengono sincronizzati automaticamente tra il gateway Edge Cloud AWS e il gateway SiteWise Edge ogni 10 minuti. È inoltre possibile eseguire la sincronizzazione manualmente dall'applicazione gateway SiteWise Edge locale.

Elaborazione dei dati all'edge

È necessario configurare il modello di asset per l'edge prima di poter elaborare i dati del gateway SiteWise Edge sull'edge. La configurazione edge del modello di asset specifica dove vengono calcolate le proprietà degli asset. Puoi scegliere di calcolare tutte le proprietà sull'edge e inviare i risultati a Cloud AWS, oppure personalizzare dove calcolare separatamente ogni proprietà degli asset. Per ulteriori informazioni, consulta Abilitare l'elaborazione dei dati edge.

Le proprietà delle risorse includono metriche, trasformazioni e misurazioni:

- Le metriche sono i dati aggregati della risorsa in un periodo di tempo specificato. Puoi calcolare nuove metriche utilizzando i dati metrici esistenti. AWS IoT SiteWise invia sempre le tue metriche al AWS Cloud per l'archiviazione a lungo termine. AWS IoT SiteWise calcola le metriche sul AWS Cloud per impostazione predefinita. Puoi configurare il tuo modello di asset per calcolare le tue metriche all'edge. AWS IoT SiteWise invia i risultati elaborati al Cloud. AWS
- Le trasformazioni sono espressioni matematiche che mappano i punti dati delle proprietà di un asset da un modulo all'altro. Le trasformazioni possono utilizzare le metriche come dati di input e devono essere calcolate e archiviate nella stessa posizione dei relativi input. Se configuri un input metrico per il calcolo sull'edge, calcola AWS IoT SiteWise anche la trasformazione associata sull'edge.
- Le misurazioni sono formattate come dati grezzi che il dispositivo raccoglie e invia al Cloud per impostazione predefinita. AWS Puoi configurare il tuo modello di asset per archiviare questi dati sul tuo dispositivo locale.

Per ulteriori informazioni sulle proprietà degli asset, consultathe section called “Definizione delle proprietà dei dati”.

Dopo aver creato il modello di asset, puoi configurarlo per l'edge. Per ulteriori informazioni sulla configurazione del modello di asset per l'edge, consultathe section called “Creazione di un modello di asset (console)”.

> **Note**
>
> I modelli di asset e i dashboard vengono sincronizzati automaticamente tra il AWS Cloud e il gateway SiteWise Edge ogni 10 minuti. Puoi anche sincronizzare manualmente da. Gestione dei gateway SiteWise Edge

Puoi utilizzare le API AWS IoT SiteWise REST e AWS Command Line Interface (AWS CLI) per interrogare il tuo gateway SiteWise Edge per i dati sull'edge. Prima di interrogare il gateway SiteWise Edge per i dati sull'edge, è necessario soddisfare i seguenti prerequisiti:

- Le credenziali devono essere impostate per le API REST. Per ulteriori informazioni sull'impostazione delle credenziali, consulta. the section called “Gestione dei gateway SiteWise Edge”

- L'endpoint SDK deve puntare all'indirizzo IP del gateway Edge. SiteWise Puoi trovare ulteriori informazioni nella documentazione del tuo SDK. Ad esempio, consulta Specificare gli endpoint personalizzati nella Guida per gli AWS SDK for Java 2.x sviluppatori.
- Il certificato SiteWise Edge Gateway deve essere registrato. Puoi trovare ulteriori informazioni sulla registrazione del certificato SiteWise Edge gateway nella documentazione del tuo SDK. Ad esempio, consulta la registrazione dei pacchetti di certificati in Node.js nella Guida per gli sviluppatori. AWS SDK for Java 2.x

Per ulteriori informazioni sull'interrogazione dei dati con AWS IoT SiteWise, vedere. Interroga i dati da AWS IoT SiteWise

Configurazione del componente AWS IoT SiteWise Publisher

Dopo aver creato un gateway AWS IoT SiteWise Edge e installato il software, configura il componente Publisher in modo che il gateway SiteWise Edge possa esportare i dati AWS nel cloud. Per ulteriori informazioni, consulta AWS IoT SiteWise Publisher nella AWS IoT Greengrass Version 2 Developer Guide.

Per configurare l'editore (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Edge gateway.
3. Seleziona il gateway SiteWise Edge per il quale desideri configurare l'editore.
4. Nella sezione Configurazione di Publisher, scegli Modifica
5. Per Ordine di pubblicazione, scegliete una delle seguenti opzioni:
   - Pubblica prima i dati più vecchi: per impostazione predefinita, il gateway SiteWise Edge pubblica prima i dati più vecchi sul cloud.
   - Pubblica prima i dati più recenti: il gateway SiteWise Edge pubblica prima i dati più recenti sul cloud.
6. (Facoltativo) Se non desideri che il gateway SiteWise Edge comprima i tuoi dati, deseleziona Attiva la compressione durante il caricamento dei dati.
7. (Facoltativo) Se non desideri pubblicare vecchi dati, scegli Escludi dati scaduti e procedi come segue:

- Per Periodo limite, inserisci un numero e scegli un'unità. Il periodo limite deve essere compreso tra cinque minuti e sette giorni. Ad esempio, se il periodo limite è di tre giorni, i dati precedenti a tre giorni non vengono pubblicati sul cloud.

8. (Facoltativo) Per configurare impostazioni personalizzate sulla gestione dei dati sul dispositivo locale, scegli Impostazioni di archiviazione locale ed esegui le seguenti operazioni:

   a. Per Periodo di conservazione, inserisci un numero e scegli un'unità. Il periodo di conservazione deve essere compreso tra un minuto e 30 giorni e deve essere superiore o uguale al periodo di rotazione. Ad esempio, se il periodo di conservazione è di 14 giorni, il gateway SiteWise Edge elimina tutti i dati sull'edge che sono precedenti al periodo limite specificato dopo che sono stati archiviati per 14 giorni.

   b. Per Periodo di rotazione, inserisci un numero e scegli un'unità. Il periodo di rotazione deve essere superiore a un minuto e pari o inferiore al periodo di conservazione. Ad esempio, se il periodo di rotazione è di due giorni, il gateway SiteWise Edge raggruppa e salva i dati precedenti al periodo limite in un unico file. Il gateway SiteWise Edge trasferisce anche un batch di dati nella seguente directory locale una volta ogni due giorni:. `/greengrass/v2/work/aws.iot.SiteWiseEdgePublisher/exports`

   c. Per Capacità di archiviazione, inserisci un numero maggiore o uguale a 1. Se la capacità di archiviazione è di 2 GB, il gateway SiteWise Edge inizia a eliminare i dati quando più di 2 GB di dati vengono archiviati localmente.

9. Selezionare Salva.

Configurazione delle origini dati

Dopo aver configurato un gateway AWS IoT SiteWise Edge, puoi configurare le fonti di dati in modo che il gateway SiteWise Edge possa importare dati dalle apparecchiature industriali locali. AWS IoT SiteWise Ogni fonte rappresenta un server locale, ad esempio un server OPC-UA, a cui il gateway SiteWise Edge collega e recupera i flussi di dati industriali. Per ulteriori informazioni sulla configurazione di un gateway SiteWise Edge, vedere. Configurazione di un gateway AWS IoT Greengrass V1 SiteWise Edge

> **Note**
>
> AWS IoT SiteWise riavvia il gateway SiteWise Edge ogni volta che aggiungi o modifichi una fonte. Il gateway SiteWise Edge non inserirà dati durante il riavvio. Il tempo necessario per

riavviare il gateway SiteWise Edge dipende dal numero di tag presenti nelle sorgenti del gateway SiteWise Edge. Il tempo di riavvio può variare da pochi secondi (per un gateway SiteWise Edge con pochi tag) a diversi minuti (per un gateway SiteWise Edge con molti tag).

Dopo aver creato le fonti, puoi associare i flussi di dati alle proprietà delle risorse. Per ulteriori informazioni su come creare e utilizzare le risorse, consulta Modellazione degli asset industriali eMappatura dei flussi di dati industriali alle proprietà degli asset.

Puoi visualizzare le CloudWatch metriche per verificare che una fonte di dati sia connessa AWS IoT SiteWise. Per ulteriori informazioni, consulta AWS IoT Greengrass Version 2 metriche del gateway.

Attualmente, AWS IoT SiteWise supporta i seguenti protocolli di origine dati:

- OPC-UA — Un protocollo di comunicazione machine-to-machine (M2M) per l'automazione industriale.

> **Note**
>
> SiteWise Gli edge gateway in esecuzione AWS IoT Greengrass V2 attualmente non supportano le sorgenti IP Modbus TCP ed Ethernet.

Argomenti

- Configura una sorgente OPC-UA
- Configurazione dell'autenticazione delle fonti di dati
- Scelta di una destinazione per i dati del server di origine

Configura una sorgente OPC-UA

È possibile utilizzare la AWS IoT SiteWise console o la funzionalità di un gateway SiteWise Edge per definire e aggiungere una sorgente OPC-UA al gateway SiteWise Edge per rappresentare un server OPC-UA locale.

Argomenti

- Configura una sorgente OPC-UA (console)

- Configurazione di una sorgente OPC-UA (CLI)
- Consentire ai server di origine OPC-UA di affidarsi al SiteWise gateway Edge
- Filtra gli intervalli di inserimento dei dati con OPC-UA
- Utilizzo dei filtri dei nodi OPC-UA

Configura una sorgente OPC-UA (console)

Per configurare una sorgente OPC-UA utilizzando la console AWS IoT SiteWise

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegliere Gateways.
3. Seleziona il gateway SiteWise Edge per aggiungere una fonte OPC-UA.
4. Scegli Aggiungi origine dati
5. Immettete un nome per la fonte.
6. (Facoltativo) Immettete un prefisso del flusso di dati. Il gateway SiteWise Edge aggiunge questo prefisso a tutti i flussi di dati provenienti da questa fonte. Utilizzare un prefisso del flusso di dati per distinguere tra flussi di dati con lo stesso nome da origini diverse. Ogni flusso di dati deve avere un nome univoco all'interno del tuo account.
7. Compilare il campo Local endpoint (Endpoint locale) del server dell'origine dati. L'endpoint può essere l'indirizzo IP o il nome host. È inoltre possibile aggiungere un numero di porta all'endpoint locale. Ad esempio, l'endpoint locale potrebbe avere il seguente aspetto: **`opc.tcp://203.0.113.0:49320`**

   > **Note**
   >
   > Se il gateway SiteWise Edge ha un `Deployment type` dispositivo Siemens Industrial Edge nuovo e desideri importare dati dall'applicazione Edge OPC UA Server in esecuzione sullo stesso dispositivo Siemens Industrial Edge dell' AWS IoT SiteWise applicazione Edge, inserisci. **`opc.tcp://ie-opcua:48010`**

8. (Facoltativo) Per Node ID for selection, aggiungete filtri di nodo per limitare i flussi di dati da importare. Cloud AWS Per impostazione predefinita, i gateway SiteWise Edge utilizzano il nodo radice di un server per importare tutti i flussi di dati. Per definire i filtri dei nodi, è possibile utilizzare gli ID dei nodi * e ** i caratteri jolly.
9. Per Destinazioni, scegli la destinazione per i dati di origine:

- AWS IoT SiteWise in tempo reale: scegli questa opzione per inviare i dati direttamente allo AWS IoT SiteWise storage. Acquisisci e monitora i dati in tempo reale ed elabora i dati all'edge.
- AWS IoT SiteWise Memorizzato nel buffer con Amazon S3: invia dati in formato parquet ad Amazon S3 e quindi importali nello storage. AWS IoT SiteWise Scegli questa opzione per importare i dati in batch e archiviare i dati storici in modo conveniente. Puoi configurare la posizione preferita del bucket Amazon S3 e la frequenza con cui desideri che i dati vengano caricati su Amazon S3. Puoi anche scegliere cosa fare con i dati dopo l'ingestione. AWS IoT SiteWise Puoi scegliere di rendere i dati disponibili sia SiteWise in Amazon S3 che in Amazon S3 oppure puoi scegliere di eliminarli automaticamente da Amazon S3.
  - Il bucket Amazon S3 è un meccanismo di staging e buffering e supporta file in formato parquet.
  - Se selezioni la casella di controllo Importa dati nello AWS IoT SiteWise storage, i dati vengono caricati prima in Amazon S3 e poi nello AWS IoT SiteWise storage.
    - Se selezioni la casella di controllo Elimina dati da Amazon S3, i dati vengono eliminati da Amazon S3 dopo essere stati importati nello storage. SiteWise
    - Se deselezioni la casella di controllo Elimina dati da Amazon S3, i dati vengono archiviati sia in Amazon S3 che in storage. SiteWise
  - Se deselezioni la casella di controllo Importa dati nello AWS IoT SiteWise storage, i dati vengono archiviati solo in Amazon S3. Non viene importato nello SiteWise storage.

  Visita Gestione dell'archiviazione dei dati per i dettagli sulle varie opzioni di archiviazione AWS IoT SiteWise offerte. Per ulteriori informazioni sulle opzioni di prezzo, consulta la pagina AWS IoT SiteWise dei prezzi.
- AWS IoT Greengrass stream manager: utilizza AWS IoT Greengrass stream manager per inviare dati alle seguenti Cloud AWS destinazioni: canali in ingresso AWS IoT Analytics, flussi in Amazon Kinesis Data Streams, proprietà degli asset o oggetti AWS IoT SiteWise in Amazon Simple Storage Service (Amazon S3). Per ulteriori informazioni, consulta Manage data stream on the AWS IoT Greengrass Core nella Developer Guide.AWS IoT Greengrass Version 2

  Inserisci un nome per lo AWS IoT Greengrass stream.

10. Durante la configurazione di un'origine dati, l'ID del nodo per la selezione viene utilizzato per determinare la destinazione del flusso di dati.

- Se gli stessi dati vengono pubblicati sia AWS IoT SiteWise in tempo reale che in AWS IoT SiteWise buffer utilizzando Amazon S3, devi aggiungere due fonti di dati da pubblicare su entrambe le destinazioni.
- Per suddividere i dati in modo che una parte venga pubblicata AWS IoT SiteWise in tempo reale e l'altra parte su AWS IoT SiteWise Buffered utilizzando Amazon S3, devi filtrare i seguenti alias di dati:

```
/Alias01/Data1
/Alias02/Data1
/Alias03/Data1
/Alias03/Data2
```

Ad esempio, puoi aggiungere un'origine dati che punta al filtro dei `/**/Data1` nodi, AWS IoT SiteWise in tempo reale, e un'altra fonte di dati che punta al `/**/Data2` AWS IoT SiteWise buffer utilizzando Amazon S3

11. Nel riquadro Configurazione avanzata, procedi come segue:

    a. Scegli una modalità di sicurezza dei messaggi per le connessioni e i dati in transito tra il server di origine e il gateway SiteWise Edge. Questo campo è la combinazione della politica di sicurezza OPC-UA e della modalità di sicurezza dei messaggi. Scegli la stessa politica di sicurezza e la stessa modalità di sicurezza dei messaggi che hai specificato per il tuo server OPC-UA.

    b. Se la tua fonte richiede l'autenticazione, scegli un AWS Secrets Manager segreto dall'elenco di configurazione dell'autenticazione. Il gateway SiteWise Edge utilizza le credenziali di autenticazione contenute in questo segreto quando si connette a questa fonte di dati. È necessario allegare segreti al AWS IoT Greengrass componente del gateway SiteWise Edge per utilizzarli per l'autenticazione delle fonti di dati. Per ulteriori informazioni, consulta the section called “Configurazione dell'autenticazione delle fonti di dati”.

    > **Tip**
    >
    > Il server di dati potrebbe disporre di un'opzione denominata Allow anonymous login (Consenti accesso anonimo). Se questa opzione è impostata su Yes (Sì), l'origine non richiede l'autenticazione.

    c. Per i gruppi di proprietà, scegli Aggiungi nuovo gruppo.

d. Inserisci un nome per il gruppo di proprietà.

e. Per le proprietà:

1. (Facoltativo) Per i percorsi dei nodi, aggiungi i filtri dei nodi OPC-UA per limitare i percorsi OPC-UA su cui vengono caricati. AWS IoT SiteWiseÈ possibile utilizzare i filtri dei nodi per ridurre il tempo di avvio e l'utilizzo della CPU del gateway SiteWise Edge includendo solo i percorsi dei dati utilizzati per la modellazione. AWS IoT SiteWise Per impostazione predefinita, i gateway SiteWise Edge caricano tutti i percorsi OPC-UA tranne quelli che iniziano con. `/Server/` Per definire i filtri dei nodi OPC-UA, è possibile utilizzare i percorsi dei nodi o i caratteri jolly `*` e `**`. Per ulteriori informazioni, consulta Utilizzo dei filtri dei nodi OPC-UA.

f. Per le impostazioni di gruppo, effettuate le seguenti operazioni:

1. (Facoltativo) Per l'impostazione della qualità dei dati, scegliete il tipo di qualità dei dati che desiderate che AWS IoT SiteWise Collector acquisisca.
2. (Facoltativo) Per l'impostazione della modalità di scansione, configurate le seguenti proprietà di abbonamento standard:
   - Per la modalità di scansione, scegli la modalità che desideri AWS IoT SiteWise utilizzare per raccogliere i dati. Per ulteriori informazioni sulla modalità di scansione, vederethe section called “Filtraggio degli intervalli di inserimento dei dati con OPC-UA”.
   - Avvio della modifica dei dati: è possibile definire la condizione che avvia un avviso di modifica dei dati.
   - Dimensione della coda di sottoscrizione: la profondità della coda su un server OPC-UA per una particolare metrica in cui vengono messe in coda le notifiche per gli elementi monitorati.
   - Intervallo di pubblicazione dell'abbonamento: l'intervallo (in millisecondi) del ciclo di pubblicazione specificato al momento della creazione dell'abbonamento.
   - Intervallo di istantanea: è possibile configurare l'impostazione del timeout della frequenza delle istantanee per garantire che Edge acquisisca un flusso costante di dati. AWS IoT SiteWise
   - Per la velocità di scansione, aggiorna la frequenza con cui desideri che il gateway SiteWise Edge legga i tuoi registri. AWS IoT SiteWise calcola automaticamente la velocità di scansione minima consentita per il SiteWise gateway Edge.
3. (Facoltativo) Configura un tipo di Deadband per la tua fonte. Questo controlla quali dati ti invia la AWS IoT SiteWise fonte e quali dati scarta. Per ulteriori informazioni

sull'impostazione della banda morta, consulta. the section called “Filtraggio degli intervalli di inserimento dei dati con OPC-UA”

g. Scegli Aggiungi.

12. Seleziona Successivo.

Configurazione di una sorgente OPC-UA (CLI)

È possibile definire sorgenti dati OPC-UA per un SiteWise gateway Edge utilizzando. AWS CLI A tale scopo, create un file JSON di configurazione della funzionalità OPC-UA e utilizzate il update-gateway-capability-configurationcomando per aggiornare la configurazione del gateway Edge. SiteWise Devi definire tutte le origini OPC-UA in un'unica configurazione della funzionalità.

Per ulteriori informazioni sulla definizione delle fonti con, vedere. AWS Command Line Interfacethe section called “Configurazione delle origini dati (AWS CLI)”

Questa funzionalità dispone delle versioni seguenti.

Versione	Spazio dei nomi
1	`iotsitewise:opcuacollector:1`

Sintassi della richiesta

```
{
  "sources": [
    {
      "name": "string",
      "endpoint": {
        "certificateTrust": {
          "type": "string"
          "certificateBody": "string"
          "certificateChain": "string"
        },
        "endpointUri": "string",
        "securityPolicy": "string",
        "messageSecurityMode": "string",
        "identityProvider": {
          "type": "string",
          "usernameSecretArn": "string"
```

```
        },
        "nodeFilterRules": [
          {
            "action": "string",
            "definition": {
              "type": "string",
              "rootPath": "string"
            }
          }
        ]
      },
      "measurementDataStreamPrefix": "string"
      "propertyGroups": [
      {
          "name": "string",
          "deadband": {
              "type":"string",
              "value": string,
              "eguMin": string,
              "eguMax": string,
              "timeoutMilliseconds": string
          },
          "scanMode": {
              "type": "string",
              "rate": string
          },
          "nodeFilterRuleDefinitions": [
              {
                  "type": "string",
                  "rootPath": "string"
              }
          ]
      }
    }
  ]
}
```

Corpo della richiesta

fonti

Un elenco delle strutture di definizione di origine OPC-UA che contengono le seguenti informazioni:

name

Un nome descrittivo univoco per l'origine.

endpoint

Una struttura endpoint contenente le seguenti informazioni:

Certificate Trust

Una struttura delle policy di attendibilità dei certificati contenente le seguenti informazioni:

tipo

La modalità di attendibilità dei certificati per l'origine. Seleziona una delle seguenti opzioni:

- **`TrustAny`**— Il gateway SiteWise Edge si fida di qualsiasi certificato quando si connette alla fonte OPC-UA.
- `X509`— Il gateway SiteWise Edge si fida di un certificato X.509 quando si connette alla fonte OPC-UA. Se si sceglie questa opzione, è necessario definire `certificateBody` in `certificateTrust`. È inoltre possibile definire `certificateChain` in `certificateTrust`.

Organismo del certificato

(Facoltativo) Il corpo di un certificato X.509.

Questo campo è obbligatorio se si sceglie `X509` per `type` in `certificateTrust`.

CertificateChain

(Facoltativo) La catena di attendibilità per un certificato X.509.

Questo campo viene utilizzato solo se si sceglie `X509` per `type` in `certificateTrust`.

URI dell'endpoint

L'endpoint locale dell'origine OPC-UA. Ad esempio, l'endpoint locale potrebbe essere simile a `opc.tcp://203.0.113.0:49320`.

Politica di sicurezza

La politica di sicurezza da utilizzare per proteggere i messaggi letti dalla fonte OPC-UA. Seleziona una delle seguenti opzioni:

- `NONE`— Il gateway SiteWise Edge non protegge i messaggi provenienti dalla fonte OPC-UA. Ti consigliamo di scegliere una politica di sicurezza diversa. Se si sceglie questa opzione, è necessario anche selezionare `NONE` per `messageSecurityMode`.
- `BASIC256_SHA256`— La politica `Basic256Sha256` di sicurezza.
- `AES128_SHA256_RSAOAEP`— La politica `Aes128_Sha256_RsaOaep` di sicurezza.
- `AES256_SHA256_RSAPSS`— La politica `Aes256_Sha256_RsaPss` di sicurezza.
- `BASIC128_RSA15`— (Obsoleta) La politica di `Basic128Rsa15` sicurezza è obsoleta nelle specifiche OPC-UA perché non è più considerata sicura. Ti consigliamo di scegliere una politica di sicurezza diversa. Per ulteriori informazioni, vedere Basic128Rsa15.
- `BASIC256`— (Obsoleto) La politica di `Basic256` sicurezza è obsoleta nelle specifiche OPC-UA perché non è più considerata sicura. Ti consigliamo di scegliere una politica di sicurezza diversa. Per ulteriori informazioni, consulta Basic256.

> **Important**
>
> Se si sceglie una politica di sicurezza diversa da`NONE`, è necessario scegliere `SIGN` o `SIGN_AND_ENCRYPT` per. `messageSecurityMode` È inoltre necessario configurare il server di origine in modo che consideri attendibile il gateway SiteWise Edge. Per ulteriori informazioni, consulta Consentire ai server di origine OPC-UA di affidarsi al SiteWise gateway Edge.

messageSecurityMode

La modalità di sicurezza dei messaggi da utilizzare per proteggere le connessioni all'origine OPC-UA. Seleziona una delle seguenti opzioni:

- `NONE`— Il gateway SiteWise Edge non protegge le connessioni alla sorgente OPC-UA. Ti consigliamo di scegliere una modalità di sicurezza dei messaggi diversa. Se si sceglie questa opzione, è necessario anche selezionare `NONE` per `securityPolicy`.
- `SIGN`— I dati in transito tra il gateway SiteWise Edge e la fonte OPC-UA sono firmati ma non crittografati.
- `SIGN_AND_ENCRYPT`— I dati in transito tra il gateway e la sorgente OPC-UA sono firmati e crittografati.

> **Important**
>
> Se si sceglie una modalità di sicurezza dei messaggi diversa da`NONE`, è necessario sceglierne una `securityPolicy` diversa. `NONE` È inoltre necessario configurare il server di origine in modo che consideri attendibile il gateway SiteWise Edge. Per ulteriori informazioni, consulta Consentire ai server di origine OPC-UA di affidarsi al SiteWise gateway Edge.

Provider di identità

Una struttura del provider di identità che contiene le seguenti informazioni:

tipo

Il tipo di credenziali di autenticazione richieste dall'origine. Seleziona una delle seguenti opzioni:

- `Anonymous`— La fonte non richiede l'autenticazione per la connessione.
- `Username`— L'origine richiede un nome utente e una password per la connessione. Se si sceglie questa opzione, è necessario definire `usernameSecretArn` in `identityProvider`.

usernameSecretArn

(Facoltativo) L'ARN di un AWS Secrets Manager segreto. Il gateway SiteWise Edge utilizza le credenziali di autenticazione contenute in questo segreto quando si connette a questa fonte. È necessario collegare segreti al SiteWise connettore IoT del gateway SiteWise Edge per utilizzarli per l'autenticazione dell'origine. Per ulteriori informazioni, consulta Configurazione dell'autenticazione delle fonti di dati.

Questo campo è obbligatorio se si sceglie `Username` per `type` in `identityProvider`.

nodeFilterRules

Un elenco di strutture di regole di filtro dei nodi che definiscono i percorsi del flusso di dati OPC-UA da inviare al AWS Cloud. Puoi utilizzare i filtri dei nodi per ridurre il tempo di avvio e l'utilizzo della CPU del gateway SiteWise Edge includendo solo i percorsi dei dati in cui esegui il modello. AWS IoT SiteWise Per impostazione predefinita, i gateway SiteWise Edge caricano tutti i percorsi OPC-UA tranne quelli che iniziano con. `/Server/`

Per definire i filtri dei nodi OPC-UA, è possibile utilizzare i percorsi dei nodi o i caratteri jolly `*` e `**`. Per ulteriori informazioni, consulta Utilizzo dei filtri dei nodi OPC-UA.

Ogni struttura dell'elenco deve contenere le seguenti informazioni:

action

L'operazione per questa regola di filtro dei nodi. Puoi scegliere le seguenti opzioni:

- `INCLUDE`— Il gateway SiteWise Edge include solo flussi di dati che soddisfano questa regola.

definizione

Una struttura di regole del filtro dei nodi che contiene le seguenti informazioni:

tipo

Il tipo di percorso del filtro dei nodi per questa regola. Puoi scegliere le seguenti opzioni:

- `OpcUaRootPath`— Il gateway SiteWise Edge valuta questo percorso di filtro del nodo rispetto alla radice della gerarchia dei percorsi OPC-UA.

RootPath

Il percorso del filtro dei nodi da valutare rispetto alla radice della gerarchia dei percorsi OPC-UA. Questo percorso deve iniziare con. `/`

measurementDataStreamPrefisso

Una stringa da aggiungere a tutti i flussi di dati dalla fonte. Il gateway SiteWise Edge aggiunge questo prefisso a tutti i flussi di dati provenienti da questa fonte. Utilizzare un prefisso del flusso di dati per distinguere tra flussi di dati con lo stesso nome da origini diverse. Ogni flusso di dati deve avere un nome univoco all'interno del tuo account.

Gruppi di proprietà

(Facoltativo) L'elenco dei gruppi di proprietà che definiscono `deadband` e `scanMode` richiesti dal protocollo.

name

Il nome del gruppo di proprietà. Dovrebbe essere un identificatore univoco.

zona morta

La `deadband` struttura che contiene le seguenti informazioni:

tipo

I tipi di banda morta supportati. I valori accettati sono `ABSOLUTE` e. `PERCENT`

value

Il valore della banda morta. Quando `type` è`ABSOLUTE`, questo valore è un doppio senza unità. Quando `type` è`PERCENT`, questo valore è un doppio tra `1` e`100`.

eGumin

(Facoltativo) L'unità tecnica minima quando si utilizza una `PERCENT` banda morta. Si imposta questa impostazione se il server OPC-UA non ha unità tecniche configurate.

EguMax

(Opzionale) Il numero massimo dell'unità tecnica quando si utilizza una banda `PERCENT` morta. Si imposta questa impostazione se il server OPC-UA non ha unità tecniche configurate.

Timeout (millisecondi)

La durata in millisecondi prima del timeout. Il valore minimo è. `100`

Modalità di scansione

La `scanMode` struttura che contiene le seguenti informazioni:

tipo

I tipi supportati di`scanMode`. I valori accettati sono `POLL` e`EXCEPTION`.

tasso

L'intervallo di campionamento per la modalità di scansione.

nodeFilterRuleDefinizioni

(Facoltativo) Un elenco di percorsi di nodi da includere nel gruppo di proprietà. I gruppi di proprietà non possono sovrapporsi. Se non si specifica un valore per questo campo, il gruppo contiene tutti i percorsi sotto la radice e non è possibile creare gruppi di proprietà aggiuntivi. La struttura `nodeFilterRuleDefinitions` contiene le seguenti informazioni:

tipo

`OpcUaRootPath`è l'unico tipo supportato. Ciò specifica che il valore di `rootPath` è un percorso relativo alla radice dello spazio di navigazione OPC-UA.

RootPath

Un elenco delimitato da virgole che specifica i percorsi (relativi alla radice) da includere nel gruppo di proprietà.

Esempi di configurazione della funzionalità

L'esempio seguente definisce una configurazione della funzionalità del gateway OPC-UA SiteWise Edge da un payload archiviato in un file JSON.

```
aws iotsitewise update-gateway-capability-configuration \
--capability-namespace "iotsitewise:opcuacollector:1" \
--capability-configuration file://opc-ua-configuration.json
```

Example : configurazione del codice sorgente OPC-UA

Il `opc-ua-configuration.json` file seguente definisce una configurazione sorgente OPC-UA di base e non sicura.

```
{
"sources": [
  {
    "name": "Wind Farm #1",
    "endpoint": {
      "certificateTrust": {
        "type": "TrustAny"
      },
      "endpointUri": "opc.tcp://203.0.113.0:49320",
      "securityPolicy": "NONE",
      "messageSecurityMode": "NONE",
      "identityProvider": {
        "type": "Anonymous"
      },
      "nodeFilterRules": []
    },
    "measurementDataStreamPrefix": ""
  }
]
}
```

Example : configurazione del codice sorgente OPC-UA con gruppi di proprietà definiti

Il `opc-ua-configuration.json` file seguente definisce una configurazione di origine OPC-UA di base e non sicura con gruppi di proprietà definiti.

```
{
  "sources": [
      {
          "name": "source1",
          "endpoint": {
              "certificateTrust": {
                  "type": "TrustAny"
              },
              "endpointUri": "opc.tcp://10.0.0.9:49320",
              "securityPolicy": "NONE",
              "messageSecurityMode": "NONE",
              "identityProvider": {
                  "type": "Anonymous"
              },
              "nodeFilterRules": [
                  {
                      "action": "INCLUDE",
                      "definition": {
                          "type": "OpcUaRootPath",
                          "rootPath": "/Utilities/Tank"
                      }
                  }
              ]
          },
          "measurementDataStreamPrefix": "propertyGroups",
         "propertyGroups": [

              {
                  "name": "Deadband_Abs_5",
                  "nodeFilterRuleDefinitions": [
                      {
                          "type": "OpcUaRootPath",
                          "rootPath": "/Utilities/Tank/Temperature/TT-001"
                      },
                      {
                          "type": "OpcUaRootPath",
                          "rootPath": "/Utilities/Tank/Temperature/TT-002"
                      }
                  ],
```

```
                "deadband": {
                    "type":"ABSOLUTE",
                    "value": 5.0,
                    "timeoutMilliseconds": 120000
                }
            },
            {
                "name": "Polling_10s",
                "nodeFilterRuleDefinitions": [
                    {
                        "type": "OpcUaRootPath",
                        "rootPath": "/Utilities/Tank/Pressure/PT-001"
                    }
                ],
                "scanMode": {
                    "type": "POLL",
                    "rate": 10000
                }
            },
            {
                "name": "Percent_Deadband_Timeout_90s",
                "nodeFilterRuleDefinitions": [
                    {
                        "type": "OpcUaRootPath",
                        "rootPath": "/Utilities/Tank/Flow/FT-*"
                    }
                ],
                "deadband": {
                    "type":"PERCENT",
                    "value": 5.0,
                    "eguMin": -100,
                    "eguMax": 100,
                    "timeoutMilliseconds": 90000
                }
            }
        ]
    }
  ]
}
```

Example : configurazione del codice sorgente OPC-UA con proprietà

L'esempio JSON seguente per `opc-ua-configuration.json` definisce una configurazione di origine OPC-UA con le seguenti proprietà:

- Considera attendibile qualsiasi certificato.
- Utilizza la politica `BASIC256` di sicurezza per proteggere i messaggi.
- Usa la modalità `SIGN_AND_ENCRYPT` per proteggere le connessioni.
- Utilizza le credenziali di autenticazione memorizzate in un segreto di Secrets Manager.
- Filtra i flussi di dati tranne quelli il cui percorso inizia con `/WindFarm/2/WindTurbine/`.
- Aggiunge `/Washington` all'inizio di ogni percorso del flusso di dati per distinguere tra questo "Parco eolico #2" e un "Parco eolico #2" in un'altra area.

```
{
"sources": [
  {
    "name": "Wind Farm #2",
    "endpoint": {
      "certificateTrust": {
        "type": "TrustAny"
      },
      "endpointUri": "opc.tcp://203.0.113.1:49320",
      "securityPolicy": "BASIC256",
      "messageSecurityMode": "SIGN_AND_ENCRYPT",
      "identityProvider": {
        "type": "Username",
        "usernameSecretArn":
 "arn:aws:secretsmanager:region:123456789012:secret:greengrass-windfarm2-auth-1ABCDE"
      },
      "nodeFilterRules": [
        {
          "action": "INCLUDE",
          "definition": {
            "type": "OpcUaRootPath",
            "rootPath": "/WindFarm/2/WindTurbine/"
          }
        }
      ]
    },
    "measurementDataStreamPrefix": "/Washington"
```

```
  }
]
}
```

Example

L'esempio JSON seguente per `opc-ua-configuration.json` definisce una configurazione di origine OPC-UA con le seguenti proprietà:

- Considera attendibile un determinato certificato X.509.
- Utilizza la politica `BASIC256` di sicurezza per proteggere i messaggi.
- Usa la modalità `SIGN_AND_ENCRYPT` per proteggere le connessioni.

```
{
"sources": [
  {
    "name": "Wind Farm #3",
    "endpoint": {
      "certificateTrust": {
        "type": "X509",
        "certificateBody": "-----BEGIN CERTIFICATE-----
MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w
 0BAQUFADCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZ
 WF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIw
 EAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5
 jb20wHhcNMTEwNDI1MjA0NTIxWhcNMTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBh
 MCVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBb
 WF6b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMx
 HzAdBgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wgZ8wDQYJKoZIhvcNAQE
 BBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ21uUSfwfEvySWtC2XADZ4nB+BLYgVI
 k60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9TrDHudUZg3qX4waLG5M43q7Wgc/MbQ
 ITxOUSQv7c7ugFFDzQGBzZswY6786m86gpEIbb3OhjZnzcvQAaRHhdlQWIMm2nr
 AgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4nUhVVxYUntneD9+h8Mg9q6q+auN
 KyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0FkbFFBjvSfpJIlJ00zbhNYS5f6Guo
 EDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTbNYiytVbZPQUQ5Yaxu2jXnimvw
 3rrszlaEXAMPLE=
-----END CERTIFICATE-----",
        "certificateChain": "-----BEGIN CERTIFICATE-----
MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w
 0BAQUFADCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZ
 WF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIw
```

```
 EAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5
 jb20wHhcNMTEwNDI1MjA0NTIxWhcNMTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBh
 MCVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBb
 WF6b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMx
 HzAdBgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wgZ8wDQYJKoZIhvcNAQE
 BBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ21uUSfwfEvySWtC2XADZ4nB+BLYgVI
 k60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9TrDHudUZg3qX4waLG5M43q7Wgc/MbQ
 ITxOUSQv7c7ugFFDzQGBzZswY6786m86gpEIbb3OhjZnzcvQAaRHhdlQWIMm2nr
 AgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4nUhVVxYUntneD9+h8Mg9q6q+auN
 KyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0FkbFFBjvSfpJIlJ00zbhNYS5f6Guo
 EDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTbNYiytVbZPQUQ5Yaxu2jXnimvw
 3rrszlaEXAMPLE=
-----END CERTIFICATE-----"
      },
      "endpointUri": "opc.tcp://203.0.113.2:49320",
      "securityPolicy": "BASIC256",
      "messageSecurityMode": "SIGN_AND_ENCRYPT",
      "identityProvider": {
        "type": "Anonymous"
      },
      "nodeFilterRules": []
    },
    "measurementDataStreamPrefix": ""
  }
]
}
```

Consentire ai server di origine OPC-UA di affidarsi al SiteWise gateway Edge

Se si sceglie un valore `messageSecurityMode` diverso da Nessuno durante la configurazione della sorgente OPC-UA, è necessario consentire ai server di origine di considerare attendibile il gateway Edge. AWS IoT SiteWise Il gateway SiteWise Edge genera un certificato che il server di origine potrebbe richiedere. Il processo varia a seconda dei server di origine. Per ulteriori informazioni, consulta la documentazione relativa ai server in uso.

La procedura seguente descrive i passaggi di base.

Per consentire a un server OPC-UA di considerare attendibile il gateway Edge SiteWise

1. Apri l'interfaccia per configurare il tuo server OPC-UA.
2. Immettere il nome utente e la password dell'amministratore del server OPC-UA.
3. Individua Trusted Clients nell'interfaccia, quindi scegli AWS IoT SiteWise Gateway Client.

4. Scegliere Trust (Considera attendibile).

Esportazione del certificato client OPC-UA

Alcuni server OPC-UA richiedono l'accesso al file di certificato del client OPC-UA per considerare attendibili il gateway Edge. SiteWise Se ciò si applica ai server OPC-UA, è possibile utilizzare la seguente procedura per esportare il certificato client OPC-UA dal gateway Edge. SiteWise Quindi, è possibile importare il certificato sul server OPC-UA.

Per esportare il file del certificato client OPC-UA per un'origine

1. Eseguire il comando seguente per passare alla directory che contiene il file del certificato. *Sostituisci sitewise-work con il percorso di archiviazione locale per aws.iot. SiteWiseEdgeCollectorOpcua*Cartella di lavoro Greengrass e sostituisci *source-name con il nome* dell'origine dati.

   *Per impostazione predefinita, la cartella di lavoro di Greengrass è / greengrass/v2/work/aws.iot. SiteWiseEdgeCollectorOpcua*su Linux e *C: / greengrass/v2/work/aws.iot. SiteWiseEdgeCollectorOpcua*su Windows.

   ```
   cd /sitewise-work/source-name/opcua-certificate-store
   ```

2. Il certificato client OPC-UA del gateway SiteWise Edge per questa fonte è nel `aws-iot-opcua-client.pfx` file.

   Eseguire il comando seguente per esportare il certificato in un file `.pem` chiamato `aws-iot-opcua-client-certificate.pem`.

   ```
   keytool -exportcert -v -alias aws-iot-opcua-client -keystore aws-iot-opcua-
   client.pfx -storepass amazon -storetype PKCS12 -rfc > aws-iot-opcua-client-
   certificate.pem
   ```

3. Trasferisci il file del certificato dal gateway SiteWise Edge al server OPC-UA. `aws-iot-opcua-client-certificate.pem`

   Per fare ciò, è possibile utilizzare software comuni come il programma `scp` per trasferire il file utilizzando il protocollo SSH. Per ulteriori informazioni, consultare la pagina Secure copy su Wikipedia.

> **Note**
>
> Se il tuo SiteWise Edge gateway è in esecuzione su Amazon Elastic Compute Cloud (Amazon EC2) e ti connetti ad esso per la prima volta, devi configurare i prerequisiti per la connessione. Per ulteriori informazioni, consulta Connessione a un'istanza Linux nella Guida per l'utente di Amazon EC2 per le istanze Linux.

4. Importa il file del certificato sul server OPC-UA per considerare attendibile il gateway Edge. `aws-iot-opcua-client-certificate.pem` SiteWise Le fasi variano a seconda dei server di origine in uso. Consultare la documentazione relativa al server.

Filtra gli intervalli di inserimento dei dati con OPC-UA

È possibile controllare il modo in cui si inseriscono i dati con una fonte OPC-UA utilizzando la modalità di scansione e gli intervalli di banda morta. Queste funzionalità consentono di controllare il tipo di dati da importare e come e quando il server e il gateway SiteWise Edge si scambiano queste informazioni.

Controlla la frequenza di raccolta dei dati con la modalità Scan

È possibile configurare la modalità di scansione OPC-UA per controllare il modo in cui si raccolgono i dati dalla fonte OPC-UA. Puoi scegliere la modalità di abbonamento o di sondaggio.

- Modalità di abbonamento: la fonte OPC-UA raccoglie i dati da inviare al gateway SiteWise Edge alla frequenza definita dalla velocità di scansione. Il server invia i dati solo quando il valore è cambiato, quindi questa è la frequenza massima di ricezione dei dati del gateway SiteWise Edge.
- Modalità polling: il gateway SiteWise Edge esegue il polling della sorgente OPC-UA a una frequenza prestabilita definita dalla velocità di scansione. Il server invia i dati indipendentemente dal fatto che il valore sia cambiato, quindi il gateway SiteWise Edge riceve sempre i dati a questo intervallo.

> **Note**
>
> L'opzione della modalità polling ha la precedenza sulle impostazioni della banda morta per questa fonte.

Filtra l'ingestione di dati OPC-UA con intervalli di banda morta

Puoi applicare una banda morta ai tuoi gruppi di proprietà di origine OPC-UA per filtrare ed eliminare determinati dati invece di inviarli al Cloud. AWS Una banda morta specifica una finestra di fluttuazioni previste nei valori dei dati in entrata dalla fonte OPC-UA. Se i valori rientrano in questa finestra, il server OPC-UA non li invierà al Cloud. AWS Puoi utilizzare il filtro a banda morta per ridurre la quantità di dati che stai elaborando e inviando al Cloud. AWS Per informazioni su come configurare le sorgenti OPC-UA per il gateway SiteWise Edge, consulta. the section called “Configurazione delle origini dati”

> **Note**
>
> Il server elimina tutti i dati che rientrano nella finestra specificata dalla banda morta. Non puoi recuperare questi dati scartati.

Tipi di zone morte

È possibile specificare due tipi di bande morte per il gruppo di proprietà del server OPC-UA. Questi consentono di scegliere la quantità di dati da inviare al AWS Cloud e la quantità da scartare.

- Percentuale: si specifica una finestra utilizzando una percentuale della fluttuazione prevista nel valore di misurazione. Il server calcola la finestra esatta in base a questa percentuale e invia al AWS Cloud i dati che superano i limiti della finestra. Ad esempio, specificando un valore di banda morta del 2% su un sensore con un intervallo compreso tra -100 gradi Fahrenheit e +100 gradi Fahrenheit, si indica al server di inviare dati al Cloud quando il valore cambia di 4 gradi Fahrenheit o più. AWS

  > **Note**
  >
  > Facoltativamente, puoi specificare un valore di banda morta minimo e massimo per questa finestra se il server di origine non definisce le unità tecniche. Se non viene fornito un intervallo di unità tecniche, il server OPC-UA utilizza per impostazione predefinita l'intervallo completo del tipo di dati di misurazione.

- Assoluto: si specifica una finestra utilizzando unità esatte. Ad esempio, se si specifica un valore di banda morta pari a 2 su un sensore, si indica al server di inviare dati al AWS Cloud quando il loro valore cambia di almeno 2 unità. È possibile utilizzare la banda morta assoluta per ambienti dinamici in cui sono regolarmente previste fluttuazioni durante le normali operazioni.

Timeout con banda morta

Facoltativamente, puoi configurare un'impostazione di timeout per la banda morta. Dopo questo timeout, il server OPC-UA invia il valore di misurazione corrente anche se rientra nella fluttuazione prevista della banda morta. È possibile utilizzare l'impostazione del timeout per garantire AWS IoT SiteWise l'acquisizione di un flusso costante di dati in ogni momento, anche quando i valori non superano la finestra di banda morta definita.

Utilizzo dei filtri dei nodi OPC-UA

Quando si definiscono le sorgenti dati OPC-UA per un gateway SiteWise Edge, è possibile definire filtri di nodo. I filtri dei nodi consentono di limitare i percorsi del flusso di dati che il gateway SiteWise Edge invia al cloud. Puoi utilizzare i filtri dei nodi per ridurre il tempo di avvio e l'utilizzo della CPU del gateway SiteWise Edge includendo solo i percorsi dei dati utilizzati per la modellazione AWS IoT SiteWise. Per impostazione predefinita, i gateway SiteWise Edge caricano tutti i percorsi OPC-UA tranne quelli che iniziano con. `/Server/` È possibile utilizzare i caratteri jolly `*` e `**` nei filtri dei nodi per includere più percorsi dei flussi di dati con un solo filtro. Per informazioni su come configurare le sorgenti OPC-UA per il SiteWise gateway Edge, consulta. Configurazione delle origini dati

> **Note**
>
> AWS IoT SiteWise riavvia il gateway SiteWise Edge ogni volta che aggiungi o modifichi una fonte. Il gateway SiteWise Edge non inserirà dati durante il riavvio. Il tempo necessario per riavviare il gateway SiteWise Edge dipende dal numero di tag presenti nelle sorgenti del gateway SiteWise Edge. Il tempo di riavvio può variare da pochi secondi (per un gateway SiteWise Edge con pochi tag) a diversi minuti (per un gateway SiteWise Edge con molti tag).

Nella tabella seguente sono elencati i caratteri jolly che è possibile utilizzare per filtrare le origini dati OPC-UA.

Caratteri jolly dei filtri dei nodi OPC-UA

Carattere jolly	Descrizione
*	Corrisponde a un singolo livello in un percorso dei flussi di dati.

Carattere jolly	Descrizione
**	Corrisponde a più livelli in un percorso dei flussi di dati.

> **Note**
>
> Se configuri una fonte con un filtro ampio e successivamente modifichi la fonte per utilizzare un filtro più restrittivo, AWS IoT SiteWise interrompe l'archiviazione dei dati che non corrispondono al nuovo filtro.

Example Scenario di esempio utilizzando i filtri dei nodi

Quelli che seguono sono ipotetici flussi di dati:

- `/WA/Factory 1/Line 1/PLC1`
- `/WA/Factory 1/Line 1/PLC2`
- `/WA/Factory 1/Line 2/Counter1`
- `/WA/Factory 1/Line 2/PLC1`
- `/OR/Factory 1/Line 1/PLC1`
- `/OR/Factory 1/Line 2/Counter2`

Utilizzando i flussi di dati precedenti, è possibile definire i filtri dei nodi per limitare i dati dell'origine OPC-UA da includere.

- Per selezionare tutti i nodi in questo esempio, usa `/` o`/**/`. È possibile includere più directory o cartelle con i caratteri jolly `**`.
- Per selezionare tutti i flussi di dati `PLC`, si possono utilizzare i caratteri `/*/*/*/PLC*` o `/**/PLC*`.
- Per selezionare tutti i contatori in questo esempio, utilizzate `/**/Counter*` o`/*/*/*/Counter*`.
- Per selezionare tutti i contatori da `Line 2`, utilizzare `/**/Line 2/Counter*`.

Configurazione dell'autenticazione delle fonti di dati

Se il server OPC-UA richiede credenziali di autenticazione per la connessione, è possibile utilizzarle AWS Secrets Manager per creare e distribuire un segreto sul gateway Edge. SiteWise AWS Secrets Manager crittografa i segreti sul dispositivo per proteggere il nome utente e la password finché non è necessario utilizzarli. Per ulteriori informazioni, consulta Secret manager nella AWS IoT Greengrass Version 2 Developer Guide.

Fase 1: Creare segreti di autenticazione all'origine

Puoi utilizzarlo AWS Secrets Manager per creare un segreto di autenticazione per la tua fonte di dati. Nel campo segreto, definisci **`username`** coppie **`password`** chiave-valore che contengono i dettagli di autenticazione per la tua fonte di dati.

Creazione di un segreto (console)

1. Passare alla console AWS Secrets Manager.
2. Scegli Archivia un nuovo segreto.
3. In Tipo segreto, scegli Altro tipo di segreti.
4. In Coppie chiave/valore, procedi come segue:
    1. Nella prima casella di immissione, immettete **`username`** e nella seconda casella di immissione inserite il nome utente.
    2. Scegli Aggiungi riga.
    3. Nella prima casella di immissione, inserisci **`password`** e nella seconda casella di immissione inserisci la password.
5. Per la chiave di crittografia, seleziona aws/secretsmanager, quindi scegli Avanti.
6. Nella pagina Salva una nuova pagina segreta, inserisci un nome segreto.
7. (Facoltativo) Inserisci una descrizione che ti aiuti a identificare questo segreto, quindi scegli Avanti.
8. (Facoltativo) In Memorizza una nuova pagina segreta, attiva Rotazione automatica. Per ulteriori informazioni, consulta Ruotare i segreti nella Guida per l'AWS Secrets Manager utente.
9. Specificate un programma di rotazione.
10. Scegli una funzione Lambda in grado di ruotare questo segreto, quindi scegli Avanti.
11. Controlla le configurazioni segrete, quindi scegli Store.

Per autorizzare l'interazione con il gateway SiteWise Edge AWS Secrets Manager, il ruolo IAM del gateway SiteWise Edge deve consentire l'azione`secretsmanager:GetSecretValue`. Puoi utilizzare il dispositivo principale Greengrass per cercare la policy IAM. Per ulteriori informazioni sull'aggiornamento di una policy IAM, consulta Modifica delle policy IAM nella Guida per l'AWS Identity and Access Management utente.

Example policy

Sostituisci *`secret-arn`* con l'Amazon Resource Name (ARN) del segreto creato nel passaggio precedente. Per ulteriori informazioni su come ottenere l'ARN di un segreto, consulta Recupera il segreto da AWS Secrets Manager nella Guida per l'AWS Secrets Manager utente.

```
{
"Version":"2012-10-17",
"Statement":[
  {
     "Action":[
        "secretsmanager:GetSecretValue"
     ],
     "Effect":"Allow",
     "Resource":[
        "secret-arn"
     ]
  }
]
}
```

Passaggio 2: distribuisci i segreti sul tuo SiteWise dispositivo gateway Edge

Puoi utilizzare la AWS IoT SiteWise console per distribuire segreti sul tuo gateway SiteWise Edge.

Per distribuire un segreto (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegliere Gateways.
3. Dall'elenco dei gateway, scegli il gateway SiteWise Edge di destinazione.
4. Nella sezione Configurazione del gateway, scegli il collegamento del dispositivo principale Greengrass per aprire il AWS IoT Greengrass core associato al gateway SiteWise Edge.
5. Nel riquadro di navigazione, scegli Implementazioni.
6. Scegli la distribuzione di destinazione, quindi scegli Rivedi.

7. Nella pagina Specificare la destinazione, scegli Avanti.
8. Nella pagina Seleziona componenti, nella sezione Componenti pubblici, disattiva Mostra solo i componenti selezionati.
9. Cerca e scegli aws.greengrass. SecretManagercomponente, quindi scegli Avanti.
10. Dall'elenco Componenti selezionati, scegli aws.greengrass. SecretManagercomponente, quindi scegli Configura componente.
11. Nel campo Configurazione da unire, aggiungi il seguente oggetto JSON.

> **Note**
>
> Sostituisci *secret-arn* con l'ARN del segreto creato nel passaggio precedente. Per ulteriori informazioni su come ottenere l'ARN di un segreto, consulta Recupera il segreto da AWS Secrets Manager nella Guida per l'AWS Secrets Manager utente.

```
{
"cloudSecrets":[
  {
     "arn":"secret-arn"
  }
]
}
```

12. Scegli Conferma.
13. Seleziona Successivo.
14. Nella pagina Configura impostazioni avanzate, scegli Avanti.
15. Esamina le configurazioni di distribuzione, quindi scegli Distribuisci.

Fase 3: Aggiungere configurazioni di autenticazione

È possibile utilizzare la AWS IoT SiteWise console per aggiungere configurazioni di autenticazione al gateway SiteWise Edge.

Per aggiungere configurazioni di autenticazione (console)

1. Passare alla console AWS IoT SiteWise.
2. Dall'elenco dei gateway, scegli il gateway SiteWise Edge di destinazione.

3. Dall'elenco Sorgenti dati, scegli l'origine dati di destinazione, quindi scegli Modifica.
4. Nella pagina Aggiungi un'origine dati, scegli Configurazione avanzata.
5. Per la configurazione dell'autenticazione, scegli il segreto che hai distribuito nel passaggio precedente.
6. Selezionare Salva.

Configurazione delle origini dati (AWS CLI)

Puoi utilizzare l' AWS IoT SiteWise API e aggiungere fonti AWS Command Line Interface al tuo gateway AWS IoT SiteWise Edge. Le fonti vengono definite nelle funzionalità SiteWise del gateway Edge. Una funzionalità SiteWise Edge gateway rappresenta una funzionalità software che viene eseguita sul gateway SiteWise Edge, ad esempio la capacità di raccogliere dati industriali da fonti OPC-UA.

SiteWise Le funzionalità del gateway Edge hanno i seguenti componenti:

- Una configurazione: un documento JSON che definisce tutte le fonti di dati per una funzionalità.
- Un namespace: una stringa univoca che identifica il tipo e la versione di una funzionalità. Ad esempio, lo spazio dei nomi della funzionalità di origine OPC-UA è `iotsitewise:opcuacollector:`*`version`*, dove *`versione`* indica la versione della funzionalità OPC-UA. Tutte le origini OPC-UA sono definite in un'unica funzionalità con questo spazio dei nomi.
- Uno stato di sincronizzazione: uno stato che indica se una funzionalità è sincronizzata tra il AWS cloud e il gateway Edge. SiteWise Lo stato di sincronizzazione può essere uno dei seguenti:
  - `IN_SYNC`— Il gateway SiteWise Edge esegue la configurazione delle funzionalità.
  - `OUT_OF_SYNC`— Il gateway SiteWise Edge non ha ricevuto la configurazione delle funzionalità.
  - `SYNC_FAILED`— Il gateway SiteWise Edge ha rifiutato la configurazione della funzionalità.

  Dopo aver aggiornato una configurazione di funzionalità, il relativo stato di sincronizzazione è valido `OUT_OF_SYNC` fino a quando il gateway SiteWise Edge non riceve e applica o rifiuta la configurazione aggiornata.

Utilizza le seguenti operazioni per interrogare e aggiornare le sorgenti e le configurazioni delle funzionalità del gateway SiteWise Edge:

- DescribeGateway— Recupera informazioni su un gateway SiteWise Edge specifico. La risposta include un elenco di riepiloghi delle funzionalità, inclusi gli spazi dei nomi delle funzionalità.

- DescribeGatewayCapabilityConfiguration— Recupera la configurazione di una funzionalità specifica. Utilizzare questa operazione per recuperare una configurazione delle funzionalità da aggiornare.
- ListGateways— Elenca le informazioni su tutti i gateway SiteWise Edge. La risposta include un elenco di riepiloghi delle funzionalità per ogni gateway SiteWise Edge, inclusi i namespace delle funzionalità.
- UpdateGatewayCapabilityConfiguration— Aggiorna la configurazione di funzionalità di un gateway SiteWise Edge o definisce una nuova configurazione di funzionalità. Questa operazione identifica le funzionalità mediante uno spazio dei nomi delle funzionalità. Se fornisci uno spazio dei nomi già esistente, questa operazione aggiorna la funzionalità di tale spazio dei nomi. In caso contrario, questa operazione crea una nuova funzionalità.

> **Warning**
>
> L'UpdateGatewayCapabilityConfigurationoperazione sovrascrive la configurazione di funzionalità esistente con la configurazione fornita nel payload. Per evitare che la configurazione della funzionalità veNga eliminata, è necessario aggiungerla alla configurazione esistente quando si aggiorna la funzionalità.

SiteWise Funzionalità Edge Gateway

- ???
- ???
- ???

Scelta di una destinazione per i dati del server di origine

I dati vengono esportati dall'edge AWS IoT SiteWise in tempo reale o in batch utilizzando Amazon S3. Puoi anche inviare lo stream a un altro componente utilizzando uno stream. AWS IoT Greengrass

- AWS IoT SiteWise in tempo reale: scegli questa opzione per inviare i dati direttamente allo AWS IoT SiteWise storage. Acquisisci e monitora i dati in tempo reale ed elabora i dati all'edge.
- AWS IoT SiteWise Memorizzato nel buffer con Amazon S3: invia dati in formato parquet ad Amazon S3 e quindi importali nello storage. AWS IoT SiteWise Scegli questa opzione per importare i dati in batch e archiviare i dati storici in modo conveniente. Puoi configurare la posizione

preferita del bucket Amazon S3 e la frequenza con cui desideri che i dati vengano caricati su Amazon S3. Puoi anche scegliere cosa fare con i dati dopo l'ingestione. AWS IoT SiteWise Puoi scegliere di rendere i dati disponibili sia SiteWise in Amazon S3 che in Amazon S3 oppure puoi scegliere di eliminarli automaticamente da Amazon S3.

- Il bucket Amazon S3 è un meccanismo di staging e buffering e supporta file in formato parquet.
- Se selezioni la casella di controllo Importa dati nello AWS IoT SiteWise storage, i dati vengono caricati prima in Amazon S3 e poi nello AWS IoT SiteWise storage.
  - Se selezioni la casella di controllo Elimina dati da Amazon S3, i dati vengono eliminati da Amazon S3 dopo essere stati importati nello storage. SiteWise
  - Se deselezioni la casella di controllo Elimina dati da Amazon S3, i dati vengono archiviati sia in Amazon S3 che in storage. SiteWise
- Se deselezioni la casella di controllo Importa dati nello AWS IoT SiteWise storage, i dati vengono archiviati solo in Amazon S3. Non viene importato nello SiteWise storage.

Visita Gestione dell'archiviazione dei dati per i dettagli sulle varie opzioni di archiviazione AWS IoT SiteWise offerte. Per ulteriori informazioni sulle opzioni di prezzo, consulta la pagina AWS IoT SiteWise dei prezzi.

- AWS IoT Greengrass stream manager: utilizza AWS IoT Greengrass stream manager per inviare dati alle seguenti Cloud AWS destinazioni: canali in ingresso AWS IoT Analytics, flussi in Amazon Kinesis Data Streams, proprietà degli asset o oggetti AWS IoT SiteWise in Amazon Simple Storage Service (Amazon S3). Per ulteriori informazioni, consulta Manage data stream on the AWS IoT Greengrass Core nella Developer Guide.AWS IoT Greengrass Version 2

L'esempio seguente mostra la struttura dei messaggi del flusso di dati richiesta. Tutti i campi sono obbligatori.

```
{
    "assetId": "string",
    "propertyAlias": "string",
    "propertyId": "string",
    "propertyValues": [
      {
         "quality": "string",
         "timestamp": {
            "offsetInNanos": number,
            "timeInSeconds": number
```

```
         },
         "value": {
            "booleanValue": boolean,
            "doubleValue": number,
            "integerValue": number,
            "stringValue": "string"
         }
      }
   ]
}
```

> **Note**
>
> Il messaggio del flusso di dati deve includere (`assetIdepropertyId`) o `propertyAlias` nella sua struttura.

`assetId`

(Facoltativo) L'ID della risorsa da aggiornare.

`propertyAlias`

(Facoltativo) L'alias che identifica la proprietà, ad esempio il percorso del flusso di dati del server OPC-UA. Per esempio:

```
/company/windfarm/3/turbine/7/temperature
```

Per ulteriori informazioni, consulta Mappatura dei flussi di dati industriali alle proprietà degli asset nella Guida per l'utente.AWS IoT SiteWise

`propertyId`

(Facoltativo) L'ID della proprietà dell'asset per questa voce.

`propertyValues`

(Obbligatorio) L'elenco dei valori delle proprietà da caricare. È possibile specificare fino a 10 elementi `propertyValues` dell'array.

`quality`

(Facoltativo) La qualità del valore della proprietà dell'asset.

`timestamp`

(Obbligatorio) Il timestamp del valore della proprietà dell'asset.

`offsetInNanos`

(Facoltativo) L'offset in nanosecondi da. `timeInSeconds`

`timeInSeconds`

(Obbligatorio) La data del timestamp, in secondi, nel formato Unix epoch. I dati frazionari in nanosecondi sono forniti da. `offsetInNanos`

`value`

(Obbligatorio) Il valore della proprietà dell'asset.

> **Note**
>
> Nel `value` campo può esistere solo uno dei seguenti valori.

`booleanValue`

(Facoltativo) Dati della proprietà Asset di tipo Boolean (`true`or`false`).

`doubleValue`

(Facoltativo) Dati relativi alla proprietà dell'asset di tipo double (numero a virgola mobile).

`integerValue`

(Facoltativo) Dati relativi alla proprietà dell'asset di tipo intero (numero intero).

`stringValue`

(Facoltativo) Dati delle proprietà dell'asset di tipo string (sequenza di caratteri).

Aggiungere fonti di dati dei partner ai gateway SiteWise Edge

Quando si utilizza un gateway AWS IoT SiteWise Edge, è possibile connettere una fonte di dati partner al gateway SiteWise Edge e ricevere dati dal partner nel gateway SiteWise Edge e nel

AWS cloud. Queste fonti di dati dei partner sono AWS IoT Greengrass componenti sviluppati in collaborazione tra AWS e il partner. Quando aggiungi una fonte di dati partner, AWS IoT SiteWise creerà questo componente e lo distribuirà sul tuo gateway SiteWise Edge.

Per aggiungere un'origine dati partner, procedi come segue:

- Aggiungi una fonte di dati per i partner
- Vai al portale web del partner e configura l'origine dati del partner in modo che si connetta al gateway SiteWise Edge.

Argomenti

Sicurezza

Come parte del modello di responsabilità condivisa tra AWS i nostri clienti e i nostri partner, di seguito viene descritto chi è responsabile dei diversi aspetti della sicurezza:

Responsabilità del cliente

- Controllo del partner.
- Configurazione dell'accesso alla rete fornito al partner.

AWSresponsabilità

- Isolare il partner dalle risorse AWS cloud del cliente ad eccezione di quelle necessarie al partner. In questo caso, AWS IoT SiteWise ingestione.
- Limitazione della soluzione partner a un uso ragionevole delle risorse della macchina del gateway SiteWise Edge (CPU, memoria, file system).

Responsabilità del partner

- Utilizzo di impostazioni predefinite sicure.
- Mantenimento della soluzione sicura nel tempo tramite patch e altri aggiornamenti appropriati.
- Mantenere riservati i dati dei clienti.

Aggiungi una fonte di dati per i partner

Per connettere una fonte di dati partner al tuo gateway SiteWise Edge, aggiungila come fonte di dati. Quando lo aggiungi come fonte di dati, AWS IoT SiteWise distribuirà un AWS IoT Greengrass componente privato al tuo gateway SiteWise Edge.

Prerequisiti

Per aggiungere un'origine dati partner, devi fare quanto segue:

- Crea un account con il partner.
- Associa gli account.

Per creare un gateway SiteWise Edge con una fonte di dati partner

Se desideri creare un nuovo gateway SiteWise Edge, completa i passaggi indicati inCreazione di un gateway SiteWise Edge. Dopo aver creato SiteWise Edge gateway, segui i passaggi indicati Per aggiungere una fonte di dati partner a un gateway SiteWise Edge esistente per aggiungere una fonte di dati partner.

Per aggiungere una fonte di dati partner a un gateway SiteWise Edge esistente

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegliere Gateways.
3. Scegli il gateway SiteWise Edge a cui desideri connettere l'origine dati del partner.
4. In Origini dati, scegli Aggiungi origine dati.
5. Per Tipo di origine, scegli il partner a cui vuoi connettere il tuo gateway SiteWise Edge.

   > **Note**
   >
   > Attualmente, EasyEdge è l'unica fonte di dati per i partner disponibile. La prima volta che aggiungi un'origine EasyEdge dati, dovrai creare un EasyEdge account.

6. Inserisci un nome per la fonte.
7. Per concedere al partner l'accesso all'origine dati, seleziona Autorizza.

8. Per consentire AWS IoT SiteWise l'aggiornamento del componente AWS IoT SiteWise publisher e, se il pacchetto di elaborazione dati è abilitato, del componente AWS IoT SiteWise processore, seleziona Aggiorna componenti.
9. Selezionare Salva.

Configura docker sul tuo SiteWise gateway Edge

Per aggiungere un'origine dati partner, è necessario installare Docker Engine 1.9.1 o versione successiva sul dispositivo locale.

> **Note**
>
> La versione 20.10 è l'ultima versione verificata per funzionare con il SiteWise software Edge gateway.

Per verificare che Docker sia installato

Per verificare che Docker sia installato, esegui il seguente comando da un terminale collegato al gateway SiteWise Edge:

```
docker info
```

Se il comando restituisce un `docker is not recognized` risultato o è installata una versione precedente di Docker, installa Docker Engine prima di continuare.

Per configurare Docker

L'utente di sistema che esegue un componente del contenitore Docker deve disporre delle autorizzazioni di root o di amministratore oppure è necessario configurare Docker per eseguirlo come utente non root o non amministratore.

Sui dispositivi Linux, è necessario aggiungere un `ggc_user` utente al gruppo senza il quale chiamare i comandi Docker. `docker` `sudo`

Per aggiungere al `docker` gruppo`ggc_user`, o l'utente non root che usi per eseguire i componenti del contenitore Docker, esegui il comando seguente:

```
sudo usermod -aG docker ggc_user
```

Per ulteriori informazioni, consulta i passaggi successivi all'installazione di Linux per Docker Engine.

SiteWise Origini dati dei partner Edge Gateway

Utilizza le informazioni seguenti per configurare un'origine dati partner.

EasyEdge

Portale:

https://studio.easyedge.io/

EasyEdge documentazione:

EasyEdge per AWS

Utilizzo dei pacchetti

AWS IoT SiteWiseI gateway Edge utilizzano diversi pacchetti per determinare come raccogliere ed elaborare i dati.

Attualmente sono disponibili i seguenti pacchetti:

- Pacchetto di raccolta dati: utilizza questo pacchetto per raccogliere i dati industriali e indirizzarli verso destinazioni AWS cloud. Per impostazione predefinita, questo pacchetto è abilitato automaticamente per il gateway SiteWise Edge.
- Pacchetto di elaborazione dati: utilizza questo pacchetto per abilitare la comunicazione tramite gateway SiteWise Edge con modelli e asset di asset configurati dall'edge. È possibile utilizzare la configurazione edge per controllare quali dati degli asset elaborare ed elaborare in loco. È quindi possibile inviare i dati a AWS IoT SiteWise o ad altri AWS servizi. Per ulteriori informazioni sul pacchetto di elaborazione dati, vederethe section called “Abilitare l'elaborazione dei dati edge”.

Pacchetti di aggiornamento

> **Important**
>
> L'aggiornamento delle versioni del Data Processing Pack dalla versione precedente (inclusa) 2.0.x alla versione 2.1.x comporterà la perdita dei dati delle misurazioni archiviate localmente.

SiteWise Gli edge gateway utilizzano diversi pacchetti per determinare come raccogliere ed elaborare i dati. È possibile utilizzare la AWS IoT SiteWise console per aggiornare i pacchetti.

Per aggiornare i pacchetti (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegliere Gateways.
3. Nell'elenco dei gateway, scegli il gateway SiteWise Edge con i pacchetti che desideri aggiornare.
4. Nella pagina di riepilogo del gateway SiteWise Edge, scegli Aggiornamenti.

> **Note**
>
> È possibile aggiornare solo i pacchetti abilitati. Per trovare l'elenco dei pacchetti abilitati per questo gateway SiteWise Edge, scegli Panoramica, quindi consulta la sezione Funzionalità Edge.

5. Nella sezione Aggiornamenti dei pacchetti, esegui una delle seguenti operazioni.
   - Per OPC-UA Collector, scegli una versione, quindi scegli Deploy.
   - Per Publisher, scegli una versione, quindi scegli Deploy.
   - Per il pacchetto di elaborazione dati, scegli una versione, quindi scegli Deploy.
6. Per confermare la distribuzione, scegli Deploy. Nella colonna Distribuzione dell'elenco Gateway, vedrai Completato. Se non vedi un aggiornamento dello stato della distribuzione, aggiorna la pagina.

> **Note**
>
> - Implementa solo un pacchetto alla volta. Se distribuisci più pacchetti contemporaneamente, verrà distribuito solo l'ultimo pacchetto che hai scelto.

Se riscontri problemi durante l'aggiornamento dei pacchetti, consulta. Impossibile distribuire i pacchetti sui gateway Edge SiteWise

Gestione dei gateway SiteWise Edge

È possibile utilizzare le operazioni della AWS IoT SiteWise console e dell'API per gestire i gateway AWS IoT SiteWise Edge. È inoltre possibile utilizzare l'applicazione AWS OpsHubAWS IoT SiteWise per Windows per gestire alcuni aspetti del gateway SiteWise Edge dal dispositivo locale.

Si consiglia vivamente di utilizzare l' AWS IoT SiteWise applicazione AWS OpsHub for per monitorare l'utilizzo del disco sul dispositivo locale. Puoi anche monitorare i CloudWatch parametri `Gateway.AvailableDiskSpace` e `Gateway.UsedPercentageDiskSpace` Amazon e creare allarmi per ricevere notifiche quando lo spazio su disco si sta esaurendo. Per ulteriori informazioni sugli CloudWatch allarmi Amazon, consulta Creare un CloudWatch allarme basato su una soglia statica.

Assicurati che il tuo dispositivo disponga di spazio sufficiente per i dati in arrivo. Quando lo spazio sul dispositivo locale sta per esaurire, il servizio elimina automaticamente una piccola quantità di dati con i timestamp più vecchi per fare spazio ai dati futuri.

Per verificare se il servizio ha eliminato i tuoi dati, procedi come segue:

1. Accedi all' AWS IoT SiteWise applicazione AWS OpsHub for.
2. Seleziona Impostazioni.
3. Per i registri, specifica un intervallo di tempo, quindi scegli Scarica.
4. Decomprimi il file di registro.
5. Se il file di registro contiene il seguente messaggio, il servizio ha eliminato i dati: *`alcuni`* byte di dati sono stati eliminati per evitare che lo spazio di archiviazione del gateway SiteWise Edge si esaurisca.

Gestione del gateway SiteWise Edge con la console AWS IoT SiteWise

Puoi utilizzare la AWS IoT SiteWise console per configurare, aggiornare e monitorare tutti i gateway SiteWise Edge del tuo AWS account.

È possibile visualizzare i gateway SiteWise Edge accedendo alla pagina Edge Gateways nella console.AWS IoT SiteWise Per accedere alla pagina dei dettagli del gateway Edge per un gateway specifico, scegli il nome di un gateway Edge.

Dalla scheda Panoramica della pagina dei dettagli del gateway Edge, è possibile effettuare le seguenti operazioni:

- Nella sezione Origini dati, aggiorna la configurazione dell'origine dati e configura fonti di dati aggiuntive
- Scegli Open CloudWatch metrics per visualizzare il numero di punti dati acquisiti per origine dati nella console delle metriche CloudWatch
- Nella sezione Funzionalità Edge, aggiungi pacchetti di dati al tuo gateway SiteWise Edge facendo clic su Modifica
- Nella sezione Configurazione del gateway, visualizza lo stato di connettività dei tuoi gateway SiteWise Edge
- Nella sezione Configurazione di Publisher, visualizza lo stato di sincronizzazione del gateway SiteWise Edge e la configurazione del componente AWS IoT SiteWise Publisher

Dalla scheda Aggiornamenti della pagina dei dettagli del gateway Edge, è possibile visualizzare le versioni correnti dei componenti e dei pacchetti distribuite sul gateway Edge. Qui è anche possibile distribuire nuove versioni, quando sono disponibili.

Gestione dei gateway SiteWise Edge utilizzando for AWS OpsHubAWS IoT SiteWise

Utilizzi l' AWS IoT SiteWise applicazione AWS OpsHub for per gestire e monitorare i gateway SiteWise Edge. Questa applicazione offre le seguenti opzioni di monitoraggio e gestione:

- In Panoramica, è possibile effettuare le seguenti operazioni:
  - Visualizza i dettagli del gateway SiteWise Edge che ti aiutano a ottenere informazioni dettagliate sui dati del dispositivo SiteWise Edge Gateway, a identificare i problemi e a migliorare le prestazioni del gateway SiteWise Edge.
  - Visualizza SiteWise i portali di monitoraggio che monitorano i dati provenienti da server e apparecchiature locali all'edge. Per ulteriori informazioni, consultate Cosa contiene la Guida AWS IoT SiteWise Monitor all'AWS IoT SiteWise Monitor applicazione.
- In Health, c'è una dashboard che mostra i dati dal gateway SiteWise Edge. Gli esperti del settore, come gli ingegneri di processo, possono utilizzare la dashboard per visualizzare una panoramica del comportamento del gateway SiteWise Edge.
- In Risorse, visualizza le risorse distribuite sul dispositivo locale e l'ultimo valore raccolto o calcolato per le proprietà delle risorse.
- In Impostazioni, puoi fare quanto segue:

- Se il Data Processing Pack è installato, visualizza le informazioni di configurazione del gateway SiteWise Edge e sincronizza le risorse con il AWS Cloud.
- Scarica i file di autenticazione che puoi utilizzare per accedere al gateway SiteWise Edge utilizzando altri strumenti.
- Scarica i log che puoi utilizzare per risolvere i problemi relativi al gateway Edge. SiteWise
- Visualizza i AWS IoT SiteWise componenti distribuiti sul gateway Edge. SiteWise

> **Important**
>
> È necessario utilizzare quanto segue AWS OpsHub per AWS IoT SiteWise:
>
> - Il dispositivo locale e l' AWS IoT SiteWise applicazione AWS OpsHub for devono essere connessi alla stessa rete.
> - Il pacchetto di elaborazione dati deve essere abilitato.

Per gestire i gateway SiteWise Edge utilizzando AWS OpsHub

1. Scarica e installa l'applicazione AWS OpsHubAWS IoT SiteWise per Windows.
2. Aprire l'applicazione .
3. Se non disponi di credenziali locali configurate per il gateway, segui i passaggi seguenti Accesso al gateway SiteWise Edge utilizzando le credenziali del sistema operativo locale per configurarle.
4. Puoi accedere al tuo gateway SiteWise Edge con le tue credenziali Linux o Lightweight Directory Access Protocol (LDAP). Per accedere al gateway SiteWise Edge, esegui una delle seguenti operazioni:

   Linux

   1. Per il nome host o l'indirizzo IP, inserisci il nome host o l'indirizzo IP del dispositivo locale.
   2. Per l'autenticazione, scegli Linux.
   3. Per Nome utente, inserisci il nome utente del tuo sistema operativo Linux.
   4. Per Password, inserisci la password del tuo sistema operativo Linux.
   5. Selezionare Sign in (Accedi).

LDAP

1. Per Nome host o indirizzo IP, inserisci il nome host o l'indirizzo IP del tuo dispositivo locale.
2. Per l'autenticazione, scegli LDAP.
3. Per Nome utente, inserisci il nome utente del tuo LDAP.
4. Per Password, inserisci la password del tuo LDAP.
5. Selezionare Sign in (Accedi).

Accesso al gateway SiteWise Edge utilizzando le credenziali del sistema operativo locale

Oltre a Lightweight Directory Access Protocol (LDAP), puoi utilizzare le credenziali Linux o Windows per accedere al tuo SiteWise gateway Edge.

> **Important**
>
> Per accedere al gateway SiteWise Edge con credenziali Linux, è necessario attivare il pacchetto di elaborazione dati per il SiteWise gateway Edge.

Accesso al gateway SiteWise Edge utilizzando le credenziali del sistema operativo Linux

I passaggi seguenti presuppongono l'utilizzo di un dispositivo con Ubuntu. Se utilizzi una distribuzione Linux diversa, consulta la documentazione pertinente per il tuo dispositivo.

Per creare un pool di utenti Linux

1. Per creare un gruppo di amministratori, esegui il comando seguente.

   ```
   sudo groupadd --system SWE_ADMIN_GROUP
   ```

   Gli utenti del `SWE_ADMIN_GROUP` gruppo possono consentire l'accesso amministrativo al gateway SiteWise Edge.
2. Per creare un gruppo di utenti, esegui il comando seguente.

```
sudo groupadd --system SWE_USER_GROUP
```

Gli utenti del SWE_USER_GROUP gruppo possono consentire l'accesso in sola lettura per il gateway SiteWise Edge.

3. Per aggiungere un utente al gruppo di amministratori, esegui il comando seguente. Sostituisci *nome utente* e *password* con il nome utente e la password che desideri aggiungere.

```
sudo useradd -p $(openssl passwd -1 password) user-name
```

4. Per aggiungere un utente a uno dei due SWE_ADMIN_GROUP oSWE_USER_GROUP, sostituisci il *nome utente* con il nome utente aggiunto nel passaggio precedente.

```
sudo usermod -a -G SWE_ADMIN_GROUP user-name
```

È ora possibile utilizzare il nome utente e la password per accedere al gateway SiteWise Edge sull' AWS IoT SiteWise applicazione AWS OpsHub for.

Accesso al gateway SiteWise Edge utilizzando le credenziali di Windows

I passaggi seguenti presuppongono l'utilizzo di un dispositivo con Windows.

> **Important**
>
> La sicurezza è una responsabilità condivisa tra te AWS e te. Crea una politica di password efficace con almeno 12 caratteri e una combinazione di lettere maiuscole, minuscole, numeri e simboli. Inoltre, imposta le regole di Windows Firewall per consentire il traffico in entrata sulla porta 443 e bloccare il traffico in entrata su tutte le altre porte.

Per creare un pool di utenti di Windows Server

1. Esegui PowerShell come amministratore.

   a. Sul server Windows in cui desideri installare SiteWise Edge Gateway, accedi come amministratore.

   b. Entra PowerShellnella barra di ricerca di Windows.

c. Nei risultati della ricerca, fai clic con il pulsante destro del mouse sull' PowerShellapp Windows. Scegli Esegui come amministratore.

2. Per creare un gruppo di amministratori, esegui il comando seguente.

```
net localgroup SWE_ADMIN_GROUP /add
```

Devi essere un utente del `SWE_ADMIN_GROUP` gruppo per consentire l'accesso da amministratore al gateway SiteWise Edge.

3. Per creare un gruppo di utenti, esegui il comando seguente.

```
net localgroup SWE_USER_GROUP /add
```

È necessario essere un utente del `SWE_USER_GROUP` gruppo per consentire l'accesso in modalità di sola lettura per il gateway SiteWise Edge.

4. Per aggiungere un utente, esegui il comando seguente. Sostituisci *`nome utente`* e *`password`* con il nome utente e la password che desideri creare.

```
net user user-name password /add
```

5. Per aggiungere un utente al gruppo di amministratori, esegui il comando seguente. Sostituisci *`il nome utente`* con il nome utente che desideri aggiungere.

```
net localgroup SWE_ADMIN_GROUP user-name /add
```

È ora possibile utilizzare il nome utente e la password per accedere al gateway SiteWise Edge sull' AWS IoT SiteWise applicazione AWS OpsHub for.

Gestione del certificato del gateway SiteWise Edge

È possibile utilizzare SiteWise Monitor e applicazioni di terze parti, come Grafana, sui dispositivi gateway SiteWise Edge. Queste applicazioni richiedono una connessione TLS al servizio. SiteWise I gateway Edge attualmente utilizzano un certificato autofirmato. Se si utilizza un browser per aprire le applicazioni, ad esempio un portale SiteWise Monitor, è possibile che venga visualizzato un avviso relativo alla presenza di un certificato non attendibile.

Di seguito viene illustrato come scaricare il certificato affidabile dall' AWS IoT SiteWise applicazione AWS OpsHub for.

1. Accedere all'applicazione.
2. Seleziona Impostazioni.
3. Per Autenticazione, scegli Scarica certificato.

Quanto segue presuppone che utilizzi Google Chrome o FireFox. Se utilizzi un browser diverso, consulta la documentazione pertinente del tuo browser. Per aggiungere il certificato scaricato nel passaggio precedente a un browser, esegui una delle seguenti operazioni:

- Se utilizzi Google Chrome, segui la sezione Configurazione dei certificati nella documentazione della Guida di Google Chrome Enterprise.
- Se utilizzi Firefox, segui le istruzioni Per caricare il certificato nel browser Mozilla o Firefox nella documentazione di Oracle.

Modifica della versione dei pacchetti di componenti del gateway SiteWise Edge

È possibile utilizzare la AWS IoT SiteWise console per modificare la versione dei pacchetti di componenti sui gateway SiteWise Edge.

Per modificare la versione di un pacchetto di componenti SiteWise Edge Gateway

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione a sinistra, selezionare Gateways (Gateway).
3. Seleziona il gateway SiteWise Edge per il quale desideri modificare le versioni del pacchetto.
4. In Configurazione del gateway, scegli Visualizza versioni del software.
5. Nella pagina Modifica versioni del software, per il pacchetto di cui desideri aggiornare la versione, seleziona la versione che desideri distribuire e scegli Distribuisci.
6. Seleziona Fatto.

Running SiteWise Edge su Siemens Industrial Edge

Puoi importare dati dal tuo dispositivo Siemens Industrial Edge al tuo Account AWS utilizzando un gateway SiteWise Edge sul dispositivo. Per fare ciò, create una risorsa gateway SiteWise Edge con un obiettivo di implementazione del dispositivo Siemens Industrial Edge: nuovo, scaricate il file di

configurazione e caricatelo sull'app Siemens tramite il portale Siemens Industrial Edge Management (IEM). Per ulteriori informazioni sull'esecuzione di AWS IoT SiteWise Edge su Siemens Industrial Edge, incluso come configurare le risorse Siemens richieste, vedi Cos'è Industrial Edge? nella documentazione Siemens.

> **Note**
>
> Siemens non è un fornitore o fornitore di Edge. AWS IoT SiteWise Il Siemens Industrial Edge Marketplace è un marketplace indipendente.

Argomenti

Prerequisiti

Per eseguire AWS IoT SiteWise Edge su Siemens Industrial Edge, è necessario quanto segue:

- Un account Siemens Digital Exchange Platform
- Un account Siemens Industrial Edge Hub (iehub)
- Un'istanza di Siemens Industrial Edge Management (IEM)
- Un dispositivo Siemens Industrial Edge (IED) o un dispositivo virtuale Siemens Industrial Edge (iEVD)
- Accesso all'obiettivo di implementazione del dispositivo Siemens Industrial Edge. Per ottenere l'accesso, vai alla AWS IoT SiteWise console e scegli Richiedi accesso.

Sicurezza

Nell'ambito del modello di responsabilità condivisa tra AWS i nostri clienti e i nostri partner, di seguito viene descritto chi è responsabile dei diversi aspetti della sicurezza:

Responsabilità del cliente

- Controllo del partner.
- Configurazione dell'accesso alla rete fornito al partner.
- Protezione fisica del dispositivo su cui è installato AWS IoT SiteWise Edge.

AWS responsabilità

- Isolare il partner dalle risorse AWS cloud del cliente.

Responsabilità del partner

- Utilizzo di impostazioni predefinite sicure.
- Mantenimento della soluzione sicura nel tempo tramite patch e altri aggiornamenti appropriati.
- Mantenere riservati i dati dei clienti.
- Verifica di altre applicazioni disponibili nel marketplace dei partner.

Durante la fase di anteprima di questa funzionalità, i dati dei clienti memorizzati nella AWS IoT SiteWise cache del dispositivo partner sono accessibili dal partner e dalle altre applicazioni installate tramite il marketplace del partner.

Creare il file di configurazione

Una volta che disponi degli account Siemens e delle istanze IEM appropriati, puoi creare un gateway SiteWise Edge di tipo Siemens Industrial Edge.

Per creare il file di configurazione

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Edge gateway.
3. Selezionare Create gateway (Crea gateway).
4. Per il tipo di implementazione, scegli il dispositivo Siemens Industrial Edge - nuovo.
5. Inserisci un nome per il tuo gateway SiteWise Edge o usa il nome generato da AWS IoT SiteWise.
6. (Facoltativo) In configurazione avanzata, effettuate le seguenti operazioni:
   - Immettete un nome per l' AWS IoT Core oggetto o utilizzate il nome generato da AWS IoT SiteWise.
7. Selezionare Create gateway (Crea gateway).

8. Nella finestra di dialogo Genera il file di configurazione del gateway SiteWise Edge, scegli Genera e scarica. AWS IoT SiteWise genera automaticamente un file di configurazione che utilizzerai per configurare l'applicazione AWS IoT SiteWise Edge.

   > **Important**
   >
   > Assicuratevi di salvare il file di configurazione in una posizione sicura. Utilizzerai il file in un secondo momento.

Ora che hai creato il gateway SiteWise Edge, procedi come segue per completare la configurazione del gateway SiteWise Edge:

1. Aggiungi fonti di dati
2. Configurare il componente Publisher

Una volta ottenuto il file di configurazione e configurato il gateway SiteWise Edge, scarica l'applicazione AWS IoT SiteWise Edge da Siemens Industrial Edge Marketplace e installala utilizzando il portale Siemens Industrial Edge Management (IEM). Quindi, accedi al tuo dispositivo Siemens Industrial Edge tramite il portale Siemens Industrial Edge Management (IEM) e carica il file di configurazione sul dispositivo su cui desideri installare il gateway Edge. SiteWise

Risoluzione dei problemi

Per risolvere i problemi relativi al gateway SiteWise Edge sul dispositivo Siemens Industrial Edge, è possibile accedere ai registri dell'applicazione tramite i portali Siemens Industrial Edge Management (IEM) o Siemens Industrial Edge Device (IED). Per ulteriori informazioni, consulta la sezione Download dei registri nella documentazione Siemens.

Vedo 'SESSION_TAKEN_OVER' o 'com.aws.greengrass.mqttclient. MqttClient: Impossibile pubblicare il messaggio tramite Spooler e riproverò. ' nei log

Se viene visualizzato un avviso che include `SESSION_TAKEN_OVER` o un errore incluso `com.aws.greengrass.mqttclient.MqttClient: Failed to publish the message via Spooler and will retry.` nei registri all'indirizzo`/greengrass/v2/logs/greengrass.log`, è possibile che si stia tentando di utilizzare lo stesso file di configurazione per più gateway SiteWise Edge su più dispositivi. Ogni gateway SiteWise Edge necessita di un file di configurazione unico per connettersi al tuo. Account AWS

Vedo 'com.aws.greengrass.deployment. IotJobsHelper: Nessun processo di distribuzione trovato. ' o 'Risultato della distribuzione già segnalato'. nei registri

Se vedi `com.aws.greengrass.deployment.IotJobsHelper: No deployment job found.` o `Deployment result already reported.` nei tuoi log all'indirizzo`/greengrass/v2/logs/greengrass.log`, potresti provare a riutilizzare lo stesso file di configurazione.

Esistono diverse soluzioni:

- Se desideri riutilizzare il file di configurazione, procedi come segue:
  1. Passare alla console AWS IoT SiteWise.
  2. Nel riquadro di navigazione, scegliere Gateways.
  3. Scegli il gateway SiteWise Edge che desideri riutilizzare.
  4. Scegli la scheda Aggiornamenti.
  5. Seleziona una versione diversa di Publisher e scegli Distribuisci.
- Segui i passaggi indicati Creare il file di configurazione per creare un nuovo file di configurazione.

Vedo «File di configurazione mancante AWS_REGION» nei log.

Se vedi `Config file missing AWS_REGION` nei log Siemens, il JSON del file di configurazione è stato danneggiato. Dovrai creare un nuovo file di configurazione. Segui i passaggi indicati Creare il file di configurazione per creare un nuovo file di configurazione.

Contattaci

- Se desideri richiedere l'accesso all'applicazione, vai alla AWS IoT SiteWise console e scegli Richiedi accesso.
- Se desideri assistenza per la risoluzione dei problemi dell'applicazione, vai alla AWS IoT SiteWise console, vai alla pagina dei dettagli del gateway SiteWise Edge e scegli Richiedi supporto.

Filtraggio delle risorse su un gateway SiteWise Edge

Puoi utilizzare il filtro edge per gestire in modo più efficiente le tue risorse inviando solo un sottoinsieme di risorse a uno specifico gateway SiteWise Edge da utilizzare nell'elaborazione dei dati. Se le risorse sono disposte in una struttura ad albero, o padre-figlio, è possibile impostare una

policy IAM collegata al ruolo IAM di un gateway SiteWise Edge che consenta solo l'invio della radice dell'albero, o genitore, e dei relativi figli a un gateway Edge specifico. SiteWise

> **Note**
>
> Se stai organizzando le risorse esistenti in una struttura ad albero, dopo aver creato la struttura, accedi a ogni risorsa esistente che hai aggiunto alla struttura e scegli Modifica, quindi scegli Salva per assicurarti che AWS IoT SiteWise riconosca la nuova struttura.

Configurazione del filtro perimetrale

Configura il filtro edge sul tuo gateway SiteWise Edge aggiungendo la seguente policy IAM al ruolo IAM del gateway SiteWise Edge, sostituendo *< root-asset-id >* con l'ID della risorsa radice che desideri inviare al gateway SiteWise Edge.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "iotsitewise:DescribeAsset",
                "iotsitewise:ListAssociatedAssets"
            ],
            "Resource": "arn:aws:iotsitewise:*:*:asset/*",
            "Condition": {
                "StringNotLike": {
                    "iotsitewise:assetHierarchyPath": "/<root-asset-id>*"
                }
            }
        }
    ]
}
```

Se al momento ci sono risorse sul gateway SiteWise Edge che desideri rimuovere, accedi al gateway SiteWise Edge ed esegui il comando seguente per forzare la sincronizzazione con il gateway SiteWise Edge AWS IoT SiteWise eliminando la cache.

```
sudo rm /greengrass/v2/work/aws.iot.SiteWiseEdgeProcessor/sync-app/
sync_resource_bundles/edge.json
```

Utilizzo AWS IoT SiteWise delle API sull'edge

Puoi utilizzare un sottoinsieme delle AWS IoT SiteWise API disponibili insieme a API specifiche per l'edge per interagire con i modelli di asset e i relativi asset sull'edge. I modelli di asset devono essere configurati per funzionare all'edge. Per ulteriori informazioni, consulta Elaborazione dei dati all'edge.

Utilizza queste API per raccogliere dati sui tuoi modelli e asset, monitorare i portali implementati e le metriche del dashboard e raccogliere i dati sugli asset all'edge. Ciò fornisce un host centrale nella rete con cui interagire AWS IoT SiteWise senza richiedere una chiamata all'API Web.

Argomenti

- Tutte le API disponibili per l'uso con i dispositivi AWS IoT SiteWise periferici
- API edge-only da utilizzare con dispositivi edge AWS IoT SiteWise
- Tutorial: Ottenere un elenco di modelli di asset su un gateway SiteWise Edge

Tutte le API disponibili per l'uso con i dispositivi AWS IoT SiteWise periferici

Quando lavori con dispositivi periferici, puoi utilizzare una varietà di API per interagire AWS IoT SiteWise e completare le attività localmente sul dispositivo.

API disponibili AWS IoT SiteWise

Le seguenti AWS IoT SiteWise API sono disponibili sui dispositivi periferici:

- ListAssetModels
- DescribeAssetModel
- ListAssets
- DescribeAsset
- DescribeAssetProperty
- ListAssociatedAssets
- GetAssetPropertyAggregates

- GetAssetPropertyValue
- GetAssetPropertyValueHistory
- ListDashboards
- ListPortals
- ListProjectAssets
- ListProjects
- DescribeDashboard
- DescribePortal
- DescribeProject

API disponibili solo per l'ambiente perimetrale

Le seguenti API vengono utilizzate localmente sui dispositivi periferici:

- Autenticazione— Usa questa API per ottenere le credenziali temporanee SigV4 che utilizzerai per effettuare chiamate API.

API edge-only da utilizzare con dispositivi edge AWS IoT SiteWise

Oltre alle AWS IoT SiteWise API disponibili sull'edge, ne esistono di specifiche. Queste API specifiche per l'edge sono descritte di seguito.

Autenticazione

Ottiene le credenziali dal gateway SiteWise Edge. Dovrai aggiungere utenti locali o connetterti al sistema tramite LDAP o un pool di utenti Linux. Per ulteriori informazioni sull'aggiunta di utenti, consulta LDAP o pool di utenti Linux.

Sintassi della richiesta

```
POST /authenticate HTTP/1.1
Content-type: application/json
{
  "username": "string",
  "password": "string",
  "authMechanism": "string"
}
```

Parametri di richiesta URI

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

username

Il nome utente utilizzato per convalidare la chiamata di richiesta.

Tipo: stringa

Campo obbligatorio: sì

password

La password dell'utente che richiede le credenziali.

Tipo: stringa

Campo obbligatorio: sì

Meccanismo di autenticazione

Il metodo di autenticazione per convalidare questo utente nell'host.

Tipo: stringa

Valori validi: `ldap`, `linux`, `winnt`

Campo obbligatorio: sì

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json
{
  "accessKeyId": "string",
  "secretAccessKey": "string",
  "sessionToken": "string",
  "region": "edge"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I seguenti dati vengono restituiti in formato JSON.

accessKeyId

L'ID della chiave di accesso che identifica le credenziali di sicurezza temporanee.

Vincoli di lunghezza: lunghezza minima di 16. La lunghezza massima è 128 caratteri.

Modello: `[\w]*`

secretAccessKey

La chiave di accesso segreta che può essere utilizzata per firmare le richieste.

Tipo: stringa

sessionToken

Il token che gli utenti devono passare all'API del servizio per utilizzare le credenziali temporanee.

Tipo: stringa

Regione

La regione a cui ti rivolgi per le chiamate API.

Tipo: CONSTANT - `edge`

Errori

IllegalArgumentException

La richiesta è stata respinta perché il corpo del documento fornito non era valido. Il messaggio di errore descrive l'errore specifico.

Codice di stato HTTP: 400

AccessDeniedException

L'utente non dispone di credenziali valide basate sull'attuale Identity Provider. Il messaggio di errore descrive il meccanismo di autenticazione.

Codice di stato HTTP: 403

TooManyRequestsException

La richiesta ha raggiunto il limite di tentativi di autenticazione. Il messaggio di errore contiene la quantità di tempo di attesa prima che vengano effettuati nuovi tentativi di autenticazione.

Codice di stato HTTP: 429

Tutorial: Ottenere un elenco di modelli di asset su un gateway SiteWise Edge

Puoi utilizzare un sottoinsieme delle AWS IoT SiteWise API disponibili insieme alle API specifiche di Edge per interagire con i modelli di asset e le relative risorse sull'edge. Questo tutorial ti illustrerà come ottenere credenziali temporanee per un gateway AWS IoT SiteWise Edge e ottenere un elenco dei modelli di asset sul gateway Edge. SiteWise

Prerequisiti

Nei passaggi di questo tutorial puoi utilizzare una varietà di strumenti. Per utilizzare questi strumenti, assicurati di aver installato i prerequisiti corrispondenti.

Per completare questo tutorial, è necessario quanto segue:

- A: distribuito e funzionante SiteWise Requisiti del gateway edge
- Accesso al gateway SiteWise Edge nella stessa rete tramite la porta 443.
- OpenSSL installato
- (AWS OpsHubperAWS IoT SiteWise) L'AWS OpsHubapplicazione for AWS IoT SiteWise
- (curl) curl installato
- (Python) urllib3 installato
- (Python) Python3 installato
- (Python) Boto3 installato
- (Python) installato BotoCore

Passaggio 1: ottenere un certificato firmato per il servizio gateway SiteWise Edge

Per stabilire una connessione TLS alle API disponibili sul gateway SiteWise Edge, è necessario un certificato affidabile. È possibile generare questo certificato utilizzando un OpenSSL o forAWS OpsHub. AWS IoT SiteWise

OpenSSL

> **Note**
>
> È necessario che sia installato OpenSSL per eseguire questo comando.

Apri un terminale ed esegui il comando seguente per ottenere un certificato firmato dal gateway SiteWise Edge. Sostituisci `<sitewise_gateway_ip>` con l'IP del gateway SiteWise Edge.

```
openssl s_client -connect <sitewise_gateway_ip>:443 </dev/null 2>/dev/null | openssl
 x509 -outform PEM > GatewayCert.pem
```

AWS OpsHub for AWS IoT SiteWise

Puoi usare AWS OpsHub perAWS IoT SiteWise. Per ulteriori informazioni, consulta Gestione dei gateway SiteWise Edge.

In questo tutorial viene utilizzato il percorso assoluto del certificato gateway SiteWise Edge scaricato. Esegui il comando seguente per esportare il percorso completo del certificato, sostituendolo `<absolute_path_to_certificate>` con il percorso del certificato:

```
export PATH_TO_CERTIFICATE='<absolute_path_to_certificate>'
```

Passaggio 2: ottieni il nome host SiteWise del gateway Edge

> **Note**
>
> È necessario che sia installato OpenSSL per eseguire questo comando.

Per completare il tutorial è necessario il nome host del gateway Edge. SiteWise Per ottenere il nome host del gateway SiteWise Edge, esegui quanto segue, sostituendolo `<sitewise_gateway_ip>` con l'IP del gateway SiteWise Edge:

```
openssl s_client -connect <sitewise_gateway_ip>:443 </dev/null 2>/dev/null | grep -Po
 'CN = \K.*'| head -1
```

Esegui il comando seguente per esportare il nome host da utilizzare in seguito, sostituendolo `<your_edge_gateway_hostname>` con il nome host del gateway Edge: SiteWise

```
export GATEWAY_HOSTNAME='<your_edge_gateway_hostname>'
```

Passaggio 3: Ottieni credenziali temporanee per il tuo gateway Edge SiteWise

Ora che hai il certificato firmato e il nome host del tuo gateway SiteWise Edge, devi ottenere credenziali temporanee per poter eseguire le API sul gateway. È possibile ottenere queste credenziali tramite AWS OpsHub AWS IoT SiteWise o direttamente dal gateway SiteWise Edge utilizzando le API.

> **Important**
>
> Le credenziali scadono ogni 4 ore, quindi è consigliabile ottenerle subito prima di utilizzare le API sul gateway Edge. SiteWise Non memorizzate nella cache le credenziali per più di 4 ore.

Ottieni credenziali temporanee utilizzando for AWS OpsHubAWS IoT SiteWise

> **Note**
>
> È necessario installare l'AWS IoT SiteWiseapplicazione AWS OpsHub for.

Per utilizzare l'AWS IoT SiteWiseapplicazione AWS OpsHub per ottenere le credenziali temporanee, procedi come segue:

1. Accedere all'applicazione.
2. Seleziona Impostazioni.
3. Per Autenticazione, scegli Copia credenziali.
4. Espandi l'opzione più adatta al tuo ambiente e scegli Copia.
5. Salva le credenziali per utilizzarle in seguito.

Ottieni credenziali temporanee utilizzando l'API del gateway SiteWise Edge

Per utilizzare l'API SiteWise Edge gateway per ottenere le credenziali temporanee è possibile utilizzare uno script Python o curl, per prima cosa è necessario disporre di un nome utente e una

password per SiteWise il gateway Edge. I gateway SiteWise Edge utilizzano l'autenticazione e l'autorizzazione SigV4. Per ulteriori informazioni sull'aggiunta di utenti, consulta LDAP o pool di utenti Linux. Queste credenziali verranno utilizzate nei passaggi seguenti per ottenere le credenziali locali sul gateway SiteWise Edge necessarie per utilizzare le API. AWS IoT SiteWise

Python

> **Note**
>
> È necessario installare urllib3 e Python3.

Per ottenere le credenziali usando Python

1. Crea un file chiamato get_credentials.py e poi copia il seguente codice al suo interno.

```
'''
The following demonstrates how to get the credentials from the SiteWise Edge
 gateway. You will need to add local users or connect your system to LDAP/AD
https://docs.aws.amazon.com/iot-sitewise/latest/userguide/manage-gateways-
ggv2.html#create-user-pool

Example usage:
    python3 get_credentials.py -e https://<gateway_hostname> -c
 <path_to_certificate> -u '<gateway_username>' -p '<gateway_password>' -m
 '<method>'
'''
import urllib3
import json
import urllib.parse
import sys
import os
import getopt

"""
This function retrieves the AWS IoT SiteWise Edge gateway credentials.
"""
def get_credentials(endpoint,certificatePath, user, password, method):
    http = urllib3.PoolManager(cert_reqs='CERT_REQUIRED', ca_certs=
 certificatePath)
    encoded_body = json.dumps({
        "username": user,
```

```
        "password": password,
        "authMechanism": method,
    })

    url =  urllib.parse.urljoin(endpoint, "/authenticate")

    response = http.request('POST', url,
        headers={'Content-Type': 'application/json'},
        body=encoded_body)

    if response.status != 200:
        raise Exception(f'Failed to authenticate! Response status
 {response.status}')

    auth_data = json.loads(response.data.decode('utf-8'))

    accessKeyId = auth_data["accessKeyId"]
    secretAccessKey = auth_data["secretAccessKey"]
    sessionToken = auth_data["sessionToken"]
    region = "edge"

    return accessKeyId, secretAccessKey, sessionToken, region

def print_help():
    print('Usage:')
    print(f'{os.path.basename(__file__)} -e <endpoint> -c <path/to/certificate>
 -u <user> -p <password> -m <method> -a <alias>')
    print('')
    print('-e, --endpoint   edge gateway endpoint. Usually the Edge gateway
 hostname.')
    print('-c, --cert_path path to downloaded gateway certificate')
    print('-u, --user       Edge user')
    print('-p, --password   Edge password')
    print('-m, --method     (Optional) Authentication method (linux, winnt,
 ldap), default is linux')
    sys.exit()


def parse_args(argv):
    endpoint = ""
    certificatePath = None
    user = None
    password = None
    method = "linux"
```

```
    try:
        opts, args = getopt.getopt(argv, "he:c:u:p:m:",
 ["endpoint=","cert_path=", "user=", "password=", "method="])
    except getopt.GetoptError:
        print_help()

    for opt, arg in opts:
        if opt == '-h':
            print_help()
        elif opt in ("-e", "--endpoint"):
            endpoint = arg
        elif opt in ("-u", "--user"):
            user = arg
        elif opt in ("-p", "--password"):
            password = arg
        elif opt in ("-m", "--method"):
            method = arg.lower()
        elif opt in ("-c", "--cert_path"):
            certificatePath = arg

    if method not in ['ldap', 'linux', 'winnt']:
        print("not valid method parameter, required are ldap, linux, winnt")
        print_help()

    if (user == None or password == None):
        print("To authenticate against edge user, password have to be passed
 together, and the region has to be set to 'edge'")
        print_help()

    if(endpoint == ""):
        print("You must provide a valid and reachable gateway hostname")
        print_help()

    return endpoint,certificatePath, user, password, method


def main(argv):
    # get the command line args
    endpoint, certificatePath, user, password, method = parse_args(argv)

    accessKeyId, secretAccessKey, sessionToken, region=get_credentials(endpoint,
 certificatePath, user, password, method)
```

```
    print("Copy and paste the following credentials into the shell, they are
 valid for 4 hours:")
    print(f"export AWS_ACCESS_KEY_ID={accessKeyId}")
    print(f"export AWS_SECRET_ACCESS_KEY={secretAccessKey}")
    print(f"export AWS_SESSION_TOKEN={sessionToken}")
    print(f"export AWS_REGION={region}")
    print()




if __name__ == "__main__":
   main(sys.argv[1:])
```

2. Esegui get_credentials.py dal terminale sostituendo <gateway_username> e <gateway_password> con le credenziali che hai creato.

```
python3 get_credentials.py -e https://$GATEWAY_HOSTNAME -c $PATH_TO_CERTIFICATE
 -u '<gateway_username>' -p '<gateway_password>' -m 'linux'
```

curl

> **Note**
>
> È necessario installare curl.

Per ottenere le credenziali usa curl

1. Esegui il seguente comando dal terminale sostituendo <gateway_username>e <gateway_password>con le credenziali che hai creato.

```
curl --cacert $PATH_TO_CERTIFICATE --location \
-X POST https://$GATEWAY_HOSTNAME:443/authenticate \
--header 'Content-Type: application/json' \
--data-raw '{
    "username": "<gateway_username>",
    "password": "<gateway_password>",
    "authMechanism": "linux"
}'
```

La risposta dovrebbe essere simile alla seguente:

```
{
    "username": "sweuser",
    "accessKeyId": "<accessKeyId>",
    "secretAccessKey": "<secretAccessKey>",
    "sessionToken": "<sessionToken>",
    "sessionExpiryTime": "2022-11-17T04:51:40.927095Z",
    "authMechanism": "linux",
    "role": "edge-user"
}
```

2. Eseguire il seguente comando dal terminale.

```
export AWS_ACCESS_KEY_ID=<accessKeyId>
export AWS_SECRET_ACCESS_KEY=<secretAccessKey>
export AWS_SESSION_TOKEN=<sessionToken>
export AWS_REGION=edge
```

Passaggio 4: Ottieni un elenco dei modelli di asset sul gateway SiteWise Edge

Ora che disponete di un certificato firmato, del nome host del gateway SiteWise Edge e delle credenziali temporanee per il gateway SiteWise Edge, potete utilizzare l'`ListAssetModels`API per ottenere un elenco dei modelli di asset sul gateway SiteWise Edge.

Python

> **Note**
>
> È necessario installare Python3 e Boto3. BotoCore

Per ottenere l'elenco dei modelli di asset usando Python

1. Crea un file chiamato list_asset_model.py e poi copia il seguente codice al suo interno.

```
import json
import boto3
import botocore
import os
```

```
# create the client using the credentials
client = boto3.client("iotsitewise",
    endpoint_url= "https://"+ os.getenv("GATEWAY_HOSTNAME"),
    region_name=os.getenv("AWS_REGION"),
    aws_access_key_id=os.getenv("AWS_ACCESS_KEY_ID"),
    aws_secret_access_key=os.getenv("AWS_SECRET_ACCESS_KEY"),
    aws_session_token=os.getenv("AWS_SESSION_TOKEN"),
    verify=os.getenv("PATH_TO_CERTIFICATE"),
    config=botocore.config.Config(inject_host_prefix=False))

# call the api using local credentials
response = client.list_asset_models()
print(response)
```

2. Esegui list_asset_model.py dal terminale.

```
python3 list_asset_model.py
```

curl

> **Note**
>
> È necessario installare curl.

Per ottenere l'elenco dei modelli di asset che utilizzano curl

Esegui il seguente comando dal terminale.

```
curl \
  --request GET https://$GATEWAY_HOSTNAME:443/asset-models \
  --cacert $PATH_TO_CERTIFICATE \
  --aws-sigv4 "aws:amz:edge:iotsitewise" \
  --user "$AWS_ACCESS_KEY_ID:$AWS_SECRET_ACCESS_KEY" \
  -H "x-amz-security-token:$AWS_SESSION_TOKEN"
```

La risposta dovrebbe essere simile alla seguente:

```
{
    "assetModelSummaries": [
```

```
        {
            "arn": "arn:aws:iotsitewise:{region}:{account-id}:asset-model/{asset-
model-id}",
            "creationDate": 1.669245291E9,
            "description": "This is a small example asset model",
            "id": "{asset-model-id}",
            "lastUpdateDate": 1.669249038E9,
            "name": "Some Metrics Model",
            "status": {
                "error": null,
                "state": "ACTIVE"
            }
        },
        .
        .
        .
    ],
    "nextToken": null
}
```

Backup e ripristino dei gateway SiteWise Edge

Questo argomento spiega come ripristinare i gateway SiteWise Edge e il backup dei dati metrici. Se riscontri problemi con un gateway SiteWise Edge danneggiato sullo stesso computer e devi risolvere il problema, leggi la AWS IoT SiteWise documentazione Risoluzione dei problemi SiteWise relativi al gateway Edge.

> **Note**
>
> La guida fornita in questo argomento si riferisce SiteWise ai gateway Edge installati nella AWS IoT Greengrass V2 versione 2.1.0 o successiva.

Backup giornalieri dei dati metrici

La creazione di un backup è importante se desideri trasferire o ripristinare i dati su una nuova macchina. Il backup dei dati riduce notevolmente il rischio di perdita dei dati operativi durante un processo di trasferimento o ripristino.

Il percorso della cartella influxdb è il seguente:

Linux

```
/greengrass/v2/work/aws.iot.SiteWiseEdgeProcessor/influxdb
```

Windows

```
C:\greengrass\v2\work\aws.iot.SiteWiseEdgeProcessor\influxdb
```

Ti consigliamo di eseguire il backup dell'intera cartella con tutto il contenuto sottostante.

Ti consigliamo di eseguire periodicamente il backup dei dati metrici da 1.0 SiteWise Edge su un disco rigido esterno o sul cloud. AWS

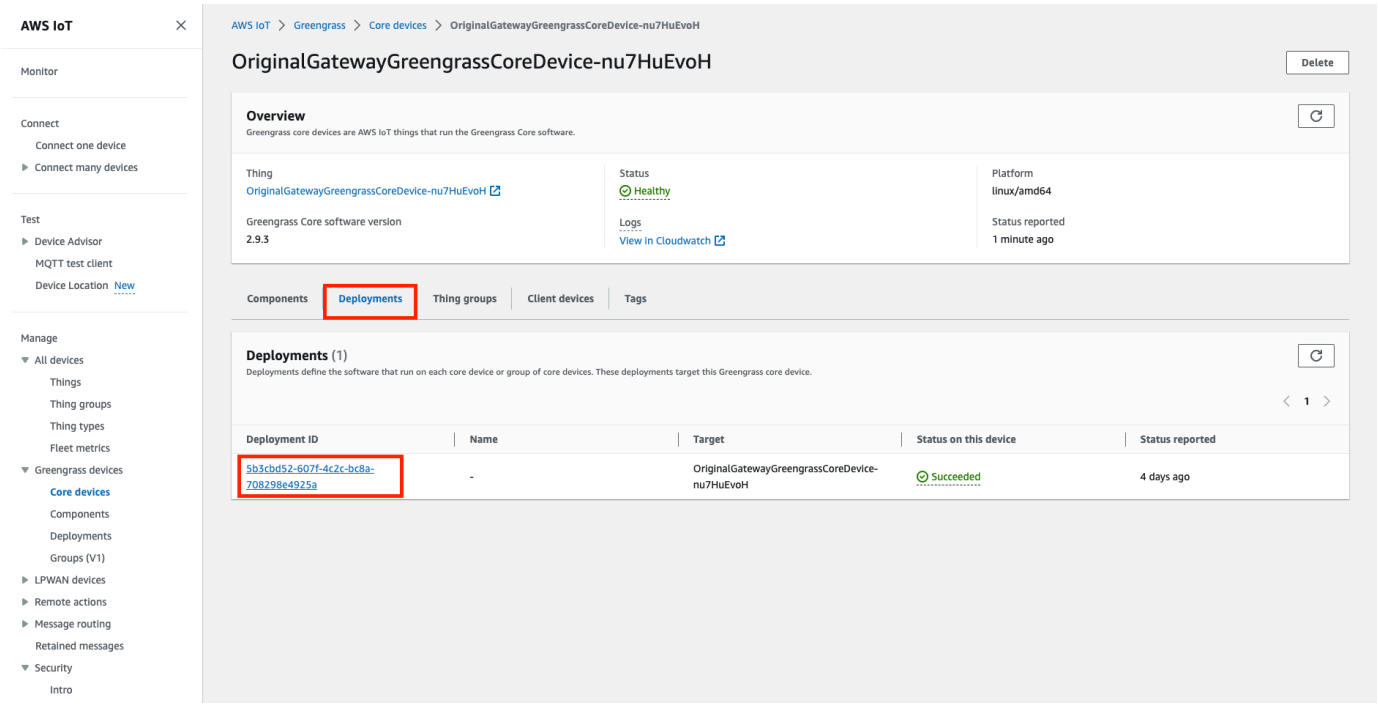
Ripristina un gateway SiteWise Edge

Utilizza la seguente procedura per ripristinare un gateway SiteWise Edge:

1. Utilizza lo script di installazione scaricato durante la creazione del gateway SiteWise Edge per ripristinare il gateway SiteWise Edge sul nuovo computer. Leggi la procedura di installazione del software SiteWise Edge gateway sul tuo dispositivo locale per configurare il gateway SiteWise Edge.

   Se perdi o non riesci a trovare lo script di installazione, contatta l'assistenza AWS clienti.
2. Una volta installato il gateway SiteWise Edge, accedi alla AWS IoT Greengrass console.
3. Per ridistribuire i componenti, vai su Gestisci, quindi in AWS IoT Greengrass Dispositivi seleziona Dispositivi principali.
4. Nella tabella dei dispositivi AWS IoT Greengrass principali, seleziona il dispositivo principale corrispondente al tuo gateway SiteWise Edge.

5. Una volta nella pagina del dispositivo, apri la scheda Distribuzioni e seleziona il tuo ID di distribuzione, si aprirà la pagina Distribuzioni con l'ID selezionato.



6. Una volta che sei nella pagina Distribuzioni, in alto a destra premi il pulsante Azioni e seleziona l'opzione Revisione. per avviare una nuova distribuzione. Configura la distribuzione. Se desideri mantenere la distribuzione così com'è, passa a Review and Deploy.

7. Attendi che lo stato di distribuzione diventi. `Completed`

> **Note**
>
> Inoltre, saranno necessari alcuni minuti prima che tutti i componenti di SiteWise Edge vengano configurati e funzionati completamente.

Ripristina AWS IoT SiteWise i dati

Utilizzare la seguente procedura per ripristinare i dati su un nuovo computer.

1. Copiare la `influxdb` cartella sul nuovo computer.
2. Arresta il SiteWise EdgeProcessor componente eseguendo il seguente comando nel tuo terminale:

Linux

```
sudo /greengrass/v2/bin/greengrass-cli component stop -n
aws.iot.SiteWiseEdgeProcessor
```

Windows

```
C:\greengrass\v2\bin\greengrass-cli component stop -n
aws.iot.SiteWiseEdgeProcesso
```

3. Individua il percorso in cui hai eseguito il backup dei dati ed esegui il seguente comando:

   Linux

   ```
   sudo yes | sudo cp -rf <influxdb_backup_path> /greengrass/v2/work/
   aws.iot.SiteWiseEdgeProcessor/influxdb
   ```

   PowerShell

   ```
   Copy-Item -Recurse -Force <influxdb_backup_path>\* C:\greengrass
   \v2\work\aws.iot.SiteWiseEdgeProcessor\
   ```

   Windows

   ```
   robocopy <influxdb_backup_path> C:\greengrass\v2\work
   \aws.iot.SiteWiseEdgeProcessor\ /E
   ```

4. Riavvia il SiteWiseEdgeProcessor componente:

   Linux

   ```
   sudo /greengrass/v2/bin/greengrass-cli component restart -n
   aws.iot.SiteWiseEdgeProcessor
   ```

   Windows

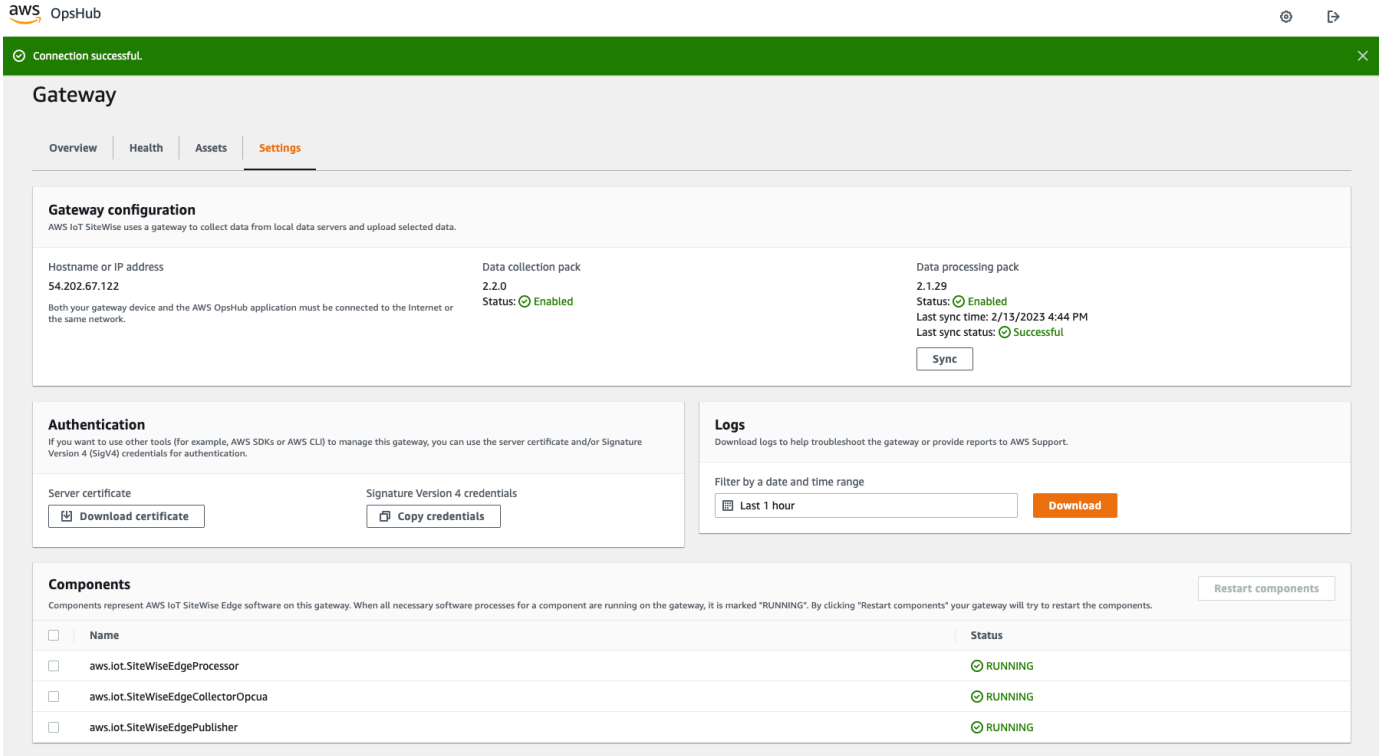
   ```
   C:\greengrass\v2\bin\greengrass-cli component restart -n
   aws.iot.SiteWiseEdgeProcessor
   ```

Convalida backup e ripristini eseguiti correttamente

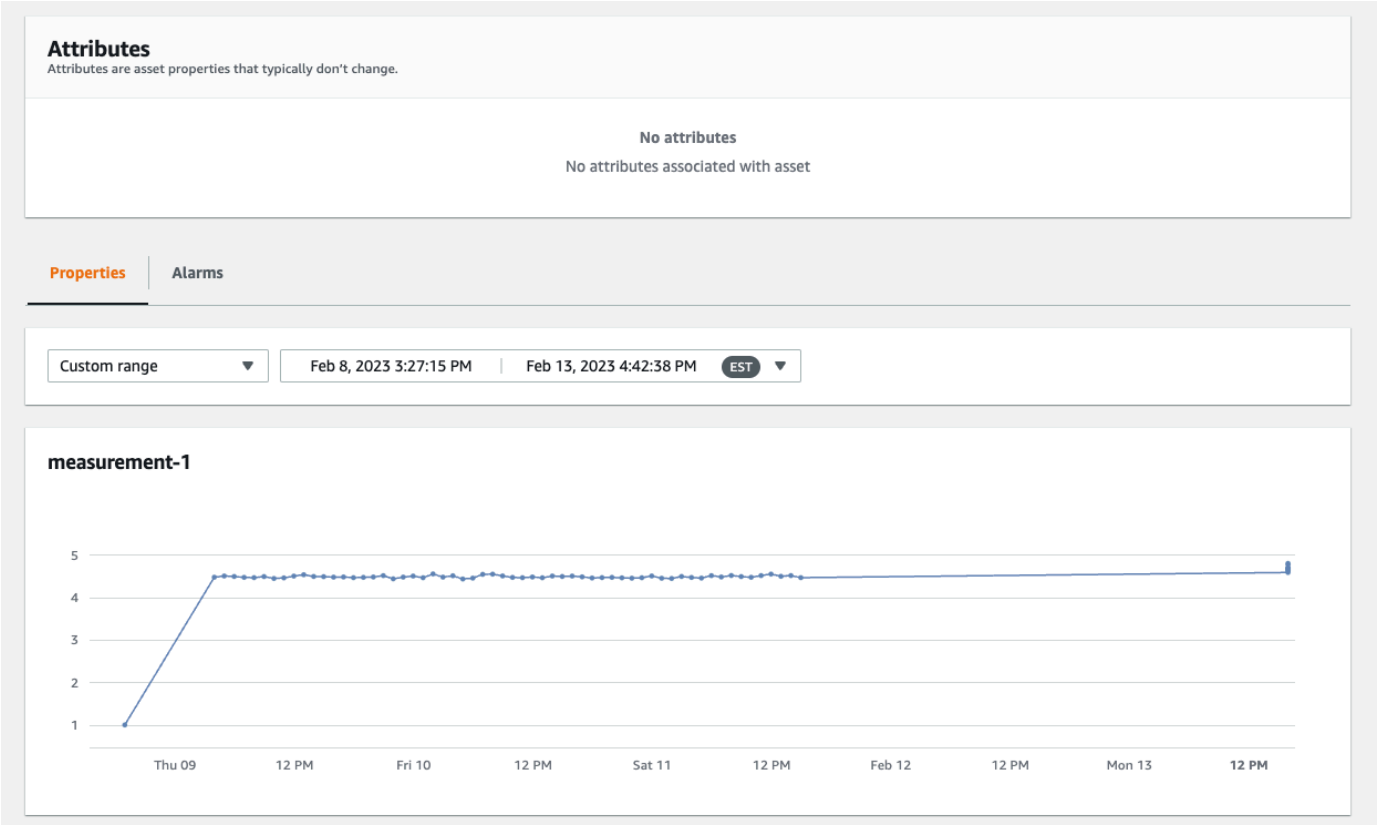
Utilizza questa procedura per convalidare i dati di backup e i ripristini del gateway Edge. SiteWise

> **Note**
>
> Questa procedura richiede l'installazione di. AWS OpsHub AWS IoT SiteWise Per ulteriori informazioni, vedere Gestione dei gateway SiteWise Edge utilizzando AWS OpsHub for AWS IoT SiteWise.

1. Aperto AWS OpsHub per AWS IoT SiteWise.
2. Nella pagina Impostazioni SiteWise Edge Gateway, controllate lo stato di ogni componente elencato nella tabella Componenti. Verificate che il colore di stato sia verde e che il display indichi RUNNING.



3. Convalida i dati precedenti nella dashboard del portale per verificare che i dati passati e i nuovi dati siano entrambi configurati correttamente. Si verificherà un periodo di inattività tra i dati passati e quelli nuovi. Dovresti fare attenzione a non visualizzare una durata in cui non vengono raccolti punti dati.



In caso di problemi con il backup o il ripristino di un gateway SiteWise Edge, consulta i seguenti argomenti di risoluzione dei problemi: Risoluzione dei problemi di un AWS IoT SiteWise gateway Edge.

Configurazione dei gateway SiteWise Edge ()AWS IoT Greengrass Version 1

> **Note**
>
> SiteWise Gli edge gateway in esecuzione AWS IoT Greengrass V1 sono disponibili solo se hai iniziato a utilizzare questa funzionalità prima del 29 luglio 2021. Altrimenti, configurerai gli SiteWise Edge gateway in esecuzione su. AWS IoT Greengrass V2

È possibile inviare dati industriali AWS IoT SiteWise utilizzando un gateway SiteWise Edge per caricare dati da apparecchiature industriali. Il gateway SiteWise Edge funge da intermediario tra le apparecchiature industriali di dati AWS IoT SiteWise e le apparecchiature industriali. AWS IoT

SiteWise fornisce AWS IoT Greengrass componenti che è possibile implementare su qualsiasi dispositivo in grado di eseguire la configurazione AWS IoT Greengrass di un gateway SiteWise Edge. AWS IoT SiteWise supporta il collegamento con il protocollo server OPC-UA.

Se disponi di gateway AWS IoT SiteWise Edge che funzionano su AWS IoT Greengrass V1, puoi aggiornare i tuoi SiteWise gateway Edge a. AWS IoT Greengrass V2 Per ulteriori informazioni, consulta Istruzioni per l'aggiornamento dei gateway SiteWise Edge da a. AWS IoT Greengrass V1 AWS IoT Greengrass V2

Argomenti

- Scelta di un dispositivo gateway AWS IoT Greengrass V1 SiteWise Edge
- Configurazione di un gateway AWS IoT Greengrass V1 SiteWise Edge
- Configurazione delle fonti di dati sui AWS IoT Greengrass V1 SiteWise gateway Edge

Scelta di un dispositivo gateway AWS IoT Greengrass V1 SiteWise Edge

Scegliete il dispositivo locale più adatto alle vostre attività industriali. Puoi configurare un gateway SiteWise Edge su qualsiasi dispositivo in grado di funzionare AWS IoT Greengrass. Tutti i dispositivi locali devono soddisfare i seguenti requisiti:

- Supporta il software AWS IoT Greengrass Core v1.10.2 o successivo. Per ulteriori informazioni, consulta Piattaforme e requisiti supportati nella Guida per gli AWS IoT Greengrass Version 1 sviluppatori.
- Dispone di almeno 4 GB di RAM.
- Almeno 10 GB di spazio libero su disco.
- Supporto di una macchina virtuale Java 8 (JVM).

Se si prevede di elaborare i dati in modalità edge con AWS IoT SiteWise, il dispositivo locale deve inoltre soddisfare i seguenti requisiti:

- Dispone di un processore quad-core x86 a 64 bit.
- Dispone di almeno 16 GB di RAM.
- Dispone di almeno 32 GB di RAM se si utilizza Windows.
- Aveva almeno 256 GB di spazio libero su disco.

Lo spazio su disco necessario per memorizzare nella cache i dati relativi alla connettività Internet intermittente dipende dai seguenti fattori:

- Numero di flussi di dati caricati
- Punti dati per flusso di dati al secondo
- Dimensione di ciascun punto dati
- Velocità di comunicazione
- Tempo previsto di inattività della rete

La capacità di elaborazione necessaria per il polling e il caricamento dei dati dipende dai seguenti fattori:

- Numero di flussi di dati caricati
- Punti dati per flusso di dati al secondo

Configurazione di un gateway AWS IoT Greengrass V1 SiteWise Edge

Un gateway AWS IoT SiteWise Edge funge da intermediario tra le apparecchiature industriali e AWS IoT SiteWise. È possibile implementare il software SiteWise Edge gateway su qualsiasi dispositivo in grado di funzionare. AWS IoT Greengrass Per ulteriori informazioni, consulta Scelta di un dispositivo gateway AWS IoT Greengrass V1 SiteWise Edge.

È possibile AWS IoT SiteWise abilitare l'elaborazione dei dati localmente sui dispositivi edge utilizzando il pacchetto di elaborazione dati sul gateway SiteWise Edge. Questa operazione viene eseguita quando si aggiunge il gateway SiteWise Edge a AWS IoT SiteWise. Per ulteriori informazioni sull'elaborazione dei dati all'edge, consultathe section called “Abilitare l'elaborazione dei dati edge”.

> **Note**
>
> Ti consigliamo di completare i seguenti passaggi con un utente che disponga di accesso amministrativo IT alle reti locali e aziendali. Questi passaggi potrebbero richiedere qualcuno con conoscenza delle apparecchiature industriali e l'autorità per configurare le impostazioni del firewall.

Argomenti

- Configurazione dell'ambiente gateway SiteWise Edge
- Creazione di una politica e di un ruolo IAM
- Configurazione di un gruppo AWS IoT Greengrass
- Configurazione del connettore AWS IoT SiteWise
- Aggiungere il gateway SiteWise Edge a AWS IoT SiteWise

Configurazione dell'ambiente gateway SiteWise Edge

In questa procedura, installi AWS IoT Greengrass e configuri il gateway SiteWise Edge da utilizzare con AWS IoT SiteWise.

> **Note**
>
> Questa sezione include le istruzioni per l'installazione dei pacchetti con il comando `apt`. La procedura è riservata ai sistemi che eseguono Ubuntu o simili. Se non si utilizza un sistema simile, basta consultare la documentazione relativa alla propria distribuzione e avvalersi del programma di installazione del pacchetto consigliato.

Per configurare il gateway SiteWise Edge

1. Se necessario, modificare le impostazioni del BIOS del gateway SiteWise Edge come segue.
   a. Assicuratevi che il gateway SiteWise Edge si riavvii automaticamente dopo una potenziale interruzione dell'alimentazione, se applicabile.
   b. Assicurati che il gateway SiteWise Edge non vada in letargo o non sia in modalità di sospensione, se applicabile.
2. Assicurati che il gateway SiteWise Edge si connetta a Internet.
3. (Facoltativo) Per utilizzare il gateway SiteWise Edge senza mouse, tastiera e monitor, effettuate le seguenti operazioni di configurazione `ssh` sul gateway SiteWise Edge:
   a. Se non è già stato fatto, installare il pacchetto SSH con il comando seguente.

      ```
      sudo apt install ssh
      ```

   b. Esegui il comando seguente.

```
service ssh status
```

c. Per verificare che il server SSH sia in esecuzione, cercare `Active: active (running)` nell'output.

d. Premere Q per uscire.

Esegui il comando seguente per utilizzare SSH per connetterti al gateway SiteWise Edge da un altro computer. Sostituisci il *`nome utente`* con il login dell'utente e l'*`IP`* con l'indirizzo IP del gateway SiteWise Edge.

```
ssh username@IP
```

È possibile utilizzare l'argomento `-p` *`port-number`* per connettersi a una porta diversa dalla porta predefinita 22.

4. Scarica e installa il software AWS IoT Greengrass Core v1.10.2 o versione successiva e crea un AWS IoT Greengrass gruppo per il tuo SiteWise gateway Edge. A tale scopo, seguire le istruzioni riportate in Nozioni di base su AWS IoT Greengrass nella Guida per gli sviluppatori di AWS IoT Greengrass .

   Si consiglia di eseguire lo script di installazione del dispositivo AWS IoT Greengrass per iniziare rapidamente. Se desideri esaminare AWS IoT Greengrass i requisiti e i processi più da vicino, puoi seguire i passaggi del Modulo 1 e del Modulo 2 per la configurazione. AWS IoT Greengrass

   > **Important**
   >
   > Consulta le AWS regioni in cui AWS IoT SiteWise è supportato. Quando scegli una regione per AWS IoT Greengrass, assicurati che anche la regione supporti AWS IoT SiteWise. Altrimenti, non puoi connettere il tuo gateway SiteWise Edge a AWS IoT SiteWise.

   Prima di passare alla fase successiva, è necessario che il software AWS IoT Greengrass Core sia installato sul gateway SiteWise Edge.

5. Eseguire i comandi seguenti per installare Java 8.

```
sudo apt update
```

```
      sudo apt install openjdk-8-jre
```

Il software SiteWise Edge gateway che installerai più avanti in questa guida utilizza un runtime Java 8.

6. Per verificare che Java sia stato installato, eseguire il comando riportato di seguito.

```
java -version
```

7. Il software AWS IoT Greengrass Core presuppone una `java8` directory. L'esecuzione del comando che segue permette il collegamento dell'installazione Java alla suddetta directory `java8`.

```
sudo ln -s /usr/bin/java /usr/bin/java8
```

8. Esegui il seguente comando per creare una directory di `/var/sitewise` dati e assegnare le `ggc_user` autorizzazioni per quella directory. AWS IoT SiteWise memorizza i dati in questa directory. È stato creato `ggc_user` durante la configurazione AWS IoT Greengrass precedente in questa procedura.

```
sudo mkdir /var/sitewise
      sudo chown ggc_user /var/sitewise
      sudo chmod 700 /var/sitewise
```

La `/var/sitewise` è la directory predefinita che AWS IoT SiteWise utilizza. È possibile personalizzare il percorso della directory (ad esempio sostituirlo `/var/sitewise` con/ `var/`*`custom`*`/`*`path`*`/`), ma per farlo sono necessari passaggi aggiuntivi dopo la creazione del gateway SiteWise Edge. Per ulteriori informazioni, consultare la fase 6 in Configurazione del connettore AWS IoT SiteWise.

9. Se necessario, chiedere all'amministratore IT di aggiungere gli endpoint e le porte seguenti all'elenco di indirizzi consentiti della rete locale.

   - Porte: 443, 8443 e 8883

> **Important**
>
> È possibile configurare AWS IoT Greengrass Core in modo che utilizzi solo la porta 443 per tutte le comunicazioni di rete. Per ulteriori informazioni, consulta Connessione

alla porta 443 o tramite un proxy di rete nella Guida per sviluppatori AWS IoT Greengrass .

- L'indirizzo IP del gateway SiteWise Edge (porta 443). Per ottenere l'indirizzo IP, basta eseguire il comando `ip address` o `ifconfig` e prendere nota del valore `inet` (ad esempio, `203.0.113.0`).
- L'endpoint AWS IoT SiteWise dei dati: `data.iotsitewise.`*`region`*`.amazonaws.com` (porta 443).
- I seguenti AWS endpoint utilizzati dal gateway SiteWise Edge. Sono disponibili nel file `/`*`greengrass-root`*`/config/config.json`. Sostituire *`greengrass-root`* con la root dell'installazione AWS IoT Greengrass .
  - ggHost: `greengrass-ats.iot.`*`region`*`.amazonaws.com` (porte 443, 8443 e 8883).
  - iotHost: *`prefix`*`-ats.iot.`*`region`*`.amazonaws.com` (porte 443, 8443 e 8883).

  Per ulteriori informazioni, consulta Endpoint e quote per AWS IoT Greengrass.

10. Se il software AWS IoT Greengrass Core non è già in esecuzione, esegui il comando seguente per avviare il software AWS IoT Greengrass Core. Sostituisci *`greengrass-root`* con la radice dell'installazione. AWS IoT Greengrass Il valore predefinito di *`greengrass-root`* è `/greengrass`.

    ```
    cd /greengrass-root/ggc/core
          sudo ./greengrassd start
    ```

    Dovrebbe comparire questo messaggio: `Greengrass successfully started with PID:` *`some-PID-number`*

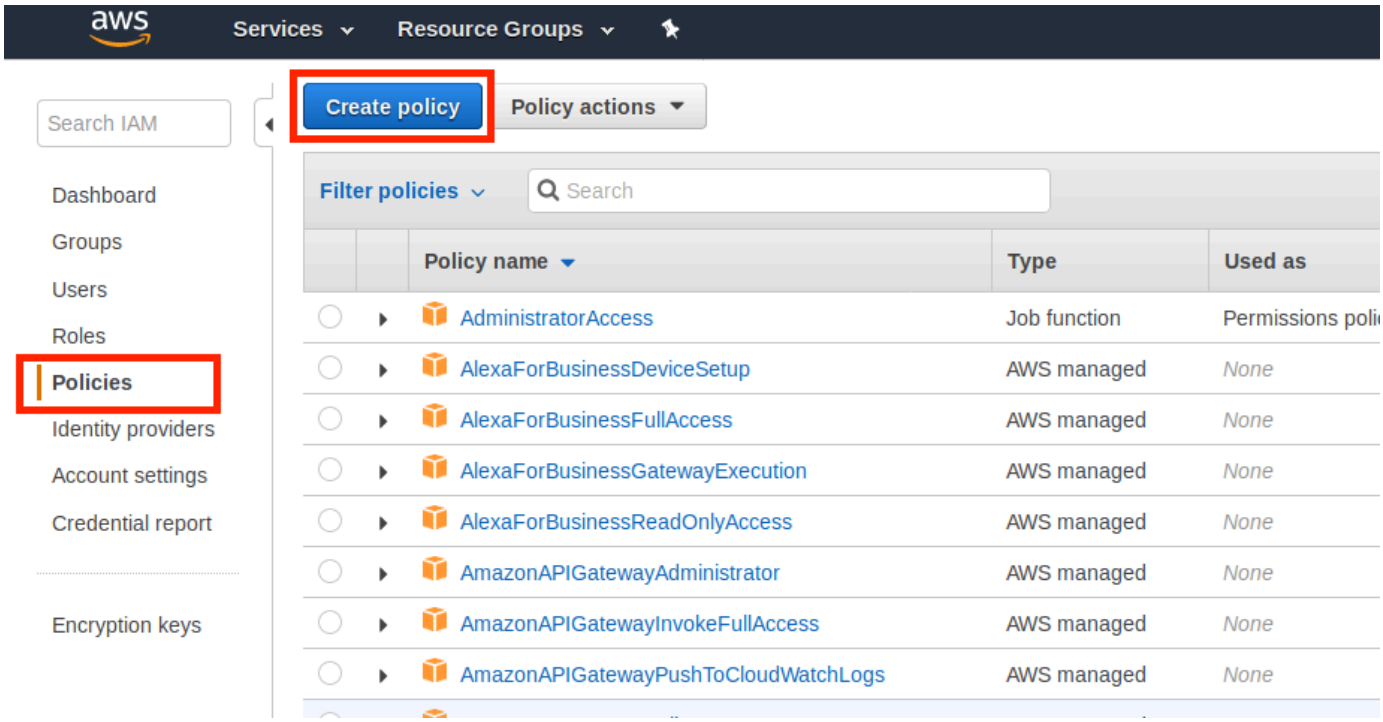
11. Configura il software AWS IoT Greengrass Core in modo che si avvii automaticamente all'accensione del gateway SiteWise Edge. Consulta la documentazione relativa al sistema operativo del tuo gateway SiteWise Edge.

Creazione di una politica e di un ruolo IAM

Devi creare una policy e un ruolo AWS Identity and Access Management (IAM) per consentire al gateway SiteWise Edge di accedere per tuo AWS IoT SiteWise conto.

Per creare una policy e un ruolo IAM

1. Passare alla IAM console (Console IAM).
2. Nel riquadro di navigazione, seleziona Policy e quindi Crea policy.



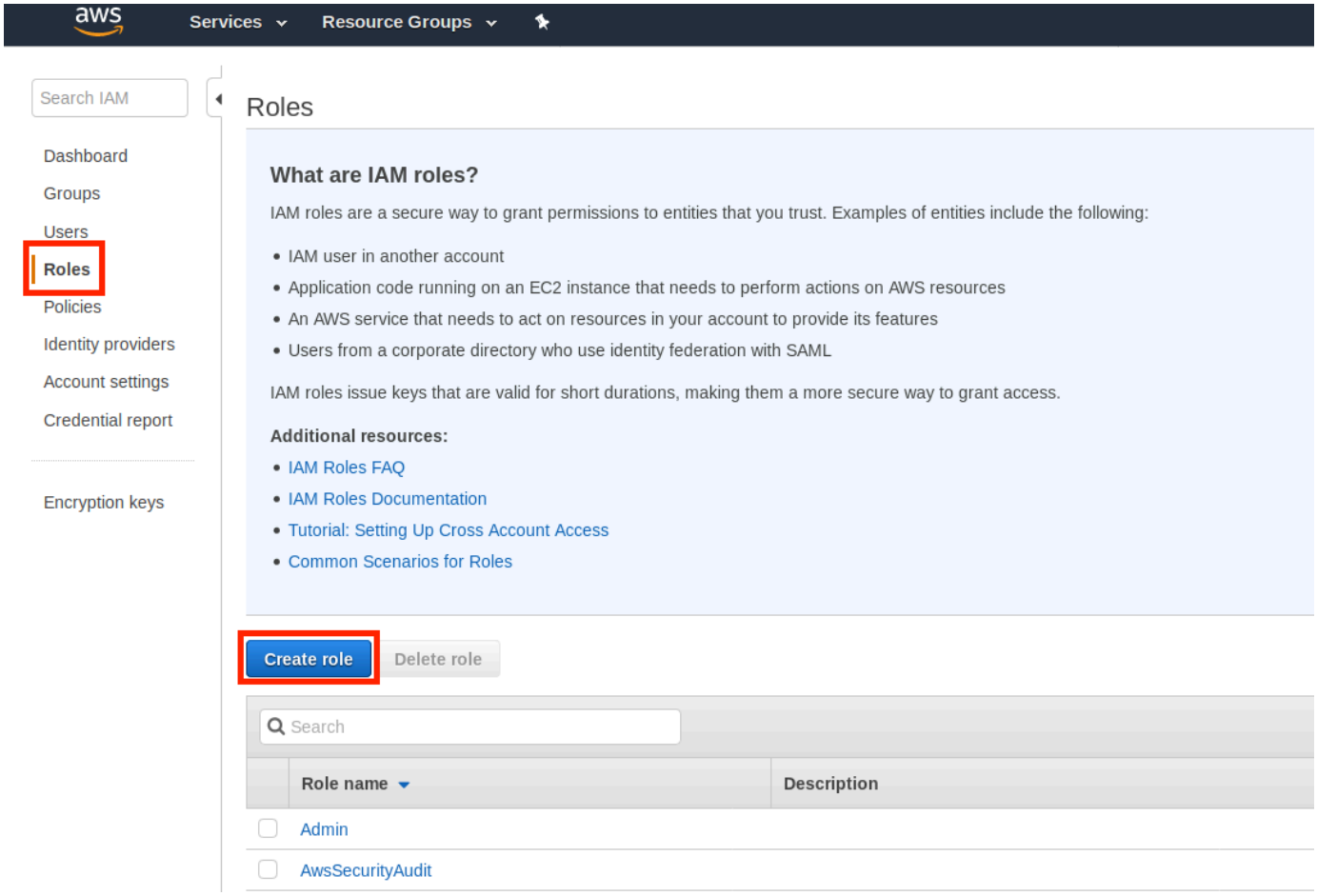
3. Selezionare la scheda JSON, eliminare i contenuti presenti nel campo della policy e incollarvi quanto segue.

```
{
        "Version": "2012-10-17",
        "Statement": [
          {
            "Effect": "Allow",
            "Action": "iotsitewise:BatchPutAssetPropertyValue",
            "Resource": "*"
          }
        ]
      }
```

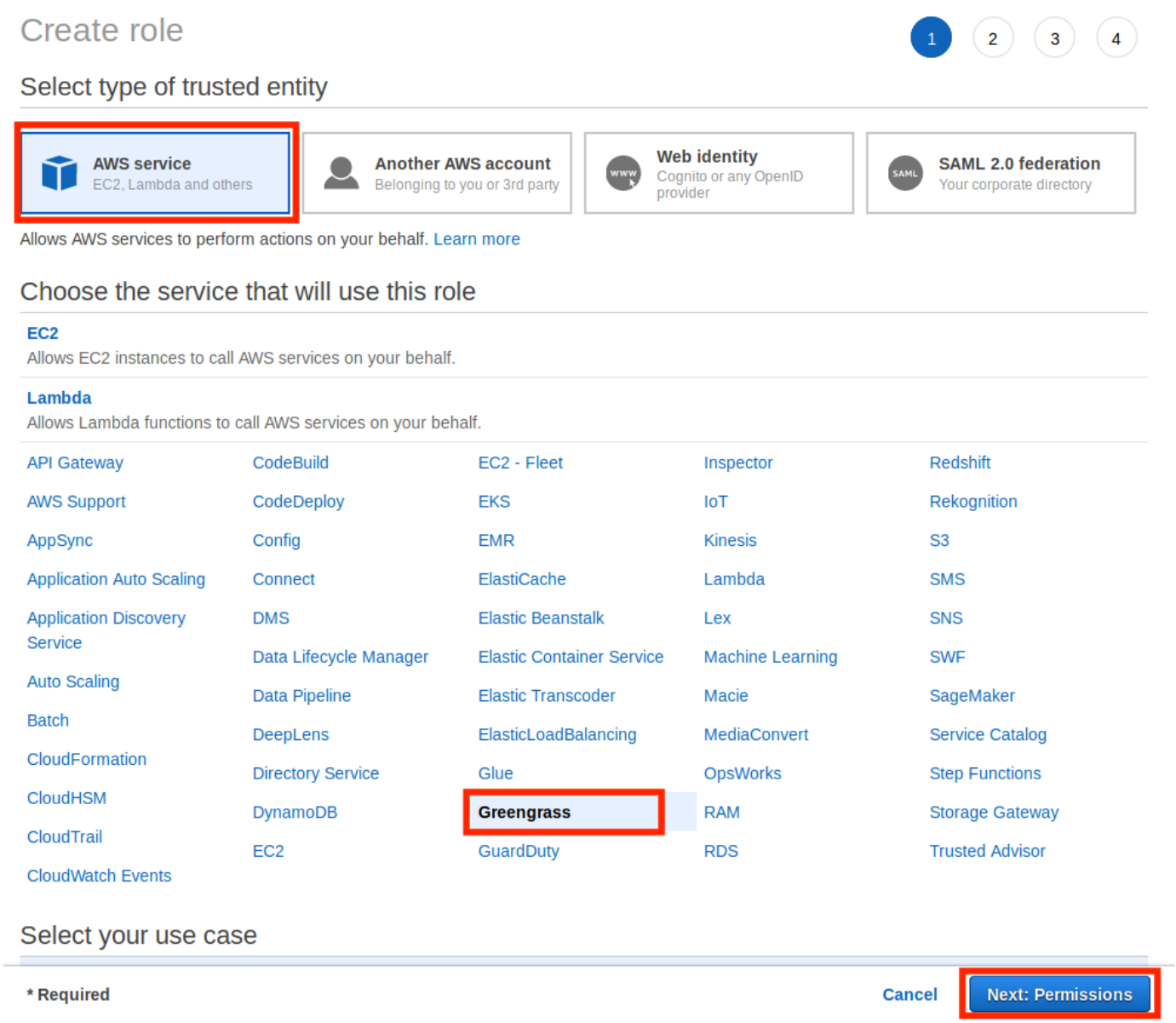
> **Note**
>
> Per migliorare la sicurezza, puoi specificare un percorso di gerarchia AWS IoT SiteWise degli asset nella `Condition` proprietà. L'esempio seguente è una policy di attendibilità che specifica un percorso della gerarchia di un asset.

```
{
        "Version": "2012-10-17",
        "Statement": [
          {
            "Effect": "Allow",
            "Action": "iotsitewise:BatchPutAssetPropertyValue",
            "Resource": "*",
            "Condition": {
              "StringLike": {
                "iotsitewise:assetHierarchyPath": [
                  "/root node asset ID",
                  "/root node asset ID/*"
                ]
              }
            }
          }
        ]
      }
```

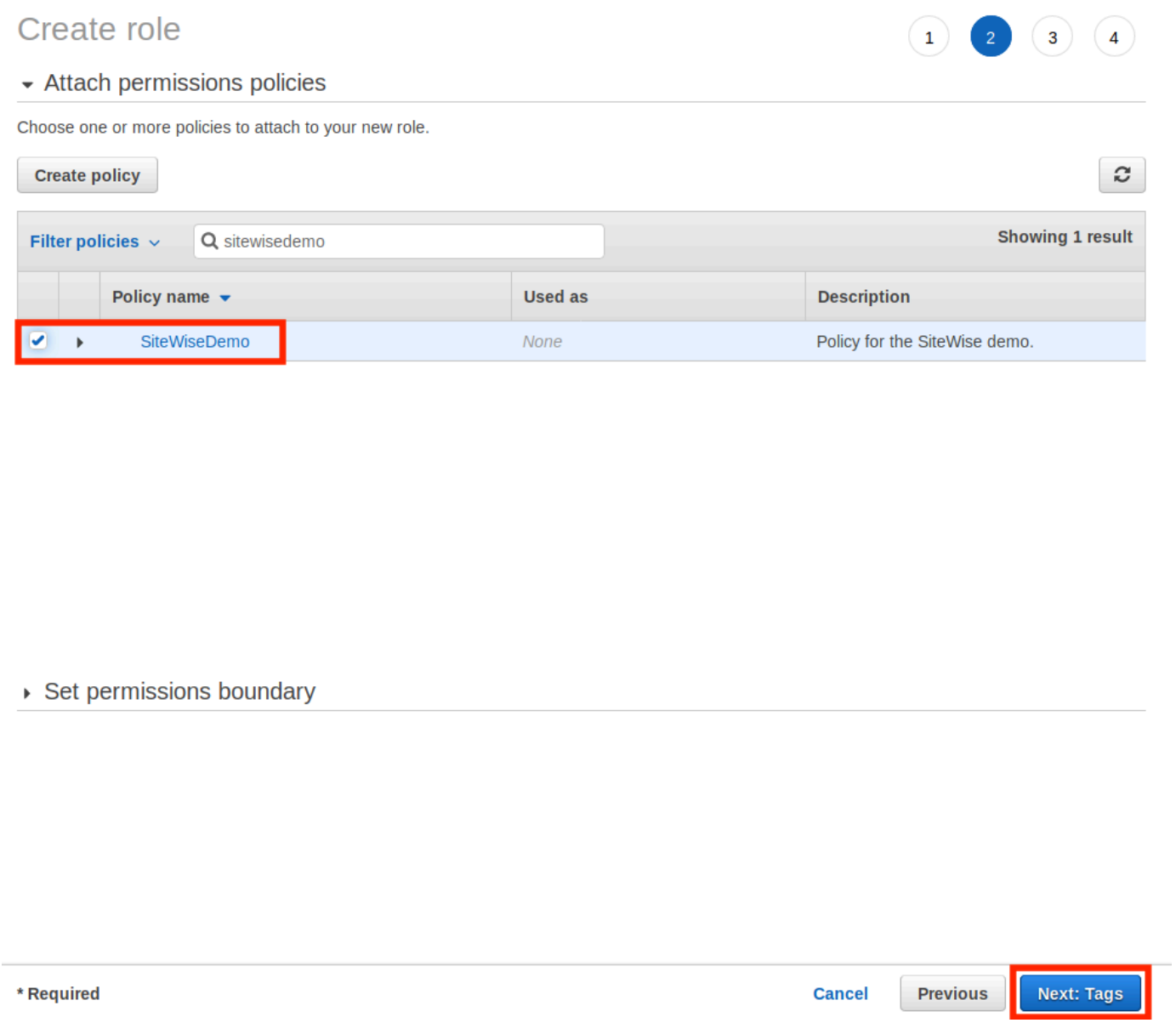
4. Scegli Verifica policy.
5. Immettere un nome e una descrizione per la policy e quindi scegliere Crea policy.
6. Nel riquadro di navigazione, scegli Ruoli e quindi Crea ruolo.



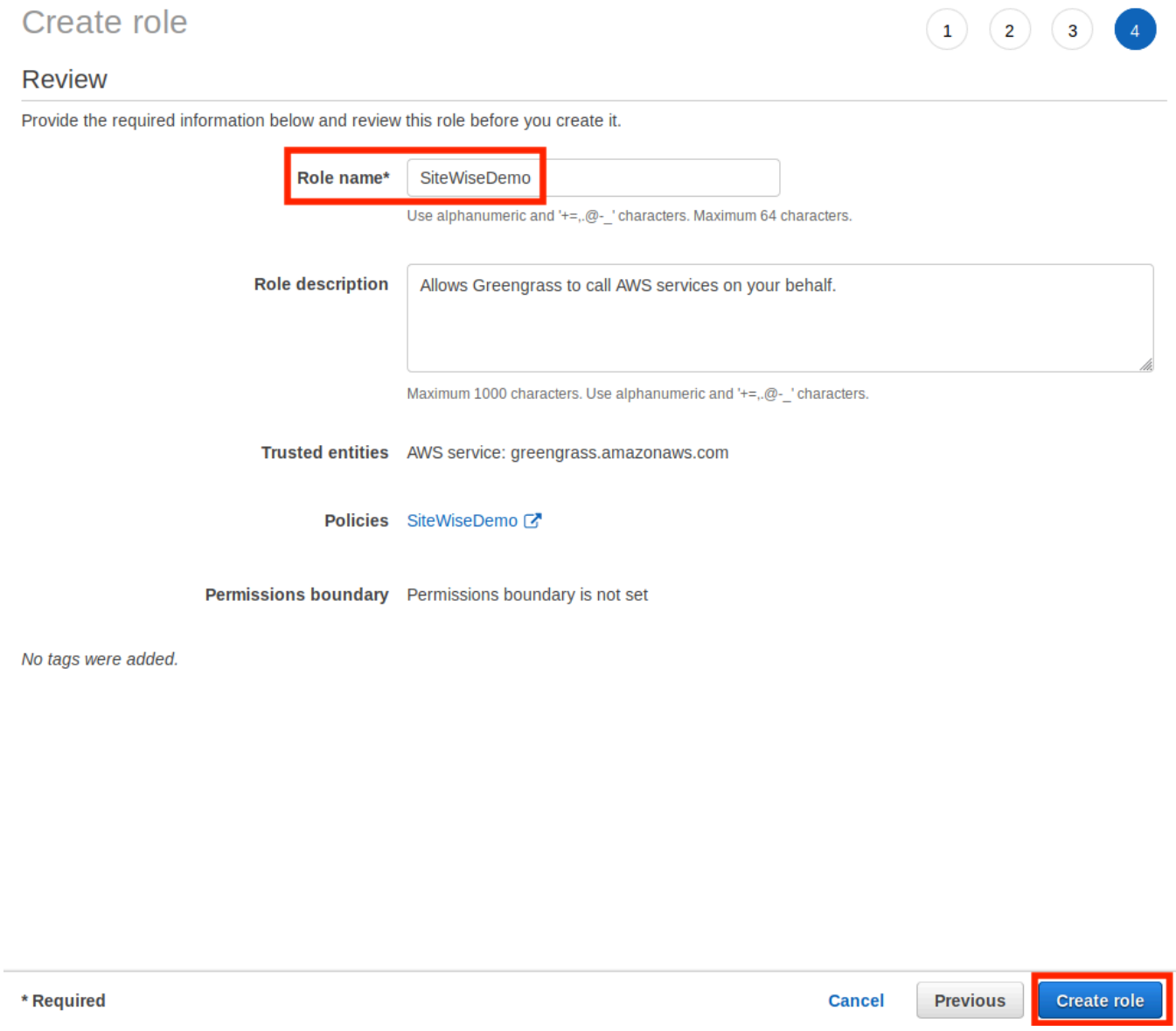
7. In Select type of trusted entity (Seleziona tipo di entità attendibile), scegli AWS service (Servizio). In Scegli il servizio che utilizzerà questo ruolo, scegliere Greengrass come servizio che utilizzerà il ruolo, quindi Successivo: Autorizzazioni.



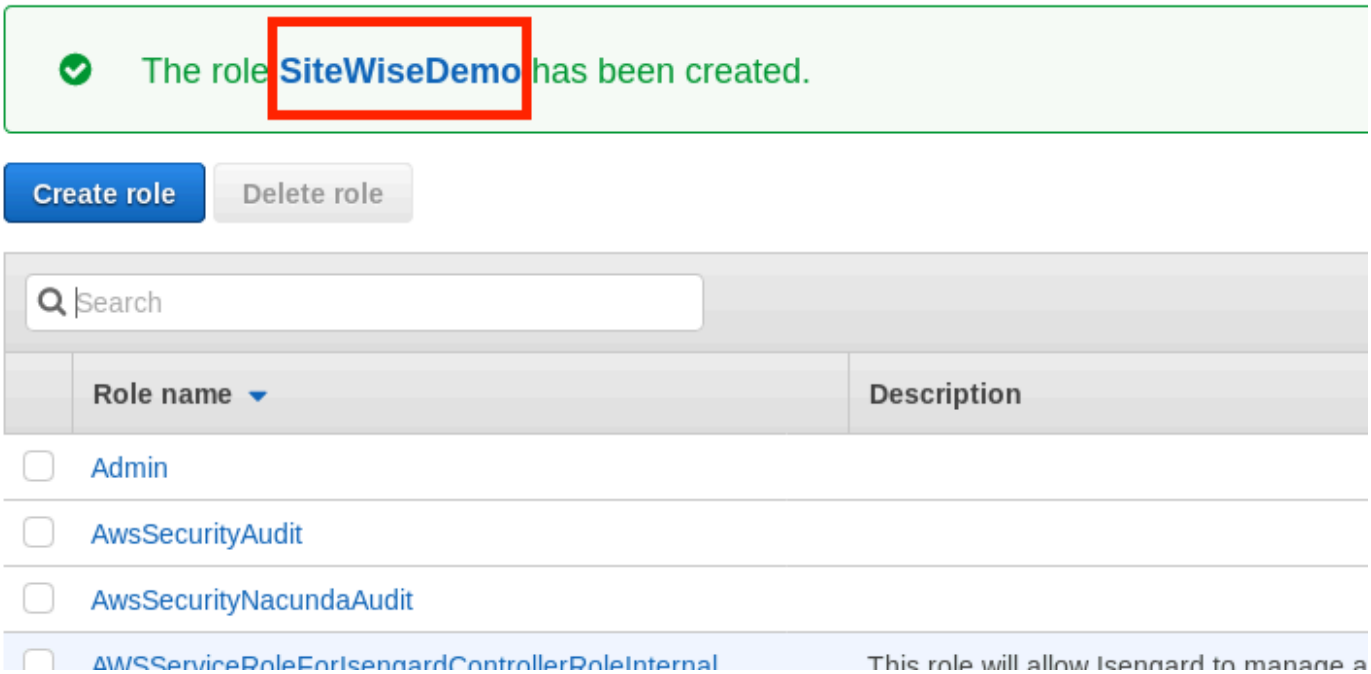
8. Cerca la policy che hai creato, seleziona la casella di controllo, quindi scegli Avanti: Tag.



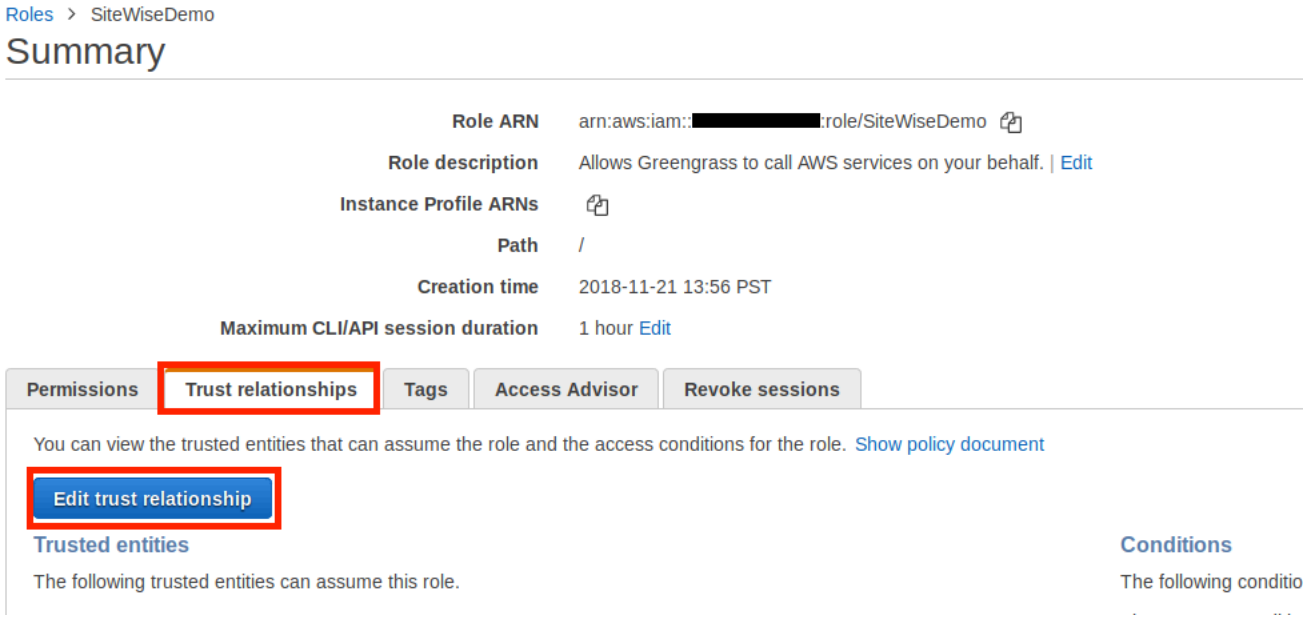
9. (Facoltativo) Aggiungere tag al ruolo, quindi scegliere Next: Review (Successivo: Verifica).
10. Immettere un nome e una descrizione per il ruolo e quindi scegliere Crea ruolo.



11. Nel banner verde, selezionare il collegamento al nuovo ruolo. Per trovare il ruolo si può anche utilizzare il campo di ricerca.



12. Selezionare la scheda Trust relationships (Relazioni di trust) e scegliere Edit trust relationship (Modifica relazione di trust).



13. Sostituire il contenuto corrente del campo della policy con il seguente, quindi scegliere Update Trust Policy (Aggiorna policy di trust).

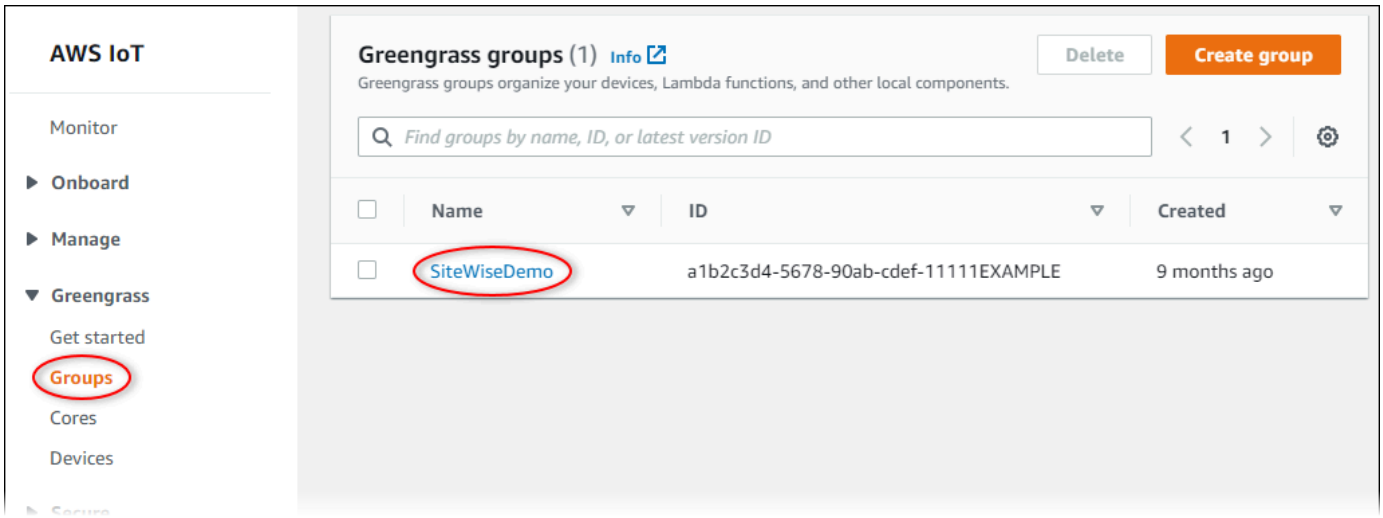
```
{
        "Version": "2012-10-17",
        "Statement": [
```

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

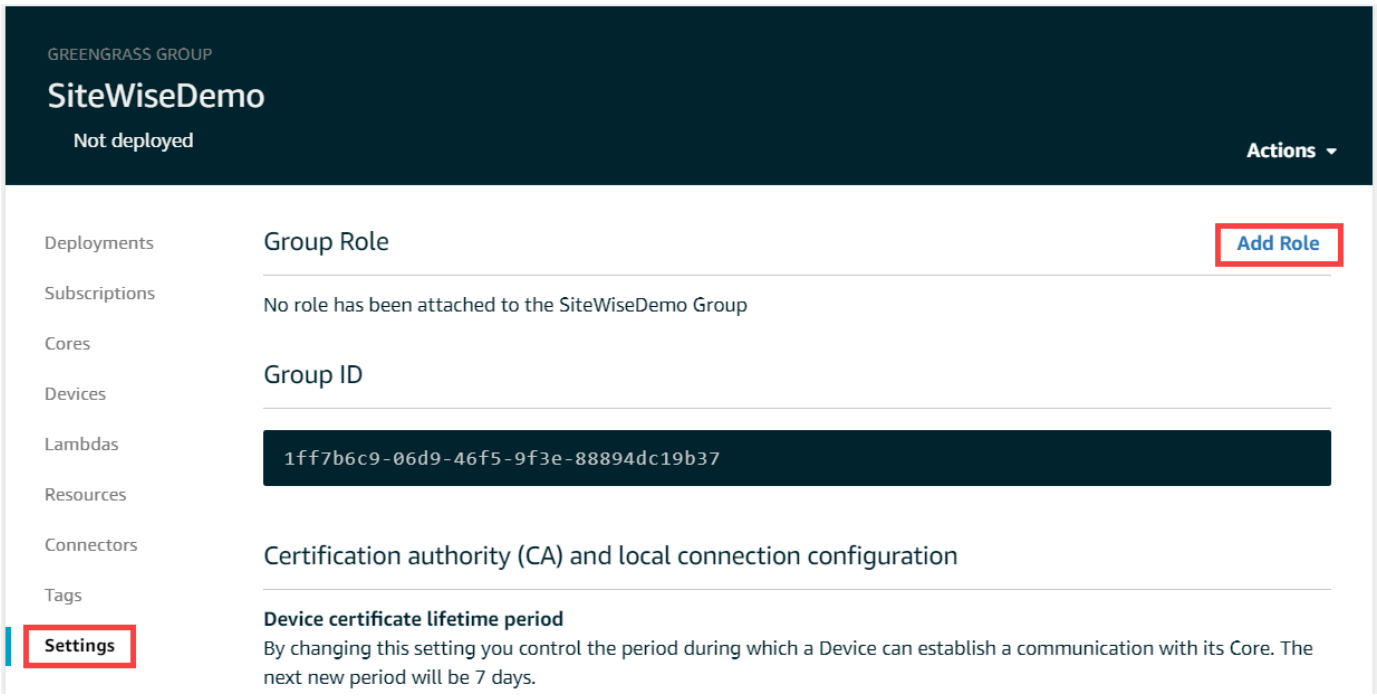
Configurazione di un gruppo AWS IoT Greengrass

Per assegnare un ruolo IAM a un gruppo e abilitare lo stream manager

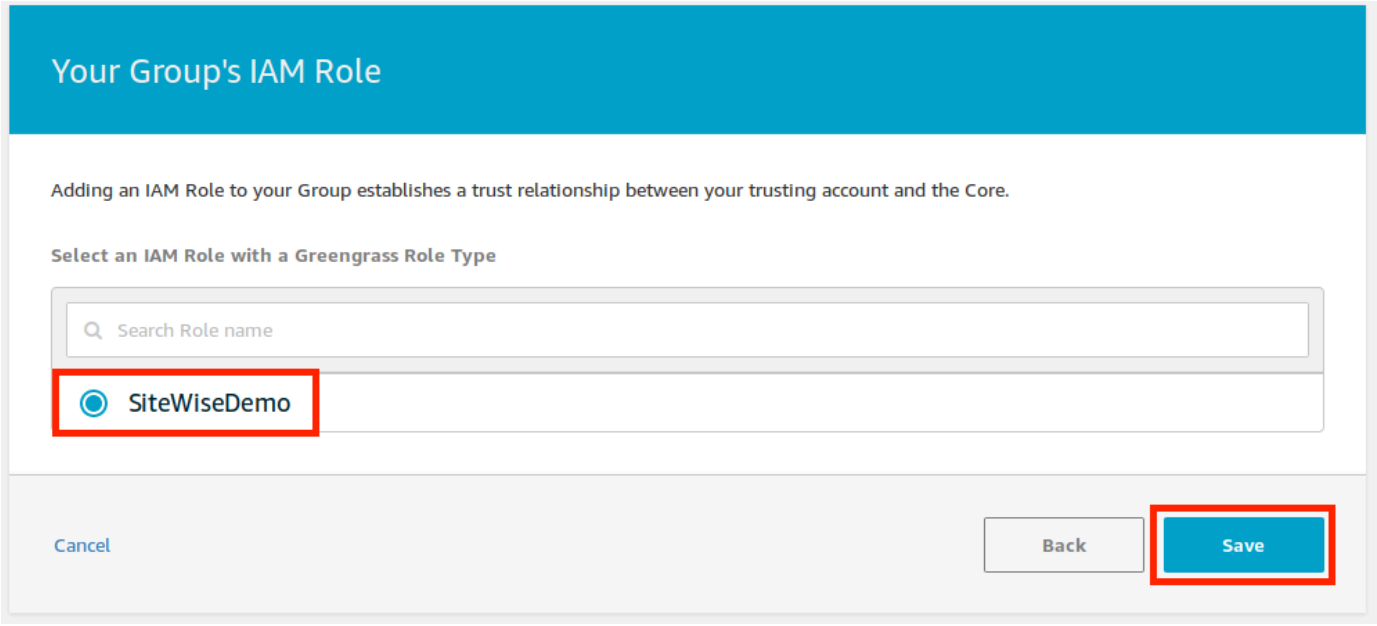
1. Passare alla console AWS IoT Greengrass.
2. Nel riquadro di navigazione a sinistra, sotto Greengrass scegliere Groups (Gruppi), quindi selezionare il gruppo creato in Configurazione dell'ambiente gateway SiteWise Edge.



3. Nel riquadro di navigazione a sinistra scegliere Impostazioni. Nella sezione Group Role (Ruolo di gruppo), scegliere Add role (Aggiungi ruolo).

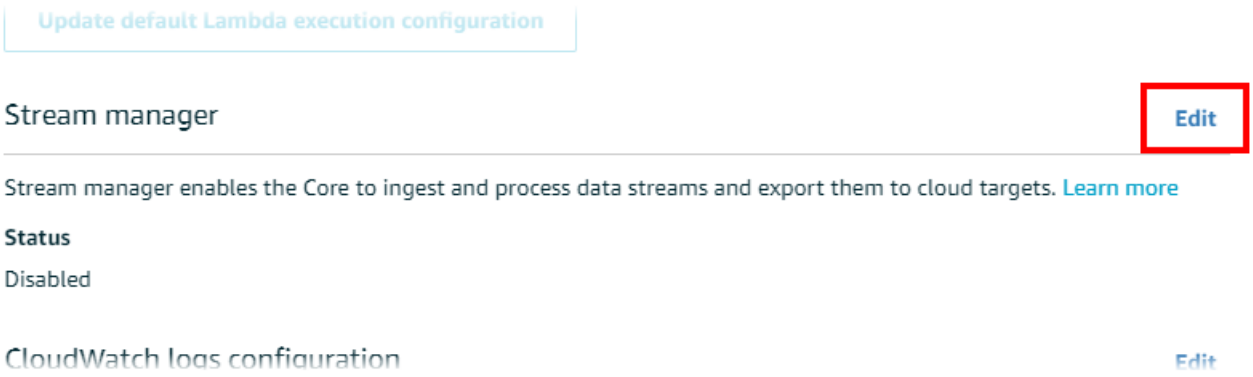


4. Scegliere il ruolo creato in Creazione di una politica e di un ruolo IAM, quindi selezionare Save (Salva).



5. Nella pagina Impostazioni, nella sezione Stream manager, scegli Modifica.

   Stream manager è una funzionalità AWS IoT Greengrass che consente a AWS IoT Greengrass Core di trasmettere dati al AWS Cloud. SiteWise I gateway edge richiedono che lo stream manager sia abilitato. Per ulteriori informazioni, consulta Manage data stream on the AWS IoT Greengrass Core nella AWS IoT Greengrass Version 1 Developer Guide.



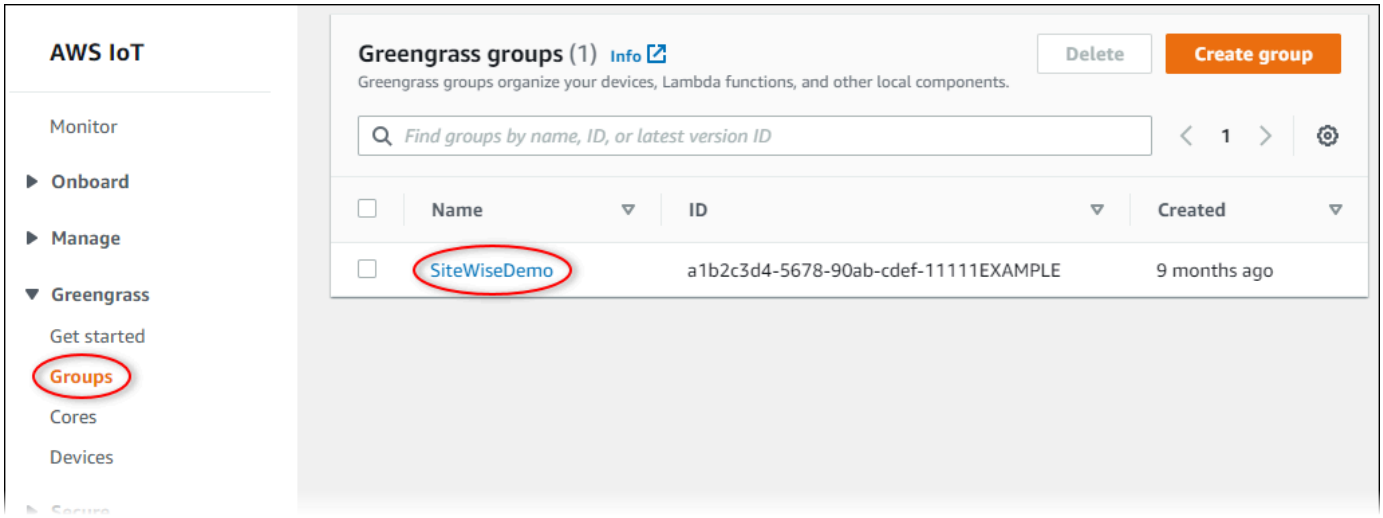
6. Scegliere Enable (Abilita), quindi Save (Salva).
7. Nell'angolo in alto a sinistra, scegliere Services (Servizi) per prepararsi alla fase successiva.

Configurazione del connettore AWS IoT SiteWise

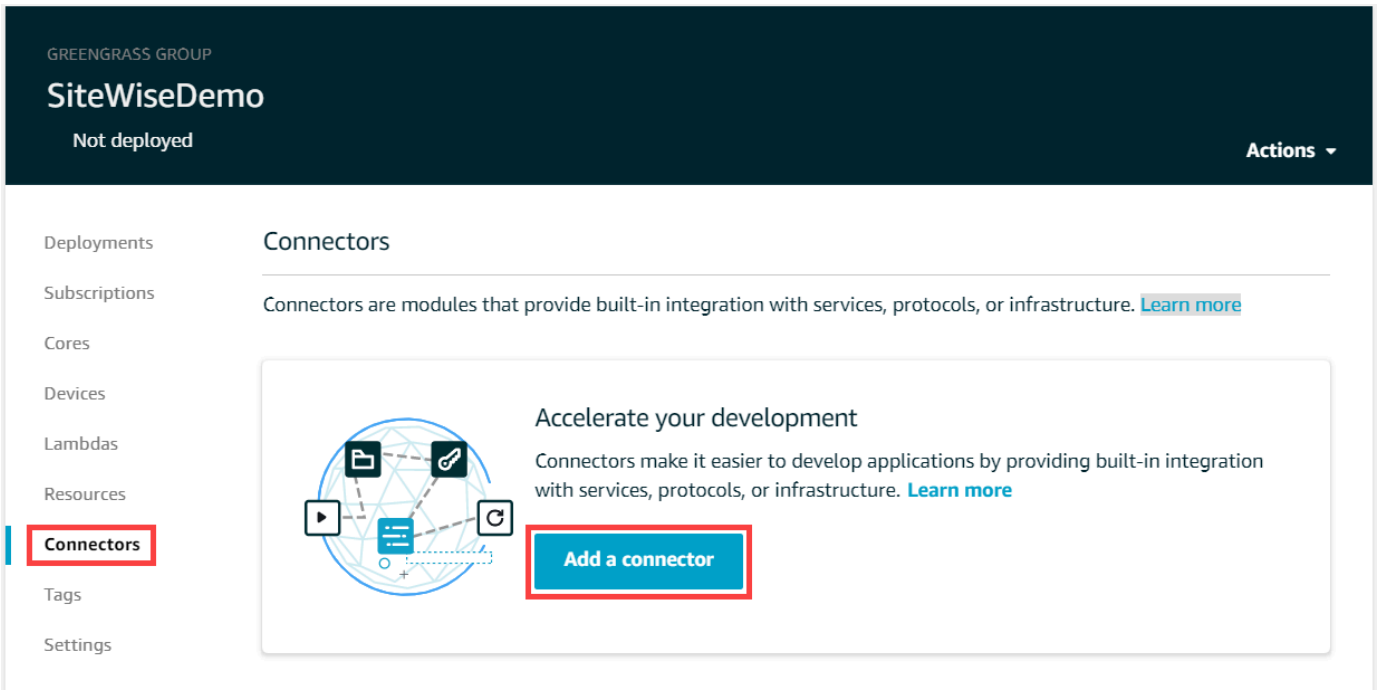
In questa procedura, configuri il AWS IoT SiteWise connettore sul tuo gruppo Greengrass. I componenti sono moduli predefiniti che accelerano il ciclo di vita dello sviluppo per scenari edge comuni. Per ulteriori informazioni, consulta i AWS IoT Greengrass connettori nella Guida per gli AWS IoT Greengrass Version 1 sviluppatori.

Per configurare il AWS IoT SiteWise connettore

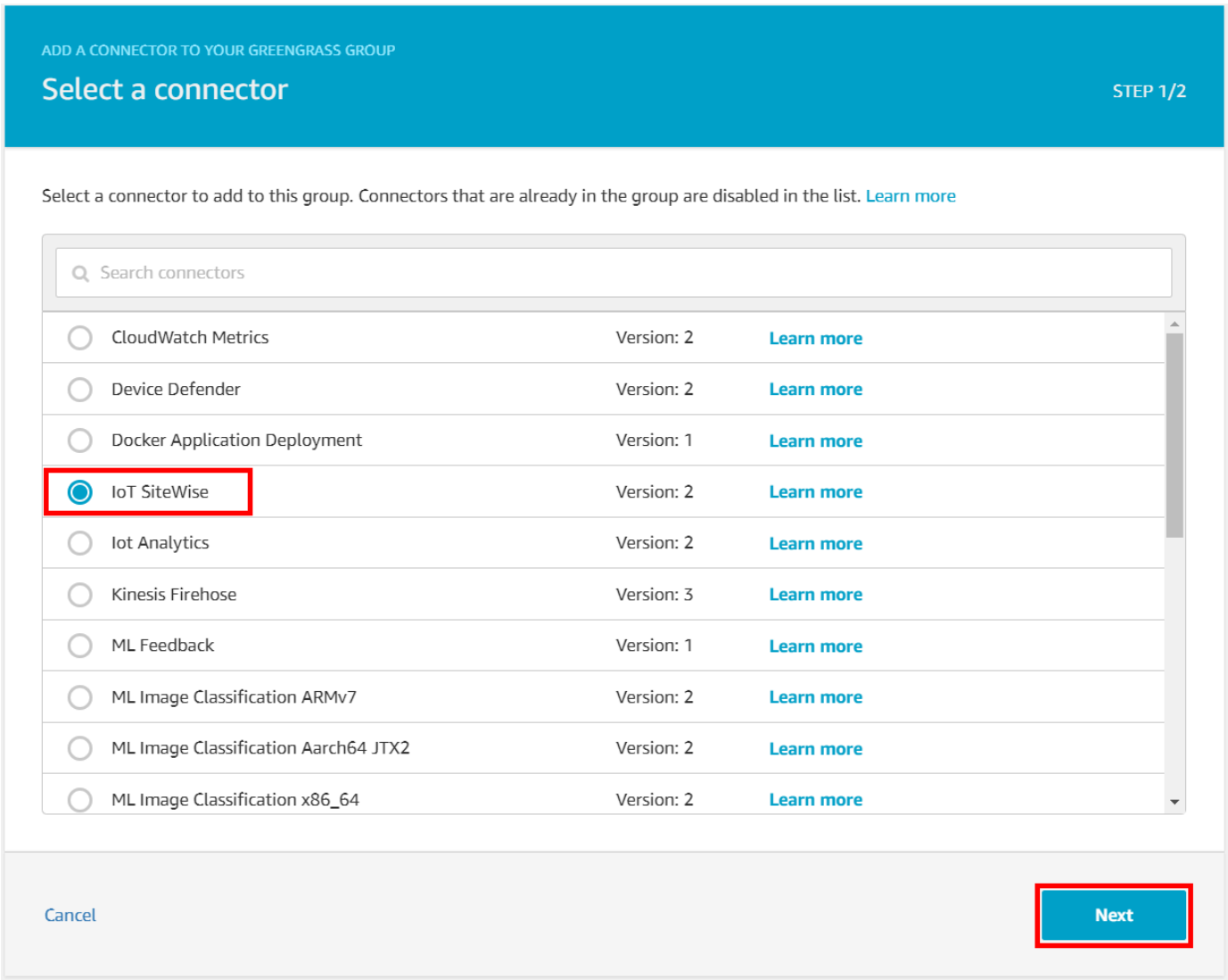
1. Passare alla console AWS IoT Greengrass.
2. Nel riquadro di navigazione a sinistra, sotto Greengrass scegliere Groups (Gruppi), quindi selezionare il gruppo creato in Configurazione dell'ambiente gateway SiteWise Edge.



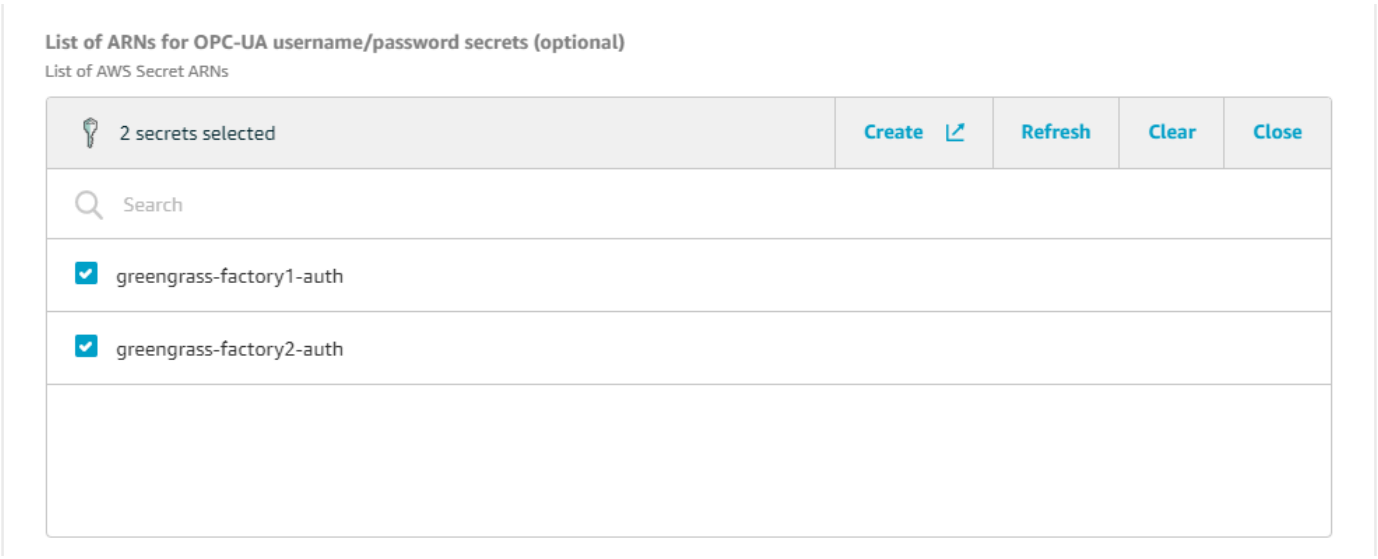
3. Nel riquadro di navigazione a sinistra, selezionare Connectors (Connettori). Alla pagina Connectors (Connettori), selezionare Add a connector (Aggiungi un connettore).



4. Scegli IoT SiteWise dall'elenco e scegli Avanti.



5. Se il server richiede l'autenticazione, puoi creare AWS Secrets Manager segreti con il nome utente e la password del server. Quindi, puoi allegare ogni segreto al tuo gruppo Greengrass e sceglierlo in Elenco di ARN per i segreti di nome utente/password. Per ulteriori informazioni su come creare e configurare i segreti, consulta Configurazione dell'autenticazione dell'origine. È inoltre possibile aggiungere segreti al connettore in un secondo momento.



6. Se configuri il gateway SiteWise Edge con un percorso diverso da quello`/var/sitewise`, inserisci quel percorso per Percorso di archiviazione locale.
7. (Facoltativo) Specificare la dimensione massima del buffer del disco per il connettore. Se il AWS IoT Greengrass core perde la connessione al AWS Cloud, il connettore memorizza i dati nella cache finché non riesce a connettersi correttamente. Se la dimensione della cache supera la dimensione massima del buffer del disco, il connettore elimina i dati meno recenti dalla coda.
8. Scegli Aggiungi.
9. Nel menu Actions (Operazioni) posto in alto a destra, selezionare Deploy (Distribuisci).
10. Per avviare la distribuzione, scegliere Automatic detection (Rilevamento automatico).

    Se la distribuzione non riesce, scegliere di nuovo Distribuisci. Se la distribuzione continua a non riuscire, è possibile consultare Risoluzione dei problemi di distribuzione di AWS IoT Greengrass.

Aggiungere il gateway SiteWise Edge a AWS IoT SiteWise

In questa procedura, aggiungete il gruppo Greengrass del gateway SiteWise Edge a. AWS IoT SiteWise Dopo aver registrato il gateway SiteWise Edge con AWS IoT SiteWise, il servizio può distribuire le configurazioni delle origini dati sul gateway Edge. SiteWise

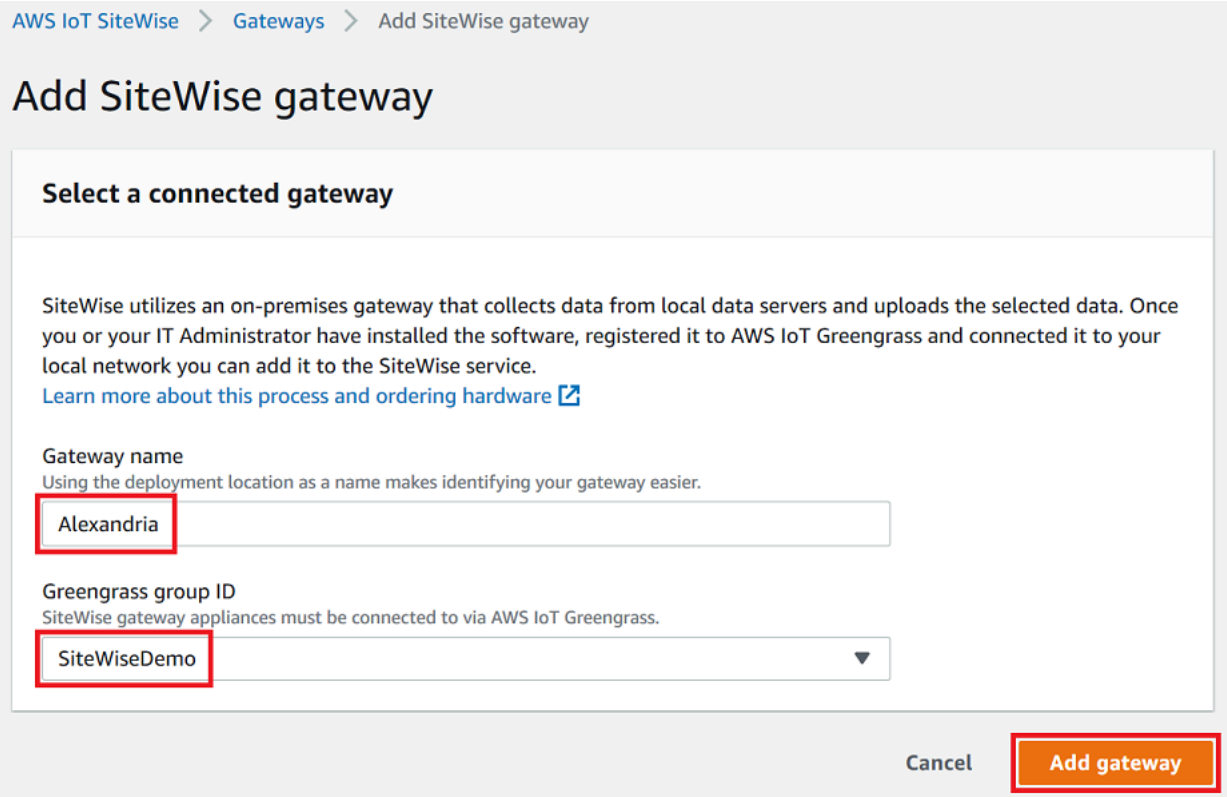
Per aggiungere il gateway SiteWise Edge a AWS IoT SiteWise

1. Passare alla console AWS IoT SiteWise.
2. Selezionare Add Gateway (Aggiungi gateway).
3. Nella pagina Aggiungi SiteWise gateway, procedi come segue:

a. Immettete un nome per il gateway SiteWise Edge. Valuta la possibilità di includere la posizione del gateway SiteWise Edge nel nome in modo da poterlo identificare facilmente.

b. Per l'ID del gruppo Greengrass, scegli il gruppo Greengrass che hai creato in precedenza.

Example



c. (Facoltativo) Per le funzionalità Edge, scegli il pacchetto di elaborazione dati. Ciò consente la comunicazione tra il gateway SiteWise Edge e qualsiasi modello di asset e asset configurato per l'edge. Per ulteriori informazioni, consulta the section called “Abilitare l'elaborazione dei dati edge”.

> **Important**
>
> Se aggiungi il pacchetto di elaborazione dati al tuo gateway SiteWise Edge, devi configurare e distribuire il connettore SiteWise Edge sul tuo AWS IoT Greengrass gruppo. Segui i passaggi successivi.

d. Selezionare Add Gateway (Aggiungi gateway).

4. Se aggiungi il pacchetto di elaborazione dati al tuo gateway SiteWise Edge, configura e implementa il connettore AWS IoT SiteWise Data Processor nel tuo AWS IoT Greengrass

gruppo. Segui i passaggi indicati the section called “Configurazione del connettore AWS IoT SiteWise” per configurare il connettore AWS IoT SiteWise Data Processor:

a. Per Seleziona un connettore nella AWS IoT Greengrass console, scegli Processore AWS IoT SiteWise dati.
b. Per Percorso di archiviazione locale, inserisci il percorso del gateway SiteWise Edge.
c. Scegli Aggiungi.
d. Nell'angolo in alto a destra, nel menu Azioni, scegli Distribuisci, quindi scegli Rilevamento automatico per avviare la distribuzione.

Dopo l'implementazione del gateway SiteWise Edge, puoi aggiungere una fonte per ogni apparecchiatura industriale da cui desideri che il gateway SiteWise Edge acquisisca i dati. Per ulteriori informazioni, consulta Configurazione delle origini dati.

Puoi visualizzare i CloudWatch parametri di Amazon per verificare che il tuo gateway SiteWise Edge si connetta a AWS IoT SiteWise. Per ulteriori informazioni, consulta AWS IoT Greengrass Version 1 metriche del gateway.

Configurazione delle fonti di dati sui AWS IoT Greengrass V1 SiteWise gateway Edge

Dopo aver configurato un gateway AWS IoT SiteWise Edge, puoi configurare le fonti di dati in modo che il gateway SiteWise Edge possa importare dati dalle apparecchiature industriali locali verso. AWS IoT SiteWise Ogni fonte rappresenta un server locale, ad esempio un server OPC-UA, a cui il gateway SiteWise Edge collega e recupera i flussi di dati industriali. Per ulteriori informazioni sulla configurazione di un gateway SiteWise Edge, vedere. Configurazione di un gateway AWS IoT Greengrass V1 SiteWise Edge

> **Note**
>
> AWS IoT SiteWise riavvia il gateway SiteWise Edge ogni volta che aggiungi o modifichi una fonte. Il gateway SiteWise Edge non inserirà dati durante il riavvio. Il tempo necessario per riavviare il gateway SiteWise Edge dipende dal numero di tag presenti nelle sorgenti del gateway SiteWise Edge. Il tempo di riavvio può variare da pochi secondi (per un gateway SiteWise Edge con pochi tag) a diversi minuti (per un gateway SiteWise Edge con molti tag).

Dopo aver creato le fonti, puoi associare i flussi di dati alle proprietà delle risorse. Per ulteriori informazioni su come creare e utilizzare le risorse, consulta Modellazione degli asset industriali eMappatura dei flussi di dati industriali alle proprietà degli asset.

Puoi visualizzare le CloudWatch metriche per verificare che una fonte di dati sia connessa AWS IoT SiteWise. Per ulteriori informazioni, consulta AWS IoT Greengrass Version 1 metriche del gateway.

Attualmente, AWS IoT SiteWise supporta i seguenti protocolli di origine dati:

- OPC-UA — Un protocollo di comunicazione machine-to-machine (M2M) per l'automazione industriale.
- Modbus TCP: protocollo di comunicazione dati utilizzato per interfacciarsi con controllori logici programmabili (PLC).
- EtherNet/IP (EIP): un protocollo di rete industriale che adatta il Common Industrial Protocol (CIP) allo standard Ethernet.

> **Note**
>
> SiteWise I gateway edge in esecuzione AWS IoT Greengrass V2 attualmente non supportano le sorgenti IP Modbus TCP ed Ethernet.

Argomenti

- Configura una sorgente Modbus TCP
- Configurare una sorgente EtherNet/IP (EIP)
- Configurazione dell'autenticazione dell'origine
- Aggiornamento di un connettore

Configura una sorgente Modbus TCP

È possibile utilizzare la AWS IoT SiteWise console o una funzionalità di gateway AWS IoT SiteWise Edge per definire e aggiungere una sorgente Modbus TCP al gateway Edge. SiteWise Questa fonte rappresenta un server Modbus TCP locale.

> **Note**
>
> - SiteWise I gateway Edge in esecuzione AWS IoT Greengrass V2 attualmente non supportano le sorgenti Modbus TCP.
> - È necessario installare il AWS IoT SiteWise connettore per utilizzare una sorgente Modbus TCP.

È possibile utilizzare la sorgente Modbus TCP per convertire il tipo di dati dalla fonte in un tipo di dati diverso quando vengono ricevuti sul gateway Edge. SiteWise Il tipo di dati di origine determina i tipi di dati che è possibile scegliere per i dati di destinazione. Puoi anche scegliere di scambiare i byte utilizzando la sorgente Modbus TCP. La tabella seguente fornisce ulteriori informazioni sui tipi di dati di origine, sui tipi di dati di destinazione e sulle modalità di scambio compatibili.

Per ulteriori informazioni sulle modalità di scambio, vedere l'articolo How Real (Floating Point) e 32-bit Data is Encoded in Modbus RTU Messages sulla codifica dei messaggi Modbus.

Tipo di dati origine	Tipi di dati di destinazione compatibili	Modalità di swap compatibili	Versioni di connettori compatibili
ASCII	Stringa	NoSwap	2
UTF8	Stringa	NoSwap	2
ISO 8859	Stringa	Nessuno scambio	2
Int16	Numero intero, doppio, stringa	NoSwap	1 e 2
Int32	Numero intero, doppio, stringa	NoSwap, ByteSwap, byteWordSwap WordSwap	1 e 2
Float	Doppio, corda	NoSwap, ByteSwap byteWordSwap, WordSwap	1 e 2
Booleano	Booleano	No Swap	1 e 2

Tipo di dati origine	Tipi di dati di destinazione compatibili	Modalità di swap compatibili	Versioni di connettori compatibili
Hex-dump	Stringa	Nessuno swap	1 e 2

Argomenti

Configurare una sorgente Modbus TCP (console)

Per configurare una sorgente Modbus TCP

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione a sinistra, selezionare Gateways (Gateway).
3. Sul gateway SiteWise Edge per cui desideri creare una fonte, scegli Gestisci, quindi scegli Visualizza dettagli.
4. Selezionare New source (Nuova origine) in alto a destra.
5. Per le opzioni di protocollo, scegli Modbus TCP.
6. Per la configurazione della sorgente Modbus TCP, inserite un nome per la sorgente.
7. Per l'indirizzo IP, inserisci l'indirizzo IP del server di origine dati.
8. (Facoltativo) Immettete l'ID di porta e di unità per il server di origine.
9. (Facoltativo) Per la durata minima tra le richieste, inserite l'intervallo di tempo tra le richieste successive inviate al server. Il gateway SiteWise Edge calcola automaticamente l'intervallo minimo consentito in base al dispositivo e al numero di registri di cui disponi.
10. Per i gruppi di proprietà, inserisci un nome.
11. Per Proprietà:
    a. Per Tag, inserisci un alias di proprietà per il tuo set di registri. Ad esempio, **`TT-001`**.
    b. Per Indirizzo di registro, inserisci l'indirizzo di registro che avvia il set di registri.
    c. Per Tipo di dati di origine, scegli il tipo di dati Modbus TCP da cui desideri convertire i dati. Il valore predefinito è Hex dump.

> **Note**
>
> Il tipo di dati di origine scelto determina la dimensione dei dati, il tipo di dati di destinazione e la modalità di scambio che è possibile scegliere. Per ulteriori informazioni, consulta the section called “Configura una sorgente Modbus TCP”.

d. In Dimensione dei dati, inserisci il numero di registri da leggere partendo dall'indirizzo del registro. Questo è determinato dal tipo di dati di origine scelto per questa fonte.

e. Per Tipo di dati di destinazione, scegli il AWS IoT SiteWise tipo di dati in cui desideri convertire i dati. L'impostazione predefinita è String. Il tipo di destinazione deve essere compatibile con il tipo di dati di origine scelto per questa origine. Per ulteriori informazioni, consulta the section called “Configura una sorgente Modbus TCP”.

f. Per la modalità Swap, scegli la modalità di scambio dei dati che desideri utilizzare per leggere i dati dal tuo set di registri. La modalità di scambio deve essere compatibile con il tipo di dati di origine scelto per questa fonte. Per ulteriori informazioni, consulta the section called “Configura una sorgente Modbus TCP”.

12. Per la velocità di scansione, aggiorna la frequenza con cui desideri che il gateway SiteWise Edge legga i tuoi registri. AWS IoT SiteWise calcola automaticamente la velocità di scansione minima consentita per il SiteWise gateway Edge.

13. (Facoltativo) Per Destinazione, scegliete dove inviare i dati di origine. Per impostazione predefinita, la fonte invia i dati a AWS IoT SiteWise. Puoi invece utilizzare uno AWS IoT Greengrass stream per esportare i dati verso una destinazione locale o nel AWS Cloud.

> **Note**
>
> Devi scegliere AWS IoT SiteWise come destinazione per i dati di origine se desideri elaborare i dati da questa fonte all'edge con AWS IoT SiteWise. Per ulteriori informazioni sull'elaborazione dei dati all'edge, consultathe section called “Abilitare l'elaborazione dei dati edge”.

Per inviare i dati a un'altra destinazione:

a. Per le opzioni di destinazione, scegli Altre destinazioni.

b. Per il nome dello stream Greengrass, inserisci il nome esatto del tuo AWS IoT Greengrass stream.

> **Note**
>
> Puoi usare uno stream che hai già creato oppure puoi creare un nuovo AWS IoT Greengrass stream per esportare i tuoi dati. Se desideri utilizzare uno stream esistente, devi inserire il nome esatto dello stream o verrà creato un nuovo stream. Per ulteriori informazioni sull'utilizzo degli AWS IoT Greengrass stream, consulta Gestire i flussi di dati nella guida per AWS IoT Greengrass sviluppatori.

14. Scegliere Add source (Aggiungi origine).

    AWS IoT SiteWise implementa la configurazione principale del gateway SiteWise Edge. AWS IoT Greengrass Non è necessario avviare manualmente una distribuzione.

Configurazione di una sorgente Modbus TCP (CLI)

È possibile definire sorgenti dati Modbus TCP in una funzionalità di gateway Edge. SiteWise È necessario definire tutte le sorgenti Modbus TCP in un'unica configurazione di funzionalità.

Per ulteriori informazioni sulla definizione delle fonti con AWS CLI, vedere. the section called “Configurazione delle origini dati (AWS CLI)”

> **Note**
>
> È necessario installare il AWS IoT SiteWise connettore per utilizzare una sorgente Modbus TCP.

Questa funzionalità dispone delle versioni seguenti.

Versione	Spazio dei nomi
1	`iotsitewise:modbuscollector:1`

Parametri di configurazione della funzionalità Modbus TCP

Quando si definiscono sorgenti Modbus TCP in una configurazione di funzionalità, è necessario specificare le seguenti informazioni nel documento JSON: `capabilityConfiguration`

fonti

Un elenco di strutture di definizione dei sorgenti Modbus-TCP, ognuna delle quali contiene le seguenti informazioni:

name

Un nome descrittivo univoco per l'origine.

measurementDataStreamPrefisso

(Facoltativo) Una stringa da aggiungere a tutti i flussi di dati dall'origine. Il gateway SiteWise Edge aggiunge questo prefisso a tutti i flussi di dati provenienti da questa fonte. Utilizzare un prefisso del flusso di dati per distinguere tra flussi di dati con lo stesso nome da origini diverse. Ogni flusso di dati deve avere un nome univoco all'interno del tuo account.

destinazione

Una struttura di destinazione che contiene le seguenti informazioni:

tipo

Il tipo di destinazione.

StreamName

Il nome dello AWS IoT Greengrass stream.

streamBufferSize

La dimensione del buffer dello stream.

endpoint

Una struttura endpoint contenente le seguenti informazioni:

IP Address

L'indirizzo IP della sorgente Modbus TCP.

port

(Facoltativo) La porta della sorgente Modbus TCP.

UnitID

(Facoltativo) L'unitID. Il valore predefinito è 1.

minimumInterRequestDurata

La durata minima tra ogni richiesta in millisecondi.

Gruppi di proprietà

L'elenco dei gruppi di proprietà che definiscono la definizione dei tag richiesta dal protocollo.

name

Il nome del gruppo di proprietà. Dovrebbe essere un identificatore univoco.

tagPathDefinitions

La posizione della misurazione all'interno della sorgente. Ad esempio, l'ordine dei byte e delle parole, l'indirizzo e il tipo di trasformazione. La struttura di ciascuno `MeasurementPathDefinition` è definita dal connettore.

Modalità di scansione

Definisce il comportamento della modalità di scansione e i parametri configurabili per la sorgente.

Configurare una sorgente EtherNet/IP (EIP)

È possibile utilizzare la AWS IoT SiteWise console o una funzionalità di gateway SiteWise Edge per definire e aggiungere una sorgente IP Ethernet al gateway SiteWise Edge. Questa fonte rappresenta un server IP Ethernet locale.

> **Note**
>
> - SiteWise I gateway Edge in esecuzione AWS IoT Greengrass V2 attualmente non supportano le sorgenti IP Ethernet.
> - È necessario installare il AWS IoT SiteWise connettore per utilizzare una sorgente IP Ethernet.

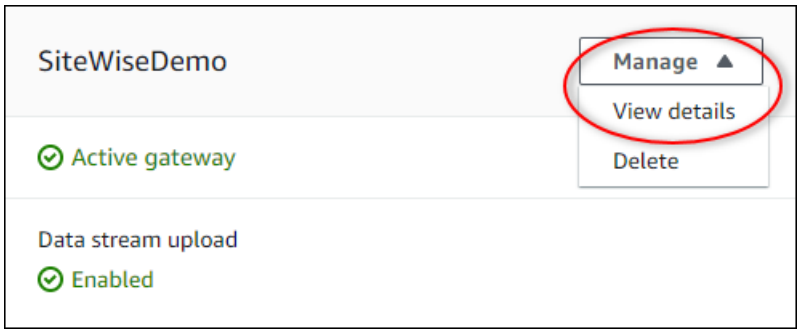
Argomenti

- Configurare una sorgente EtherNet/IP (console)
- Configurazione di una sorgente EtherNet/IP (CLI)

Configurare una sorgente EtherNet/IP (console)

Per configurare una sorgente EtherNet/IP

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione a sinistra, selezionare Gateways (Gateway).
3. Sul gateway SiteWise Edge per cui desideri creare una fonte, scegli Gestisci, quindi scegli Visualizza dettagli.



4. Selezionare New source (Nuova origine) in alto a destra.
5. Per le opzioni di protocollo, scegli EtherNet/IP (EIP).
6. Per la configurazione EtherNet dell'origine /IP, inserisci un nome per l'origine.
7. Per l'indirizzo IP, inserisci l'indirizzo IP del server di origine dati.
8. (Facoltativo) Immettete la porta per il server di origine.
9. Per Durata minima tra richieste, inserite l'intervallo di tempo tra le richieste successive inviate al server. Il gateway SiteWise Edge calcola automaticamente l'intervallo minimo consentito in base al dispositivo e al numero di registri di cui disponi.
10. Per i gruppi di proprietà, inserisci un nome.
11. Per Proprietà:
    a. Per Tag, inserisci l'alias della proprietà per il tuo set di registri. Ad esempio, **`boiler.inlet.temperature.value`**.
    b. Per Tipo di dati di destinazione, scegli il tipo di AWS IoT SiteWise dati in cui desideri convertire i dati. L'impostazione predefinita è String.
12. Per Frequenza di scansione, aggiorna la frequenza con cui desideri che il gateway SiteWise Edge legga i tuoi registri. AWS IoT SiteWise calcola automaticamente la velocità di scansione minima consentita per il SiteWise gateway Edge.

13. (Facoltativo) Per Destinazione, scegliete dove inviare i dati di origine. Per impostazione predefinita, la fonte invia i dati a AWS IoT SiteWise. Puoi invece utilizzare uno AWS IoT Greengrass stream per esportare i dati verso una destinazione locale o nel AWS Cloud.

    > **Note**
    >
    > Devi scegliere AWS IoT SiteWise come destinazione per i dati di origine se desideri elaborare i dati da questa fonte all'edge con AWS IoT SiteWise. Per ulteriori informazioni sull'elaborazione dei dati all'edge, consultathe section called “Abilitare l'elaborazione dei dati edge”.

    Per inviare i dati a un'altra destinazione:

    a. Per le opzioni di destinazione, scegli Altre destinazioni.

    b. Per il nome dello stream Greengrass, inserisci il nome esatto del tuo AWS IoT Greengrass stream.

        > **Note**
        >
        > Puoi usare uno stream che hai già creato oppure puoi creare un nuovo AWS IoT Greengrass stream per esportare i tuoi dati. Se desideri utilizzare uno stream esistente, devi inserire il nome esatto dello stream o verrà creato un nuovo stream. Per ulteriori informazioni sull'utilizzo degli AWS IoT Greengrass stream, consulta Gestire i flussi di dati nella guida per AWS IoT Greengrass sviluppatori.

14. Scegliere Add source (Aggiungi origine).

    AWS IoT SiteWise implementa la configurazione principale del gateway SiteWise Edge. AWS IoT Greengrass Non è necessario avviare manualmente una distribuzione.

Configurazione di una sorgente EtherNet/IP (CLI)

È possibile definire le fonti di dati EIP con una SiteWise funzionalità di gateway Edge. È necessario definire tutte le fonti EIP in un'unica configurazione di funzionalità.

Per ulteriori informazioni sulla definizione delle fonti con AWS CLI, vederethe section called “Configurazione delle origini dati (AWS CLI)”.

> **Note**
>
> È necessario installare il AWS IoT SiteWise connettore per utilizzare una sorgente IP Ethernet.

Questa funzionalità dispone delle versioni seguenti.

Versione	Spazio dei nomi
1	`iotsitewise:eipcollector:1`

Parametri di configurazione della funzionalità EIP

Quando si definiscono le sorgenti EIP in una configurazione di funzionalità, è necessario specificare le seguenti informazioni nel documento `capabilityConfiguration` JSON:

fonti

Un elenco di strutture di definizione dei sorgenti EIP, ciascuna delle quali contiene le seguenti informazioni:

name

Un nome descrittivo univoco per l'origine. Può contenere fino a 256 caratteri.

destinationPathPrefix

(Facoltativo) Una stringa da aggiungere a tutti i flussi di dati dall'origine. Il gateway SiteWise Edge aggiunge questo prefisso a tutti i flussi di dati provenienti da questa fonte. Utilizzare un prefisso del flusso di dati per distinguere tra flussi di dati con lo stesso nome da origini diverse. Ogni flusso di dati deve avere un nome univoco all'interno del tuo account.

destinazione

Una struttura di destinazione che contiene le seguenti informazioni:

tipo

Il tipo di destinazione.

StreamName

Il nome dello AWS IoT Greengrass stream.

streamBufferSize

La dimensione del buffer dello stream.

endpoint

Una struttura endpoint contenente le seguenti informazioni:

IP Address

L'indirizzo IP dell'origine EIP.

port

(Facoltativo) La porta dell'origine EIP. I valori accettati sono numeri compresi tra 1 e 65535.

minimumInterRequestDurata

(Facoltativo) La durata minima tra ogni richiesta, espressa in millisecondi.

Gruppi di proprietà

L'elenco dei gruppi di proprietà che definiscono la definizione dei tag richiesta dal protocollo. Ogni fonte può avere un gruppo di proprietà.

name

Il nome del gruppo di proprietà. Deve essere un identificatore univoco con una lunghezza massima di 256 caratteri.

tagPathDefinitions

L'elenco delle strutture che specificano i dati da raccogliere dal dispositivo EtherNet/IP e come trasformarli per l'output.

tipo

Il tipo di `tagPathDefinition`. Ad esempio, `EIPTagPath`.

path

Il percorso del. `tagPathDefinition` Ogni tag in un percorso può avere una lunghezza massima di 40 caratteri e può iniziare con una lettera o un carattere di sottolineatura. I tag non possono contenere caratteri di sottolineatura consecutivi o finali. Il percorso è preceduto da un qualsiasi valore di. destinationPathPrefix

dstDataType

Il tipo di dati per l'output dei dati del tag. I valori accettati sono `integerdouble`,`string`, `eboolean`.

ScanMode

Definisce il comportamento della modalità di scansione e i parametri configurabili per la sorgente.

tipo

Il tipo di comportamento della modalità di scansione. I valori accettati sonoPOLL.

tasso

La velocità in millisecondi con cui il connettore deve leggere i tag dalla sorgente EtherNet/IP.

Configurazione dell'autenticazione dell'origine

Se i server OPC-UA richiedono credenziali di autenticazione per connettersi, puoi definire un nome utente e una password in un segreto per ogni origine in AWS Secrets Manager. Quindi, aggiungi il segreto al tuo gruppo Greengrass e al SiteWise connettore IoT per renderlo disponibile al tuo gateway SiteWise Edge. Per ulteriori informazioni, consulta Deploy secret to AWS IoT Greengrass core nella AWS IoT Greengrass Version 1 Developer Guide.

Dopo che un segreto è disponibile per il gateway SiteWise Edge, puoi sceglierlo quando configuri una fonte. Quindi, il gateway SiteWise Edge utilizza le credenziali di autenticazione del segreto quando si connette alla fonte. Per ulteriori informazioni, consulta Configurazione delle origini dati.

Argomenti

- Creazione di segreti di autenticazione dell'origine
- Aggiungere segreti a un gruppo Greengrass
- Aggiungere segreti a un SiteWise connettore IoT

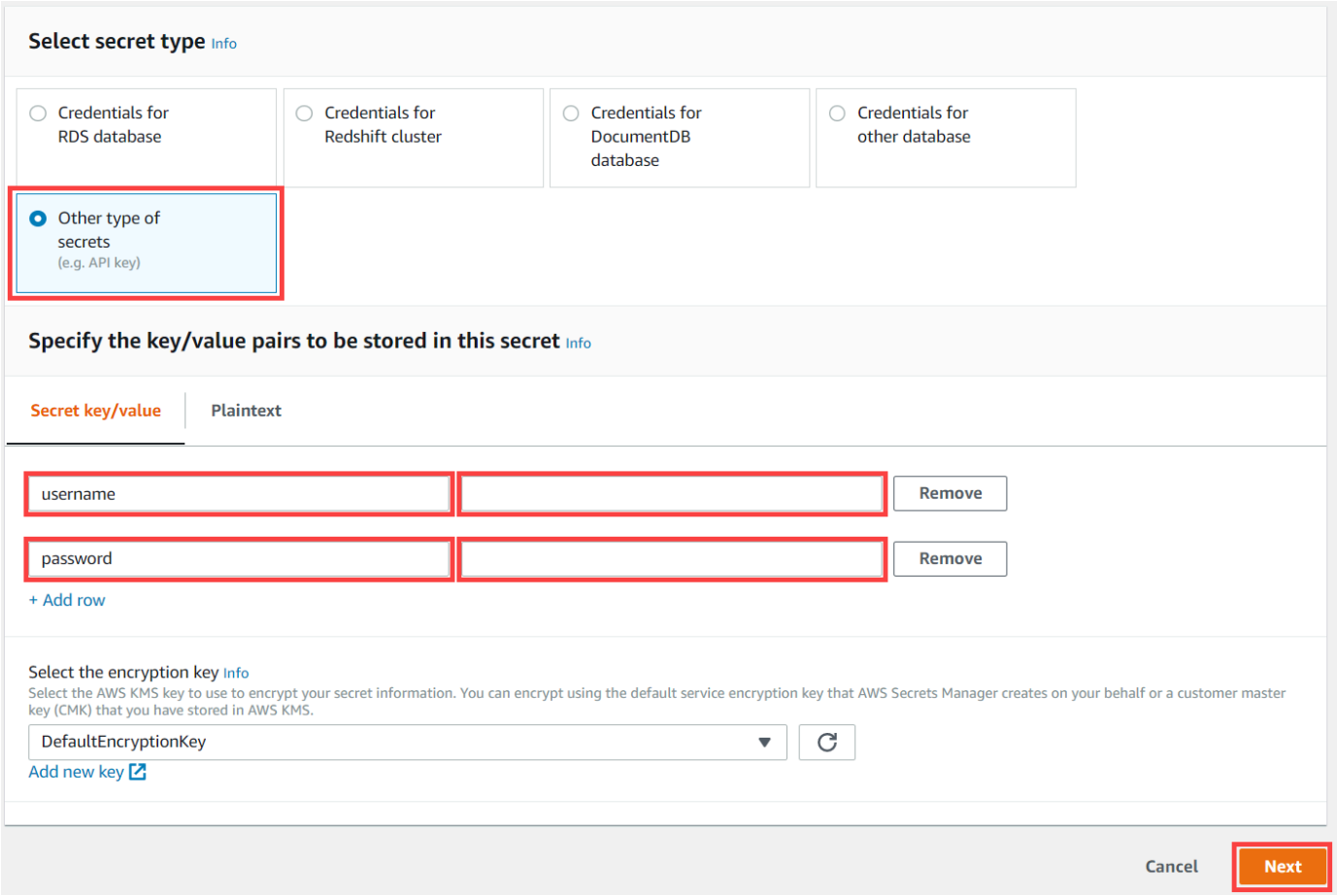
Creazione di segreti di autenticazione dell'origine

In questa procedura, crei un segreto di autenticazione per la tua fonte in Secrets Manager. Nel segreto, definisci coppie chiave-valore **`username`** e **`password`** che contengono dettagli di autenticazione per l'origine.

Per creare un segreto di autenticazione dell'origine

1. Vai alla console Secrets Manager.

2. Scegli Archivia un nuovo segreto.
3. In Select secret type (Seleziona tipo di segreto), scegliere Other type of secrets (Altro tipo di segreti).
4. Immettere le coppie chiave-valore **`username`** e **`password`** riferite ai propri valori di autenticazione del server OPC-UA, quindi selezionare Next (Avanti).



5. Compilare il campo Secret name (Nome segreto) con un nome che inizia con `greengrass-`, ad esempio **`greengrass-factory1-auth`**.

> **Important**
>
> Per accedere ai segreti, è necessario utilizzare il prefisso `greengrass-` per il ruolo di servizio predefinito AWS IoT Greengrass . Se desideri assegnare un nome ai tuoi segreti senza questo prefisso, devi concedere autorizzazioni AWS IoT Greengrass personalizzate per accedere ai tuoi segreti. Per ulteriori informazioni, consulta Consenti di AWS IoT Greengrass ottenere valori segreti nella Guida per gli AWS IoT Greengrass Version 1 sviluppatori.

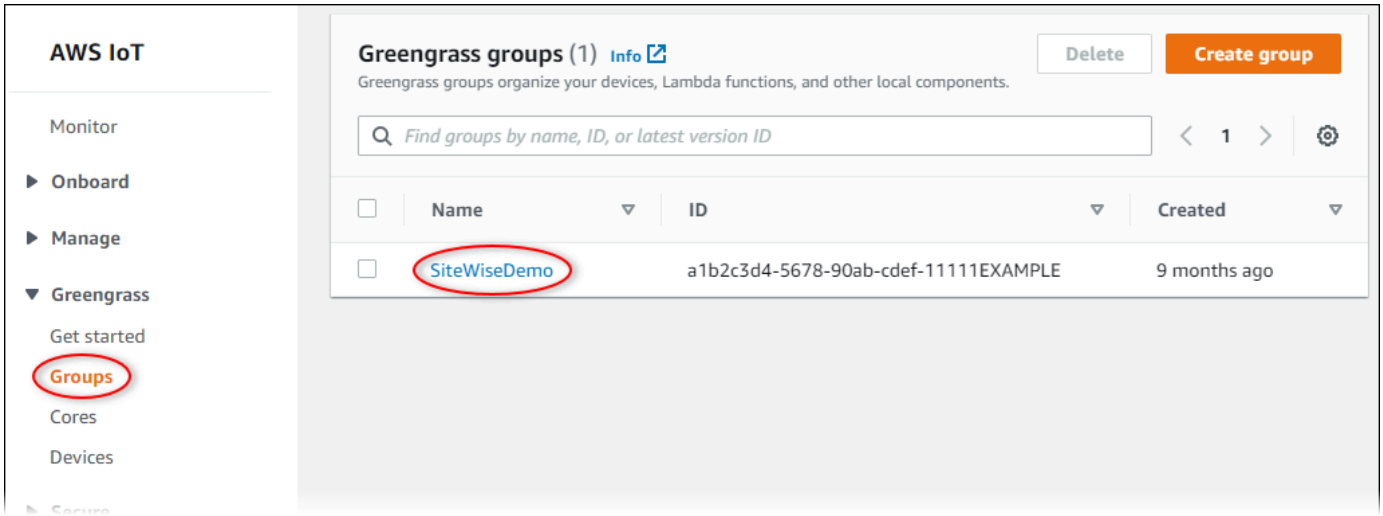
6. Immettere una Description (Descrizione) e scegliere Next (Avanti).
7. (Facoltativo) Nella pagina Configure automatic rotation (Configura rotazione automatica), configurare la rotazione automatica per i propri segreti. Se configuri la rotazione automatica, devi ridistribuire il tuo gruppo Greengrass ogni volta che ruota un segreto.
8. Nella pagina Configure automatic rotation (Configura rotazione automatica), selezionare Next (Avanti).
9. Controllare il nuovo segreto e selezionare Store (Archivia).

Aggiungere segreti a un gruppo Greengrass

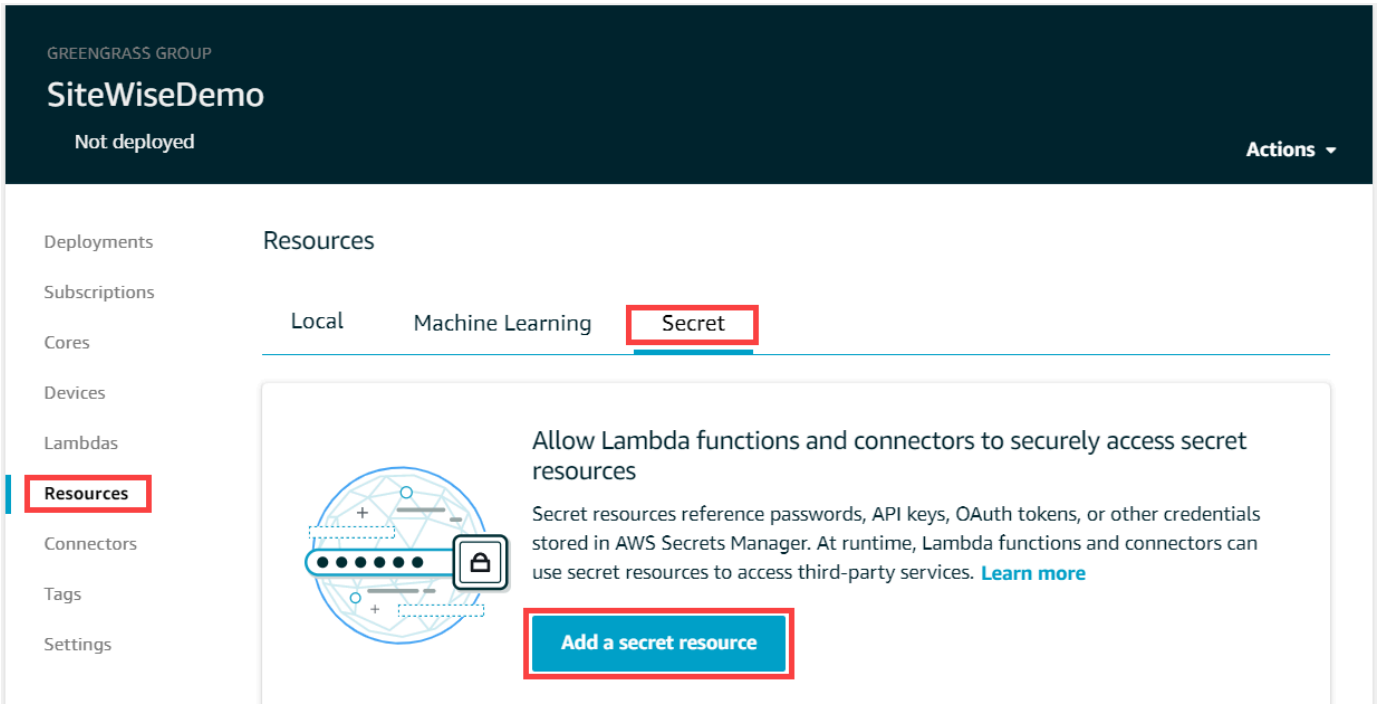
In questa procedura, aggiungi i tuoi segreti di autenticazione di origine al tuo AWS IoT Greengrass gruppo per renderli disponibili al tuo SiteWise connettore IoT.

Per aggiungere un segreto al tuo gruppo Greengrass

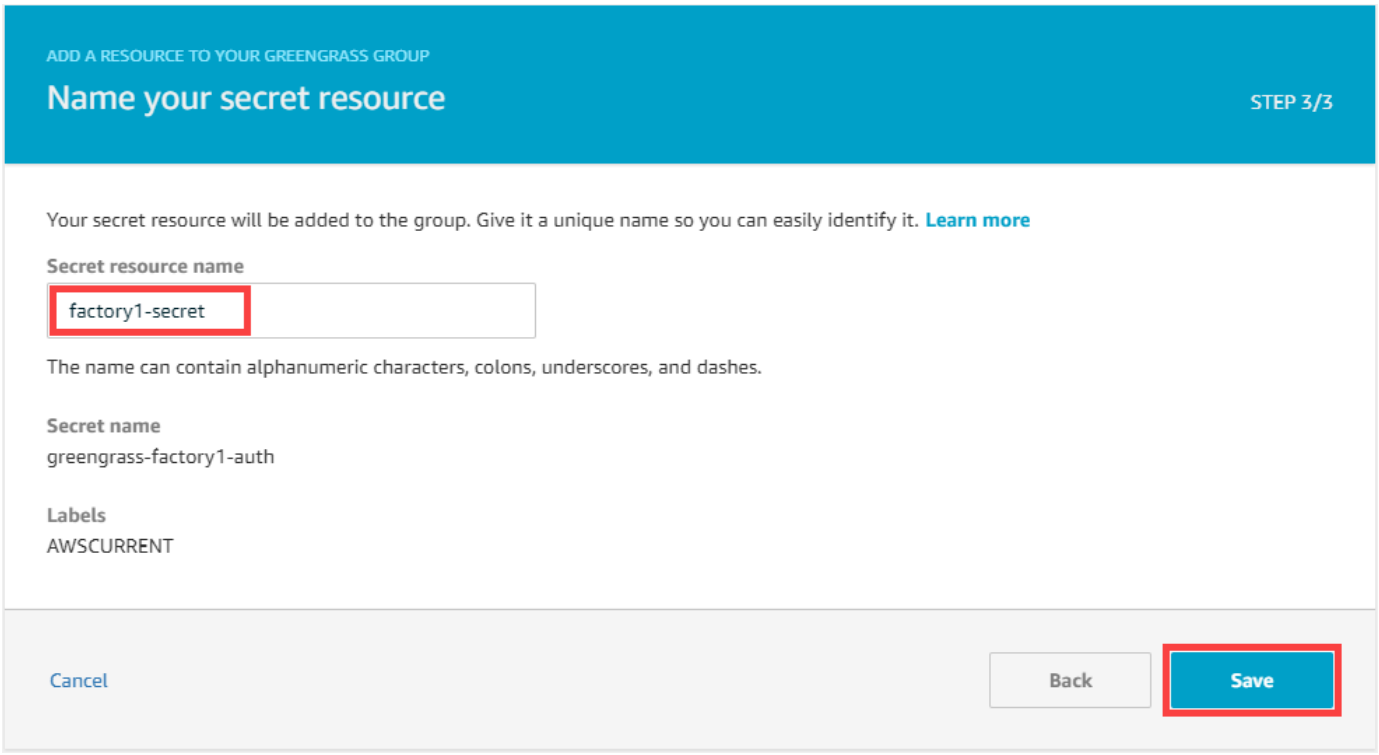
1. Passare alla console AWS IoT Greengrass.
2. Nel pannello di navigazione, in Greengrass, scegli Gruppi, quindi scegli il tuo gruppo.



3. Nella pagina di navigazione, scegli Risorse.
4. Nella pagina Resources (Risorse), scegliere la scheda Secret (Segreto), quindi selezionare Add a secret resource (Aggiungi una risorsa segreta).



5. Fare clic su Select (Seleziona) e scegliere il proprio segreto dall'elenco.
6. Seleziona Successivo.
7. In Secret resource name (Nome risorsa segreta), inserire il nome previsto per la risorsa segreta, poi selezionare Save (Salva).

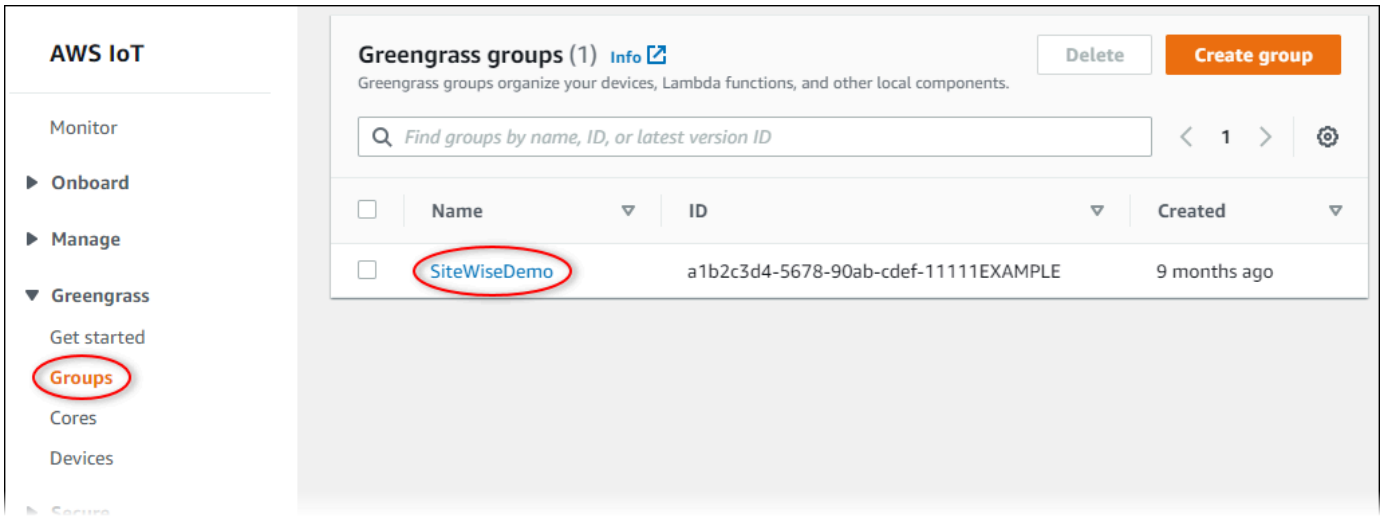


Aggiungere segreti a un SiteWise connettore IoT

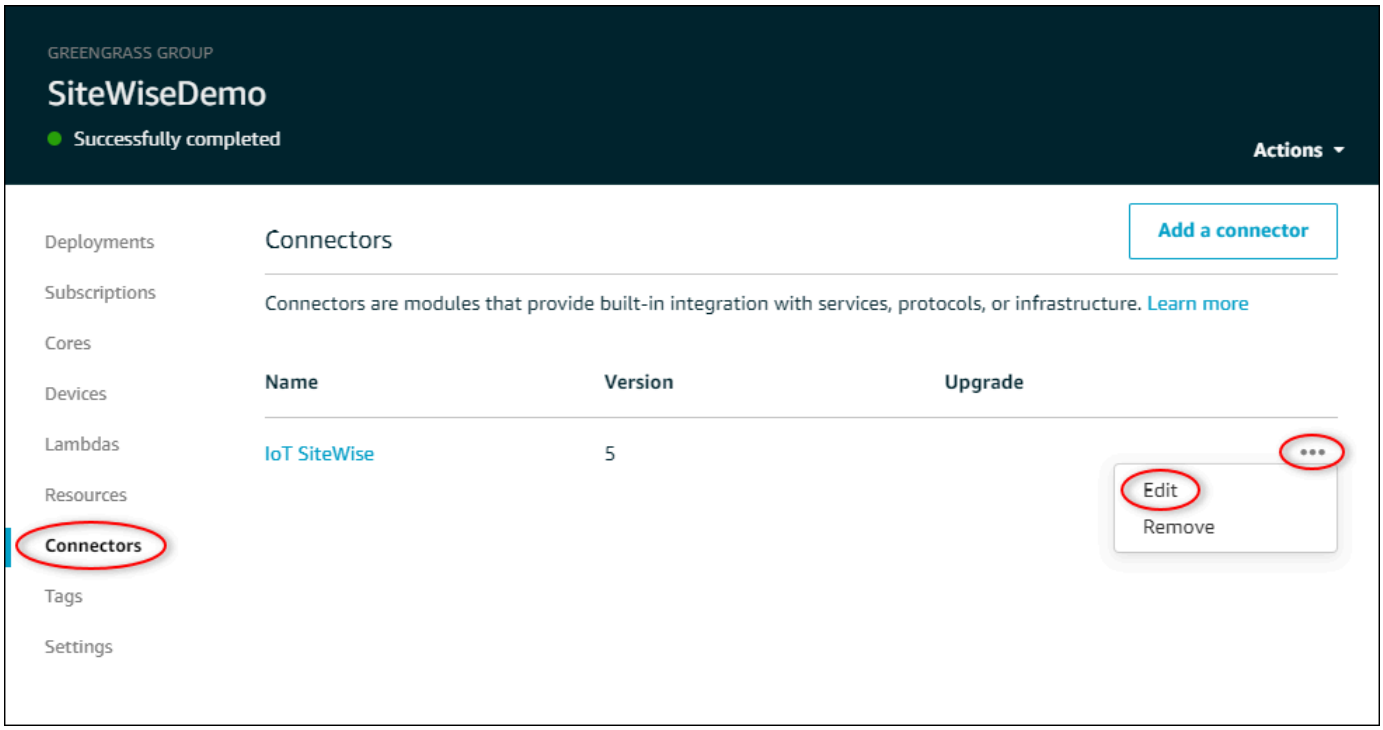
In questa procedura, aggiungi i tuoi segreti di autenticazione di origine al SiteWise connettore IoT per renderli disponibili al AWS IoT SiteWise gateway SiteWise Edge.

Per aggiungere un segreto al tuo SiteWise connettore IoT

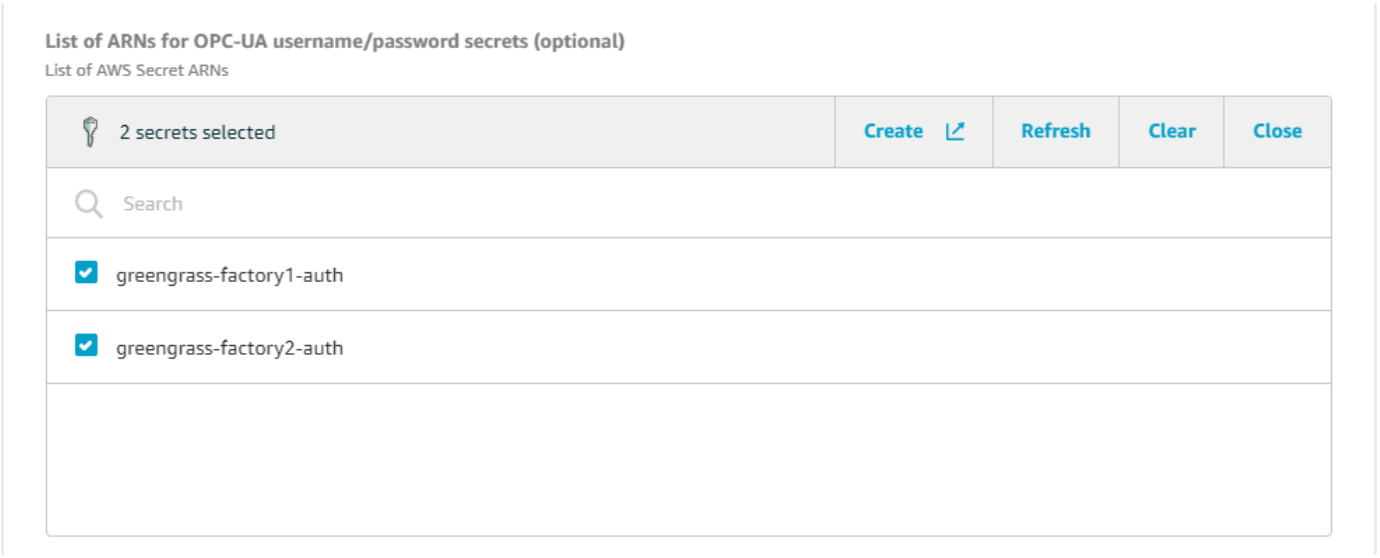
1. Passare alla console AWS IoT Greengrass.
2. Nel pannello di navigazione, in Greengrass, scegli Gruppi, quindi scegli il tuo gruppo.



3. Nella pagina di navigazione, scegli Connettori.
4. Scegli l'icona con i puntini di sospensione per il SiteWise connettore IoT per aprire il menu delle opzioni, quindi scegli Modifica.



5. In Elenco di ARN per i segreti relativi a nome utente/password OPC-UA, scegli Seleziona, quindi seleziona ogni segreto da aggiungere a questo gateway Edge. SiteWise Se occorre creare segreti, consulta Creazione di segreti di autenticazione dell'origine.



Se il segreto non viene visualizzato, scegliere Refresh (Aggiorna). Se il tuo segreto continua a non apparire, verifica di averlo aggiunto al tuo gruppo Greengrass.

6. Selezionare Salva.
7. Nel menu Actions (Operazioni) posto in alto a destra, selezionare Deploy (Distribuisci).
8. Per avviare la distribuzione, scegliere Automatic detection (Rilevamento automatico).

   Se la distribuzione non riesce, scegliere di nuovo Distribuisci. Se la distribuzione continua a non riuscire, è possibile consultare Risoluzione dei problemi di distribuzione di AWS IoT Greengrass.

   Dopo che il gruppo è stato distribuito, è possibile configurare un'origine che utilizza il nuovo segreto. Per ulteriori informazioni, consulta Configurazione delle origini dati.

Aggiornamento di un connettore

Important

La versione 6 del SiteWise connettore IoT introduce nuovi requisiti: software AWS IoT Greengrass Core v1.10.0 e stream manager. Prima di aggiornare il connettore, verifica che il gateway SiteWise Edge soddisfi questi requisiti, altrimenti non sarai in grado di implementare il gateway Edge. SiteWise

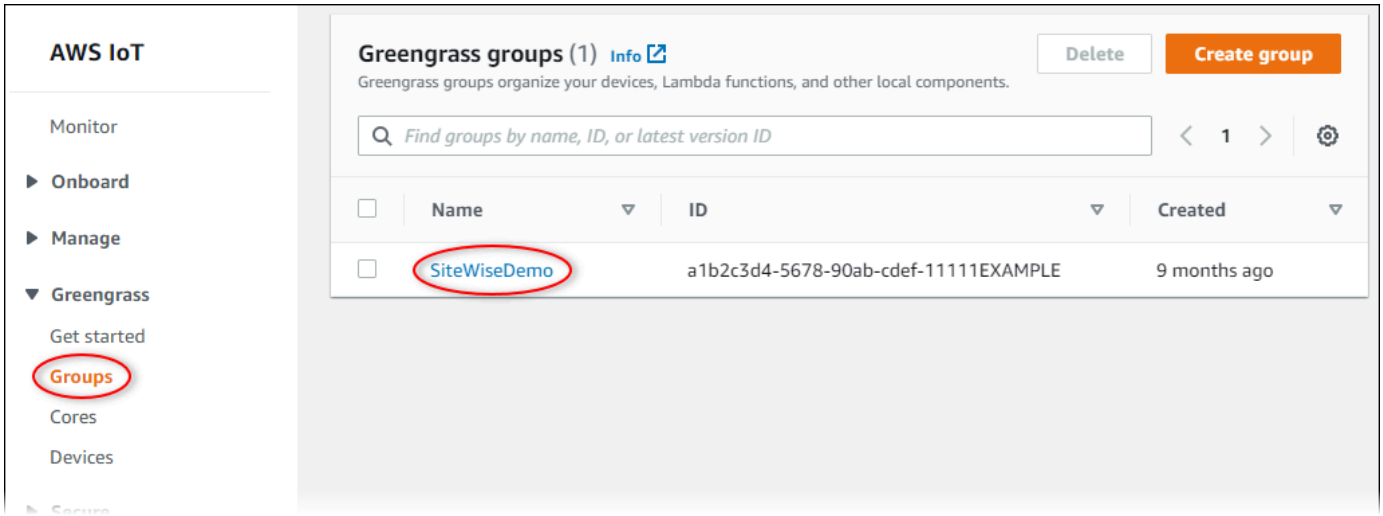
È possibile aggiornare facilmente il connettore del gateway SiteWise Edge dopo il rilascio di una nuova versione del SiteWise connettore IoT.

Note

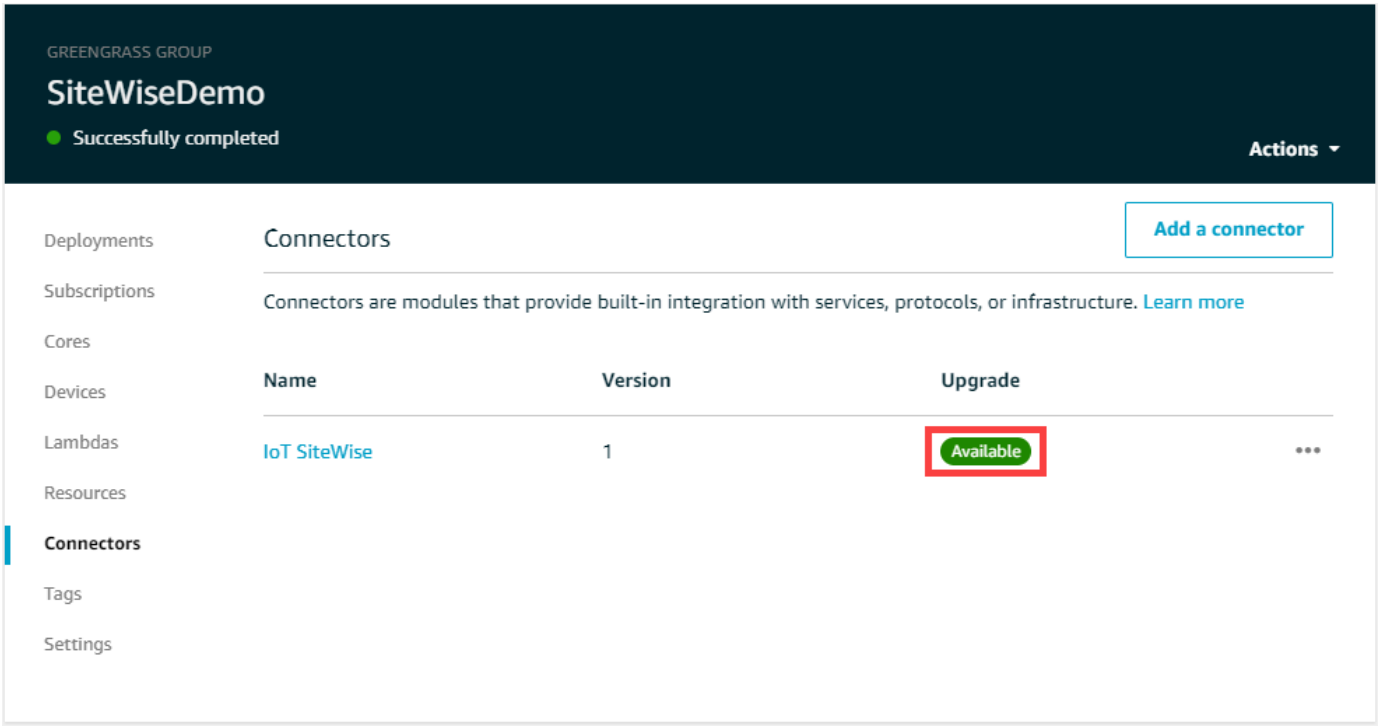
In questa procedura, si ridistribuisce il gruppo Greengrass e si riavvia il gateway Edge. SiteWise Il gateway SiteWise Edge non acquisirà dati durante il riavvio. Il tempo necessario per riavviare il gateway SiteWise Edge dipende dal numero di tag presenti nelle sorgenti del gateway SiteWise Edge. Il tempo di riavvio può variare da pochi secondi (per un gateway SiteWise Edge con pochi tag) a diversi minuti (per un gateway SiteWise Edge con molti tag).

Per aggiornare un SiteWise connettore IoT

1. Passare alla console AWS IoT Greengrass.
2. Nel pannello di navigazione, in Greengrass, scegli Gruppi, quindi scegli il gruppo creato durante la configurazione del gateway SiteWise Edge.



3. Nel pannello di navigazione, scegli Connettori.
4. Nella pagina Connettori, scegli Disponibile accanto al SiteWise connettore IoT.



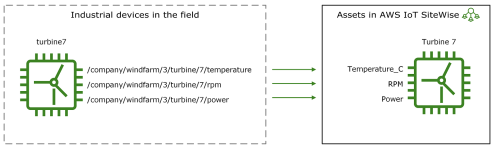
   Se non viene visualizzato l'elemento Available (Disponibile), significa che la versione del connettore è già la più recente.
5. Nella pagina Upgrade connector (Aggiorna connettore), immettere i parametri del connettore e scegliere Upgrade (Aggiorna).
6. Nel menu Actions (Operazioni) posto in alto a destra, selezionare Deploy (Distribuisci).
7. Per avviare la distribuzione, scegliere Automatic detection (Rilevamento automatico).

Se la distribuzione non riesce, scegliere di nuovo Distribuisci. Se la distribuzione continua a non riuscire, è possibile consultare Risoluzione dei problemi di distribuzione di AWS IoT Greengrass.

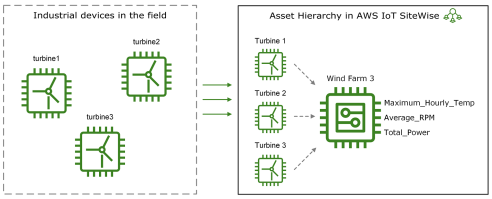
Modellazione degli asset industriali

È possibile creare rappresentazioni virtuali delle proprie operazioni industriali con AWS IoT SiteWise gli asset. Una risorsa rappresenta un dispositivo, un'apparecchiatura o un processo che carica uno o più flussi di dati su. Cloud AWS Ad esempio, un dispositivo di asset può essere una turbina eolica che invia le misurazioni delle serie temporali della temperatura dell'aria, della velocità di rotazione dell'elica e dell'uscita di potenza alle proprietà degli asset in AWS IoT SiteWise.

Ogni flusso di dati corrisponde a un alias di proprietà univoco. L'alias `/company/windfarm/3/turbine/7/temperature`, ad esempio, identifica in modo univoco il flusso di dati relativi alla temperatura proveniente dalla turbina #7 nel parco eolico #3. È possibile configurare le AWS IoT SiteWise risorse per trasformare i dati di misurazione in entrata utilizzando espressioni matematiche, ad esempio per convertire i dati di temperatura da gradi Celsius a gradi Fahrenheit.



Un asset può anche rappresentare un raggruppamento logico di dispositivi, ad esempio un intero parco eolico. È possibile associare gli asset ad altri asset per creare gerarchie di asset che rappresentano operazioni industriali complesse. Le risorse possono accedere ai dati all'interno delle risorse secondarie associate. In questo modo, è possibile utilizzare AWS IoT SiteWise le espressioni per calcolare metriche aggregate, come la potenza netta in uscita di un parco eolico.



È necessario creare ogni risorsa a partire da un modello di asset. I modelli di asset sono strutture dichiarative che standardizzano il formato degli asset. I modelli di asset applicano informazioni coerenti su più asset dello stesso tipo in modo da poter elaborare i dati in risorse che rappresentano gruppi di dispositivi. Nel diagramma precedente, si utilizza lo stesso modello di asset per tutte e tre le turbine, contraddistinte da un insieme di proprietà in comune.

È inoltre possibile creare modelli di componenti. Un modello di componente è un tipo speciale di modello di asset che è possibile includere nei modelli di asset o in altri modelli di componenti.

È possibile utilizzare i modelli di componenti per definire sottoassiemi riutilizzabili comuni, come sensori, motori e così via, da condividere tra più modelli di asset.

Dopo averne definito i modelli, è possibile creare gli asset industriali. Per creare un asset, bisogna innanzitutto selezionarne un modello `ACTIVE`. e successivamente inserire le informazioni del caso, quali gli attributi e alias del flusso di dati. Nel diagramma precedente, si creano tre asset turbina da un modello di asset e quindi si associano gli alias del flusso di dati come `/company/windfarm/3/turbine/7/temperature` per ogni turbina.

Potete anche aggiornare ed eliminare risorse, modelli di asset e modelli di componenti esistenti. Quando si aggiorna un modello, ogni asset su di esso basato assimila le modifiche apportate. Quando aggiornate un modello di componente, ciò si applica a ogni asset basato su ogni modello di asset che fa riferimento al modello di componente.

I vostri modelli di asset possono essere molto complessi, ad esempio quando si modella un'apparecchiatura complicata che ha molti sottocomponenti. Per contribuire a mantenere tali modelli di asset organizzati e gestibili, potete utilizzare modelli compositi personalizzati per raggruppare proprietà correlate o riutilizzare componenti condivisi. Per ulteriori informazioni, consulta Modelli compositi personalizzati (componenti).

Argomenti

Stati di asset e modelli

Quando create, aggiornate o eliminate una risorsa, un modello di asset o un modello di componente, la propagazione delle modifiche richiede tempo. AWS IoT SiteWise risolve queste operazioni in modo asincrono e aggiorna lo stato di ogni risorsa. Ogni asset, modello di asset e modello di componente ha un campo di stato che contiene lo stato della risorsa e qualsiasi messaggio di errore, se applicabile. Lo stato può avere uno dei seguenti valori:

- `ACTIVE`— La risorsa è attiva. Questo è l'unico stato in cui è possibile interrogare e interagire con risorse, modelli di asset e modelli di componenti.
- `CREATING`— La risorsa è in fase di creazione.
- `UPDATING`— La risorsa è in fase di aggiornamento.
- `DELETING`— La risorsa viene eliminata.
- `PROPAGATING`— (Solo modelli di asset e modelli di componenti) Le modifiche si propagano a tutte le risorse dipendenti (dal modello di asset agli asset o dal modello di componente ai modelli di asset).
- `FAILED`— La risorsa non è stata convalidata durante un'operazione di creazione o aggiornamento, probabilmente a causa di un riferimento circolare in un'espressione. È possibile eliminare le risorse presenti nello `FAILED` stato.

Alcune delle operazioni di creazione, aggiornamento ed eliminazione eseguono una risorsa, un modello di asset o un modello di componente in uno stato diverso da quello in cui `ACTIVE` l'operazione è risolta. AWS IoT SiteWise Per interrogare o interagire con una risorsa dopo aver eseguito una di queste operazioni, è necessario attendere che lo stato cambi a. `ACTIVE` In caso contrario, le tue richieste avranno esito negativo.

Argomenti

Controllo dello stato di un asset

Puoi utilizzare la AWS IoT SiteWise console o l'API per verificare lo stato di una risorsa.

Argomenti

Controllo dello stato di un asset (console)

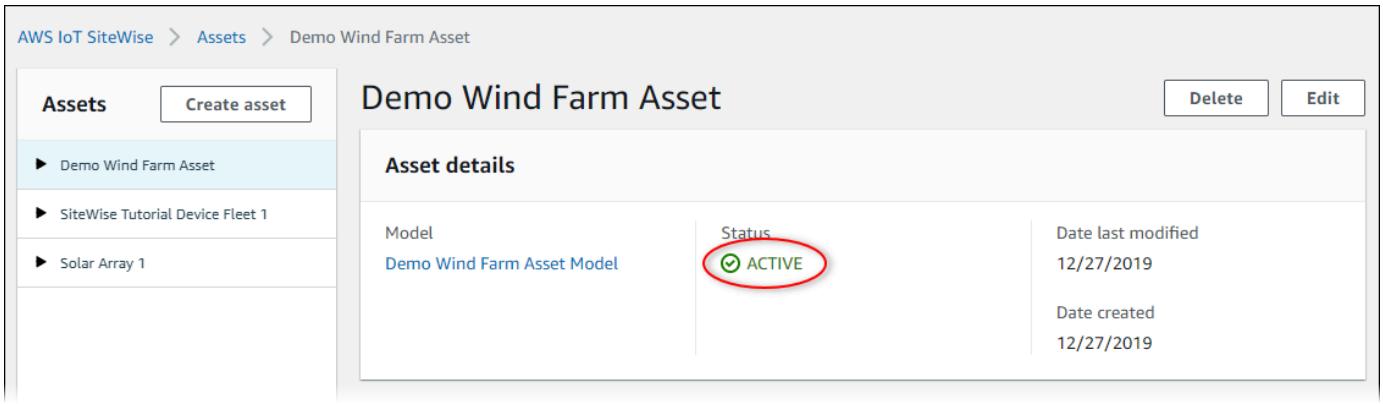
Per verificare lo stato di un asset nella console AWS IoT SiteWise , attieniti alla procedura descritta di seguito.

Per controllare lo stato di un asset (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Asset.
3. Scegli l'asset da controllare.

> **Tip**
>
> Puoi scegliere l'icona a forma di freccia per espandere una gerarchia di asset e trovare il tuo asset.

4. Trova Stato nel pannello Dettagli dell'asset.



Verifica dello stato di una risorsa (AWS CLI)

Puoi usare il AWS Command Line Interface (AWS CLI) per controllare lo stato di una risorsa.

Per verificare lo stato di una risorsa, utilizzate l'DescribeAssetoperazione con il `assetId` parametro.

Per controllare lo stato di una risorsa (AWS CLI)

- Immetti il seguente comando per descrivere l'asset. Sostituisci *asset-id* con l'ID della risorsa o l'ID esterno. L'ID esterno è un ID definito dall'utente. Per ulteriori informazioni, consulta Riferimento a oggetti con ID esterni nella Guida per l'utente di AWS IoT SiteWise .

```
aws iotsitewise describe-asset --asset-id asset-id
```

L'operazione restituisce una risposta contenente i dettagli dell'asset. La risposta contiene un `assetStatus` oggetto con la seguente struttura:

```
{
    ...
    "assetStatus": {
      "state": "String",
      "error": {
         "code": "String",
         "message": "String"
      }
    }
  }
```

Lo stato dell'asset si trova in `assetStatus.state` dell'oggetto JSON.

Verifica dello stato di un modello di asset o di un modello di componente

È possibile utilizzare la AWS IoT SiteWise console o l'API per verificare lo stato di un modello di asset o di un modello di componente.

Argomenti

- Verifica dello stato di un modello di asset o di un modello di componente (console)
- Verifica dello stato di un modello di asset o di un modello di componente ()AWS CLI

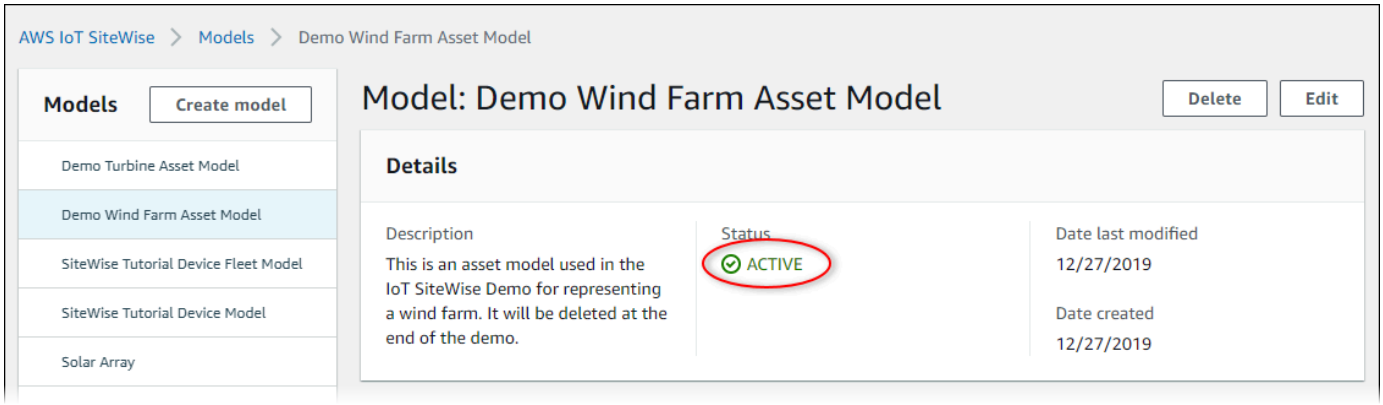
Verifica dello stato di un modello di asset o di un modello di componente (console)

Utilizzate la seguente procedura per verificare lo stato di un modello di asset o di un modello di componente nella AWS IoT SiteWise console.

> **Tip**
>
> I modelli di asset e i modelli di componenti sono entrambi elencati in Modelli nel pannello di navigazione. Il pannello Dettagli del modello di asset o del modello di componente selezionato indica di che tipo si tratta.

Per verificare lo stato di un modello di asset o di un modello di componente (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione selezionare Models (Modelli).
3. Scegliete il modello da controllare.
4. Trova Stato nel pannello Dettagli.



Verifica dello stato di un modello di asset o di un modello di componente ()AWS CLI

È possibile utilizzare il AWS CLI per verificare lo stato di un modello di asset o di un modello di componente.

Per verificare lo stato di un modello di asset o di un modello di componente, utilizzate l'DescribeAssetModeloperazione con il `assetModelId` parametro.

> **Tip**
>
> AWS CLI definisce i modelli di componenti come un tipo di modello di asset. Pertanto, si utilizza la stessa DescribeAssetModeloperazione per entrambi i tipi di modello. Il `assetModelType` campo nella risposta indica se è un `ASSET_MODEL` o un`COMPONENT_MODEL`.

Per verificare lo stato di un modello di asset o di un modello di componente (AWS CLI)

- Eseguite il comando seguente per descrivere il modello. *asset-model-id*Sostituitelo con l'ID o l'ID esterno del modello di asset o del modello di componente. L'ID esterno è un ID definito dall'utente. Per ulteriori informazioni, consulta Riferimento a oggetti con ID esterni nella Guida per l'utente di AWS IoT SiteWise .

  ```
  aws iotsitewise describe-asset-model --asset-model-id asset-model-id
  ```

  L'operazione restituisce una risposta che contiene i dettagli del modello. La risposta contiene un oggetto `assetModelStatus` che ha la seguente struttura.

  ```
  {
      ...
      "assetModelStatus": {
        "state": "String",
        "error": {
           "code": "String",
           "message": "String"
        }
      }
    }
  ```

  Lo stato del modello si trova `assetModelStatus.state` nell'oggetto JSON.

Modelli compositi personalizzati (componenti)

Quando si modella un asset industriale particolarmente complesso, ad esempio un macchinario complicato composto da molte parti, può diventare difficile mantenere i modelli di asset organizzati e gestibili.

In questi casi, puoi aggiungere modelli compositi personalizzati, o componenti, se utilizzi la console, ai modelli di asset e ai modelli di componenti esistenti. Questi vi aiutano a rimanere organizzati raggruppando le proprietà correlate e riutilizzando le definizioni dei sottocomponenti.

Esistono due tipi di modelli compositi personalizzati:

- I modelli compositi personalizzati in linea definiscono un insieme di proprietà raggruppate che si applicano al modello di asset o al modello di componente a cui appartiene il modello composito

personalizzato. Li utilizzate per raggruppare le proprietà correlate. Sono costituiti da un nome, una descrizione e un insieme di proprietà del modello di asset. Non sono riutilizzabili.

- I modelli compositi omponent-model-based personalizzati C fanno riferimento a un modello di componente che si desidera includere nel modello di asset o nel modello di componente. Li utilizzate per includere sottoassiemi standard nel modello. Sono costituiti da un nome, una descrizione e l'ID del modello di componente a cui fanno riferimento. Non hanno proprietà proprie; il modello di componente a cui si fa riferimento fornisce le proprietà associate a tutti gli asset creati.

Le seguenti sezioni illustrano come utilizzare modelli compositi personalizzati nei progetti.

Argomenti

Modelli compositi personalizzati in linea

I modelli compositi personalizzati in linea consentono di organizzare il modello di asset raggruppando le proprietà correlate.

Ad esempio, supponete di voler modellare un asset robotico. Il robot include un servomotore, un alimentatore e una batteria. Ciascuna di queste parti costituenti ha le proprie proprietà che si desidera includere nel modello. È possibile definire un modello di asset denominato `robot_model` con proprietà come le seguenti.

- `robot_model`
  - `servo_status` (numero intero)
  - `servo_position` (doppio)
  - `powersupply_status` (numero intero)
  - `powersupply_temperature` (doppio)
  - `battery_status` (numero intero)
  - `battery_charge` (doppio)

Tuttavia, in alcuni casi, potrebbero esserci molti sottoassiemi oppure i sottoassiemi stessi potrebbero avere molte proprietà. In questi casi, potrebbero esserci così tante proprietà da rendere complicato il riferimento e la gestione in un unico elenco semplice alla radice del modello, come nell'esempio precedente.

Per gestire tali situazioni, è possibile utilizzare un modello composito personalizzato in linea per raggruppare le proprietà. Un modello composito personalizzato in linea è un modello composito personalizzato che definisce le proprie proprietà. Ad esempio, puoi modellare il tuo robot come segue.

- `robot_model`
  - `servo`
    - `status`(numero intero)
    - `position`(doppio)
  - `powersupply`
    - `status`(numero intero)
    - `temperature` (doppio)
  - `battery`
    - `status`(numero intero)
    - `charge`(doppio)

Nell'esempio precedente, `servopowersupply`, e `battery` sono i nomi dei modelli compositi personalizzati in linea definiti all'interno del modello di `robot_model` asset. Ciascuno di questi modelli compositi definisce quindi le proprie proprietà.

> **Note**
>
> In questo caso, ogni modello composito personalizzato definisce le proprie proprietà, in modo che tutte le proprietà facciano parte del modello di asset stesso (`robot_model`in questo caso). Queste proprietà non sono condivise con altri modelli di asset o modelli di componenti. Ad esempio, se avete creato un altro modello di asset che aveva anche un modello composito personalizzato in linea chiamato`servo`, apportare una modifica all'`servo`interno non `robot_model` influirebbe sulla `servo` definizione dell'altro modello di asset.

Se desiderate implementare tale condivisione (ad esempio, avere una sola definizione per un servo, condivisibile da tutti i vostri modelli di asset), dovreste invece creare un modello a componenti relativo al servo e quindi creare modelli component-model-basedcompositi che vi facciano riferimento. Per i dettagli, consultate la sezione seguente.

Per informazioni su come creare modelli compositi personalizzati in linea, vedereCreazione di modelli compositi personalizzati (Componenti).

C modelli compositi omponent-model-based personalizzati

È possibile creare un modello di componente in AWS IoT SiteWise per definire un sottoassieme standard riutilizzabile. Dopo aver creato un modello di componente, potete aggiungere riferimenti ad esso negli altri modelli di asset e modelli di componenti. A tale scopo, aggiungete un modello composito component-model-based personalizzato a qualsiasi modello in cui desiderate fare riferimento al componente. È possibile aggiungere riferimenti al componente da molti modelli o più volte all'interno dello stesso modello.

In questo modo, è possibile evitare di duplicare le stesse definizioni tra i modelli. Inoltre, semplifica la manutenzione dei modelli, poiché qualsiasi modifica apportata a un modello componente si rifletterà su tutti i modelli di asset che lo utilizzano.

Ad esempio, supponete che l'impianto industriale disponga di molti tipi di apparecchiature che utilizzano tutte lo stesso tipo di servomotore. Alcuni di essi hanno molti servomotori in un'unica apparecchiatura. Crei un modello di asset per ogni tipo di apparecchiatura, ma non vuoi duplicare la definizione di `servo` ogni volta. Volete modellarlo una sola volta e utilizzarlo nei vari modelli di asset. Se successivamente apporti una modifica alla definizione di`servo`, questa verrà aggiornata in tutti i tuoi modelli e asset.

Per modellare il robot dell'esempio precedente in questo modo, potete definire servomotori, alimentatori e batterie come modelli di componenti, in questo modo.

- `servo_component_model`
  - `status`(numero intero)
  - `position`(doppio)

- `powersupply_component_model`

    - `status`(numero intero)
    - `temperature` (doppio)

- `battery__component_model`
    - `status`(numero intero)
    - `charge`(doppio)

È quindi possibile definire modelli di asset, ad esempio `robot_model` che fanno riferimento a questi componenti. Più modelli di asset possono fare riferimento allo stesso modello di componente. È inoltre possibile fare riferimento allo stesso modello di componente più volte in un unico modello di asset, ad esempio se il robot è dotato di più servomotori.

- `robot_model`
    - `servo1`(riferimento:) `servo_component_model`
    - `servo2`(riferimento:`servo_component_model`)
    - `servo3`(riferimento:`servo_component_model`)
    - `powersupply` (riferimento:`powersupply_component_model`)
    - `battery`(riferimento:`battery_component_model`)

Per informazioni su come creare modelli di componenti, vedereCreazione di modelli di componenti.

Per informazioni su come fare riferimento ai modelli di componenti in altri modelli, vedereCreazione di modelli compositi personalizzati (Componenti).

Utilizzo di percorsi per fare riferimento alle proprietà personalizzate del modello composito

Quando create una proprietà su un modello di asset, un modello di componente o un modello composito personalizzato, potete farvi riferimento da altre proprietà che ne utilizzano il valore, come trasformazioni e metriche.

AWS IoT SiteWise offre diversi modi per fare riferimento alla proprietà. Il modo più semplice è spesso quello di utilizzare l'ID della proprietà. Tuttavia, se la proprietà a cui desiderate fare riferimento si

trova su un modello composito personalizzato, potrebbe essere più utile farvi riferimento invece tramite il percorso.

Un percorso è una sequenza ordinata di segmenti di percorso che specifica una proprietà in termini di posizione tra i modelli compositi annidati all'interno di un modello di asset e di un modello composito.

Ottenere i percorsi delle proprietà

Puoi ottenere il percorso di una proprietà dal `path` campo della sua AssetModelProperty.

Ad esempio, supponete di avere un modello di asset `robot_model` che contiene un modello `servo` composito personalizzato con una proprietà`position`. Se chiami DescribeAssetModelCompositeModel`servo`, la `position` proprietà elencherà un `path` campo simile al seguente:

```
"path": [
    {
       "id": "asset model ID",
       "name": "robot_model"
    },
    {
       "id": "composite model ID",
       "name": "servo"
    },
    {
       "id": "property ID",
       "name": "position"
    }
]
```

Utilizzo dei percorsi delle proprietà

È possibile utilizzare un percorso di proprietà quando si definisce una proprietà che fa riferimento ad altre proprietà, ad esempio una trasformazione o una metrica.

Una proprietà utilizza una variabile per fare riferimento a un'altra proprietà. Per ulteriori informazioni sull'utilizzo delle variabili, vedereUtilizzo di variabili nelle espressioni delle formule.

Quando si definisce una variabile per fare riferimento a una proprietà, è possibile utilizzare l'ID della proprietà o il relativo percorso.

Per definire una variabile che utilizza il percorso della proprietà di riferimento, specificate il `propertyPath` campo del relativo valore.

Ad esempio, per definire un modello di asset con una metrica che fa riferimento a una proprietà utilizzando un percorso, potete passare un payload come questo a: CreateAssetModel

```
{
    ...
    "assetModelProperties": [
        {
            ...
            "type": {
                "metric": {
                    ...
                    "variables": [
                        {
                            "name": "variable name",
                            "value": {
                                "propertyPath": [
                                    path segments
                                ]
                            }
                        }
                    ],
                    ...
                }
            },
            ...
        },
        ...
    ],
    ...
}
```

Lavorare con gli ID degli oggetti

AWS IoT SiteWise definisce vari tipi di oggetti persistenti, come risorse, modelli di risorse, proprietà e gerarchie. Tutti questi oggetti dispongono di identificatori univoci che è possibile utilizzare per recuperarli, aggiornarli ed eliminarli.

AWS IoT SiteWise offre ai clienti diverse opzioni per la creazione di ID. AWS IoT SiteWise ne genera uno automaticamente per te al momento della creazione dell'oggetto. Gli utenti possono anche fornire i propri ID agli oggetti.

Argomenti

Lavorare con gli UUID degli oggetti

Ogni oggetto persistente AWS IoT SiteWise ha un UUID per identificarlo. Ad esempio, i modelli di asset hanno un ID del modello di asset, gli asset hanno un ID di asset e così via. Questo ID viene assegnato al momento della creazione dell'oggetto e rimane invariato per tutta la durata dell'oggetto.

Quando crei un nuovo oggetto, per impostazione predefinita AWS IoT SiteWise genera un ID univoco per te. Puoi anche fornire il tuo ID al momento della creazione in formato UUID.

> **Note**
>
> Gli UUID devono essere univoci a livello globale all'interno della AWS regione in cui sono stati creati e per lo stesso tipo di oggetto. Quando AWS IoT SiteWise genera automaticamente un ID per te, è sempre unico. Se scegli il tuo ID, assicurati che sia unico.

Ad esempio, se crei un nuovo modello di asset chiamando CreateAssetModel, puoi fornire il tuo UUID nel `assetModelId` campo opzionale della richiesta.

Al contrario, se si omette `assetModelId` dalla richiesta, AWS IoT SiteWise genera un UUID per il nuovo modello di asset.

Utilizzo di ID esterni

Per definire il proprio ID in un formato diverso dall'UUID, è possibile assegnare un ID esterno. Ad esempio, puoi farlo se riutilizzi un ID che stai utilizzando in un sistema che non lo è o se desideri renderlo più AWS leggibile dall'uomo. Gli ID esterni hanno un formato più flessibile. Puoi usarli per fare riferimento ai tuoi oggetti nelle operazioni AWS IoT SiteWise API in cui altrimenti utilizzeresti l'UUID.

Come gli UUID, ogni ID esterno deve essere unico nel suo contesto. Ad esempio, non puoi avere due modelli di asset con lo stesso ID esterno. Inoltre, come gli UUID, un oggetto può avere un solo ID esterno nel corso della sua vita, che non può cambiare.

Differenze tra ID esterni e UUID

Gli ID esterni differiscono dagli UUID nei seguenti modi:

- Ogni oggetto ha un UUID, ma gli ID esterni sono opzionali.
- AWS IoT SiteWise non genera mai ID esterni. Li fornisci tu stesso.
- Se l'oggetto non ne ha già uno, puoi assegnare un ID esterno in qualsiasi momento.

Formato degli ID esterni

Un ID esterno valido ha le seguenti proprietà:

- Ha una lunghezza compresa tra 2 e 128 caratteri.
- Il primo e l'ultimo carattere devono essere alfanumerici (A-Z, a-z, 0-9).
- I caratteri diversi dal primo e dall'ultimo devono essere alfanumerici oppure devono essere uno dei seguenti: `_-.:`

Ad esempio, un ID esterno deve essere conforme alla seguente espressione regolare:

```
[a-zA-Z0-9][a-zA-Z0-9_\-.:]*[a-zA-Z0-9]+
```

Riferimento a oggetti con ID esterni

In molti punti in cui è possibile fare riferimento a un oggetto utilizzando il relativo UUID, è possibile utilizzare invece il relativo ID esterno, se ne ha uno. A tale scopo, aggiungete l'ID esterno alla stringa. `externalId:`

Ad esempio, supponete di avere un modello di asset il cui UUID (asset model ID) è`a1b2c3d4-5678-90ab-cdef-11111EXAMPLE`, che ha anche l'ID esterno. `myExternalId` Chiama DescribeAssetModelper avere dettagli al riguardo. È possibile utilizzare uno dei seguenti valori come valore di`assetModelId`:

- Con lo stesso Asset Model ID (UUID): `a1b2c3d4-5678-90ab-cdef-11111EXAMPLE`
- Con l'ID esterno: `externalId:myExternalId`

```
aws iotsitewise describe-asset-model --asset-model-id a1b2c3d4-5678-90ab-
cdef-11111EXAMPLE
aws iotsitewise describe-asset-model --asset-model-id externalId:myExternalId
```

> **Note**
>
> Il `externalId:` prefisso, di per sé, non fa parte dell'ID esterno. È necessario fornire il prefisso solo quando si fornisce un ID esterno a un'operazione API che accetta UUID o ID esterni. Ad esempio, fornite il prefisso quando interrogate o aggiornate un oggetto esistente. Quando definite un ID esterno per un oggetto, ad esempio quando create un modello di asset, non includete il prefisso.

In questo modo potete utilizzare ID esterni al posto degli UUID per molte operazioni API in AWS IoT SiteWise, ma non per tutte. Ad esempio, GetAssetPropertyValue, deve utilizzare gli UUID; non supporta l'utilizzo di ID esterni.

Per determinare se una particolare operazione API supporta questo utilizzo, consulta l'API Reference.

Creazione di modelli di asset e modelli di componenti

AWS IoT SiteWise i modelli di asset e i modelli di componenti favoriscono la standardizzazione dei dati industriali. Un modello di asset o modello di componente contiene un nome, una descrizione, proprietà degli asset e (facoltativamente) modelli compositi personalizzati che raggruppano le proprietà o che fanno riferimento ai modelli di componenti per i sottoassiemi.

- Utilizzate un modello di asset per creare risorse. Oltre alle funzionalità sopra elencate, un modello di asset può contenere anche definizioni gerarchiche che definiscono le relazioni tra gli asset.
- Un modello di componente rappresenta un sottoassieme all'interno di un modello di asset o di un altro modello di componente. Quando create un modello di componente, potete aggiungere riferimenti ad esso nei modelli di asset e in altri modelli di componenti. Tuttavia, non è possibile creare risorse direttamente dai modelli di componenti.

Dopo aver creato un modello di asset o un modello di componente, potete creare modelli compositi personalizzati per raggruppare le proprietà o fare riferimento a modelli di componenti esistenti.

Per informazioni dettagliate su come creare modelli di asset e modelli di componenti, consultate le seguenti sezioni.

Argomenti

Creazione dei modelli di asset

AWS IoT SiteWise i modelli di asset favoriscono la standardizzazione dei dati industriali. Un modello include un nome e una descrizione, oltre a proprietà e definizioni gerarchiche di asset. Ad esempio, è possibile definire un modello di turbina eolica con proprietà di temperatura, rotazioni al minuto (RPM) e potenza. Quindi, è possibile definire un modello di parco eolico con una proprietà di potenza netta e una definizione di gerarchia di turbine eoliche.

> **Note**
>
> - Si consiglia di modellare l'operazione partendo dai nodi di livello inferiore. Ad esempio, crea il modello di turbina eolica prima di creare il modello di centrale eolica. Le definizioni della gerarchia delle risorse contengono riferimenti a modelli di asset esistenti. Con questo approccio, puoi definire le gerarchie di asset durante la creazione dei modelli.
> - I modelli di asset non possono contenere altri modelli di asset. Se dovete definire un modello a cui potete fare riferimento come sottoassieme all'interno di un altro modello, dovreste invece creare un modello componente-->. Per ulteriori informazioni, consulta Creazione di modelli di componenti.

Le sezioni seguenti descrivono come utilizzare la AWS IoT SiteWise console o l'API per creare modelli di asset. Nelle sezioni seguenti vengono inoltre descritti i diversi tipi di proprietà e gerarchie degli asset che puoi utilizzare per creare modelli.

Argomenti

- Modelli di asset di esempio
- Definizione delle gerarchie dei modelli di asset

Creazione di un modello di asset (console)

È possibile utilizzare la AWS IoT SiteWise console per creare un modello di asset. La AWS IoT SiteWise console offre varie funzionalità, come il completamento automatico delle formule, che possono aiutarti a definire modelli di asset validi.

Per creare un modello di asset (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione selezionare Models (Modelli).
3. Scegli Crea modello.
4. Nella pagina Crea modello, esegui le operazioni seguenti:

    a. Immetti un nome per il modello di asset, ad esempio **`Wind Turbine`** o **`Wind Turbine Model`**. Questo nome deve essere univoco rispetto a tutti i modelli del tuo account in questa regione.

    b. (Facoltativo) Aggiungete un ID esterno per il modello. Si tratta di un ID definito dall'utente. Per ulteriori informazioni, consulta Riferimento a oggetti con ID esterni nella Guida per l'utente di AWS IoT SiteWise .

    c. (Facoltativo) Aggiungi le definizioni misurazione per il modello. Le misurazioni rappresentano flussi di dati provenienti dall'apparecchiatura. Per ulteriori informazioni, consulta Definizione dei flussi di dati provenienti dalle apparecchiature (misurazioni).

    d. (Facoltativo) Aggiungi le definizioni di trasformazione per il modello. Le trasformazioni sono formule che mappano i dati da un modulo all'altro. Per ulteriori informazioni, consulta Trasformazione dei dati (trasformazioni).

    e. (Facoltativo) Aggiungi le definizioni parametro per il modello. Le metriche sono formule che aggregano i dati su intervalli di tempo. Le metriche possono inserire dati dalle risorse associate, in modo da poter calcolare valori che rappresentano l'operazione o un sottoinsieme dell'operazione. Per ulteriori informazioni, consulta Aggregazione di dati da proprietà e altre risorse (metriche).

    f. (Facoltativo) Aggiungi le definizioni gerarchiche per il modello. Le gerarchie sono relazioni tra risorse. Per ulteriori informazioni, consulta Definizione delle gerarchie dei modelli di asset.

g. (Facoltativo) Aggiungi i tag per il modello di asset. Per ulteriori informazioni, consulta Taggare le tue risorse AWS IoT SiteWise.

h. Scegli Crea modello.

Quando si crea un modello di asset, la AWS IoT SiteWise console accede alla pagina del nuovo modello. In questa pagina puoi vedere lo stato del modello che inizialmente è CREAZIONE IN CORSO. Questa pagina si aggiorna automaticamente, quindi attendi l'aggiornamento dello stato del modello.

> **Note**
>
> Il processo di creazione del modello di asset può richiedere fino a qualche minuto, nei casi di maggiore complessità. Dopo che lo stato del modello di asset è ATTIVO, potete utilizzare il modello di asset per creare risorse. Per ulteriori informazioni, consulta Stati di asset e modelli.

5. (Facoltativo) Dopo aver creato il modello di asset, potete configurare il modello di asset per l'edge. Per ulteriori informazioni su SiteWise Edge, consultaAbilitare l'elaborazione dei dati edge.

a. Nella pagina del modello, scegli Configure for Edge.

b. Nella pagina di configurazione del modello, scegli la configurazione del bordo per il tuo modello. Questo controlla dove AWS IoT SiteWise è possibile calcolare e archiviare le proprietà associate a questo modello di asset. Per ulteriori informazioni sulla configurazione del modello per l'edge, consulta. the section called “Configurazione della funzionalità edge”

c. Per la configurazione edge personalizzata, scegliete la posizione in cui desiderate AWS IoT SiteWise calcolare e archiviare ciascuna delle proprietà del modello di asset.

> **Note**
>
> Le trasformazioni e le metriche associate devono essere configurate per la stessa posizione. Per ulteriori informazioni sulla configurazione del modello per l'edge, consulta. the section called “Configurazione della funzionalità edge”

d. Selezionare Salva. Nella pagina del modello, la configurazione di Edge dovrebbe ora essere configurata.

Creazione di un modello di asset (AWS CLI)

È possibile utilizzare AWS Command Line Interface (AWS CLI) per creare un modello di asset.

Utilizzate l'CreateAssetModeloperazione per creare un modello di asset con proprietà e gerarchie. Questa operazione prevede un payload con la seguente struttura.

```
{
  "assetModelType": "ASSET_MODEL",
  "assetModelName": "String",
  "assetModelDescription": "String",
  "assetModelProperties": Array of AssetModelProperty,
  "assetModelHierarchies": Array of AssetModelHierarchyDefinition
}
```

Per creare un modello di asset ()AWS CLI

1. Crea un file denominato `asset-model-payload.json` e copia il seguente oggetto JSON nel file.

   ```
   {
     "assetModelType": "ASSET_MODEL",
     "assetModelName": "",
     "assetModelDescription": "",
     "assetModelProperties": [

     ],
     "assetModelHierarchies": [

     ],
     "assetModelCompositeModels": [

     ]
   }
   ```

2. Utilizza l'editor di testo JSON preferito per modificare il file `asset-model-payload.json` come segue:

   a. Immetti un nome (`assetModelName`) per il modello di asset, ad esempio **`Wind Turbine`** o **`Wind Turbine Model`**. In questo caso, questo nome deve essere univoco per tutti i modelli di asset e i modelli di componenti del tuo account Regione AWS.

b. (Facoltativo) Inserite un ID esterno (`assetModelExternalId`) per il modello di asset. Si tratta di un ID definito dall'utente. Per ulteriori informazioni, consulta Riferimento a oggetti con ID esterni nella Guida per l'utente di AWS IoT SiteWise .

c. (Facoltativo) Immetti una descrizione (`assetModelDescription`) per il modello di asset o rimuovi la coppia chiave-valore `assetModelDescription`.

d. (Facoltativo) Definisci le proprietà dell'asset (`assetModelProperties`) per il modello. Per ulteriori informazioni, consulta Definizione delle proprietà dei dati.

e. (Facoltativo) Definisci le gerarchie dell'asset (`assetModelHierarchies`) per il modello. Per ulteriori informazioni, consulta Definizione delle gerarchie dei modelli di asset.

f. (Facoltativo) Definite gli allarmi per il modello. Gli allarmi monitorano altre proprietà in modo da poter identificare quando le apparecchiature o i processi richiedono attenzione. Ogni definizione di allarme è un modello composito (`assetModelCompositeModels`) che standardizza l'insieme di proprietà utilizzate dall'allarme. Per ulteriori informazioni, consulta Monitoraggio dei dati con allarmi e Definizione degli allarmi sui modelli di asset.

g. (Facoltativo) Aggiungi i tag (`tags`) per il modello di asset. Per ulteriori informazioni, consulta Taggare le tue risorse AWS IoT SiteWise.

3. Esegui il comando seguente per creare un modello di asset dalla definizione nel file JSON.

```
aws iotsitewise create-asset-model --cli-input-json file://asset-model-payload.json
```

L'operazione restituisce una risposta contenente l'`assetModelId` univoco al quale fai riferimento quando crei un asset. La risposta contiene anche lo stato del modello (`assetModelStatus.state`) che inizialmente è `CREATING`. Lo stato del modello di asset è `CREATING` fino a quando le modifiche non si propagano.

> **Note**
>
> Il processo di creazione del modello di asset può richiedere fino a qualche minuto, nei casi di maggiore complessità. Per verificare lo stato attuale del modello di asset, utilizzate l'DescribeAssetModeloperazione specificando il. `assetModelId` Una volta contrassegnato dallo stato `ACTIVE`, il modello potrà essere utilizzato per creare asset. Per ulteriori informazioni, consulta Stati di asset e modelli.

4. (Facoltativo) Crea modelli compositi personalizzati per il tuo modello di asset. Con i modelli compositi personalizzati, è possibile raggruppare le proprietà all'interno del modello o includere

un sottoassieme facendo riferimento a un modello di componente. Per ulteriori informazioni, consulta Creazione di modelli compositi personalizzati (Componenti).

Modelli di asset di esempio

Questa sezione contiene esempi di definizioni di modelli di asset che è possibile utilizzare per creare modelli di asset con gli SDK e. AWS CLI AWS IoT SiteWise Questi modelli di asset rappresentano una turbina eolica e un parco eolico. Gli asset delle turbine eoliche acquisiscono i dati grezzi dei sensori e calcolano valori come la potenza e la velocità media del vento. Gli asset del parco eolico calcolano valori come la potenza totale per tutte le turbine eoliche del parco eolico.

Argomenti

- Modello di asset turbina eolica
- Modello di asset centrale eolica

Modello di asset turbina eolica

Il seguente modello di asset rappresenta una turbina in una centrale eolica. La turbina eolica acquisisce i dati dei sensori per calcolare valori come la potenza e la velocità media del vento.

> **Note**
>
> Questo modello di esempio è simile al modello di turbina eolica mostrato nella demo. AWS IoT SiteWise Per ulteriori informazioni, consulta Utilizzo della AWS IoT SiteWise demo.

```
{
  "assetModelType": "ASSET_MODEL",
  "assetModelName": "Wind Turbine Asset Model",
  "assetModelDescription": "Represents a turbine in a wind farm.",
  "assetModelProperties": [
    {
      "name": "Location",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "Renton"
        }
      }
```

```
    },
    {
      "name": "Make",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "Amazon"
        }
      }
    },
    {
      "name": "Model",
      "dataType": "INTEGER",
      "type": {
        "attribute": {
          "defaultValue": "500"
        }
      }
    },
    {
      "name": "Torque (KiloNewton Meter)",
      "dataType": "DOUBLE",
      "unit": "kNm",
      "type": {
        "measurement": {}
      }
    },
    {
      "name": "Wind Direction",
      "dataType": "DOUBLE",
      "unit": "Degrees",
      "type": {
        "measurement": {}
      }
    },
    {
      "name": "RotationsPerMinute",
      "dataType": "DOUBLE",
      "unit": "RPM",
      "type": {
        "measurement": {}
      }
    },
    {
```

```
      "name": "Wind Speed",
      "dataType": "DOUBLE",
      "unit": "m/s",
      "type": {
        "measurement": {}
      }
    },
    {
      "name": "RotationsPerSecond",
      "dataType": "DOUBLE",
      "unit": "RPS",
      "type": {
        "transform": {
          "expression": "rpm / 60",
          "variables": [
            {
              "name": "rpm",
              "value": {
                "propertyId": "RotationsPerMinute"
              }
            }
          ]
        }
      }
    },
    {
      "name": "Overdrive State",
      "dataType": "DOUBLE",
      "type": {
        "transform": {
          "expression": "gte(torque, 3)",
          "variables": [
            {
              "name": "torque",
              "value": {
                "propertyId": "Torque (KiloNewton Meter)"
              }
            }
          ]
        }
      }
    },
    {
      "name": "Average Power",
```

```
      "dataType": "DOUBLE",
      "unit": "Watts",
      "type": {
        "metric": {
          "expression": "avg(torque) * avg(rps) * 2 * 3.14",
          "variables": [
            {
              "name": "torque",
              "value": {
                "propertyId": "Torque (Newton Meter)"
              }
            },
            {
              "name": "rps",
              "value": {
                "propertyId": "RotationsPerSecond"
              }
            }
          ],
          "window": {
            "tumbling": {
              "interval": "5m"
            }
          }
        }
      }
    },
    {
      "name": "Average Wind Speed",
      "dataType": "DOUBLE",
      "unit": "m/s",
      "type": {
        "metric": {
          "expression": "avg(windspeed)",
          "variables": [
            {
              "name": "windspeed",
              "value": {
                "propertyId": "Wind Speed"
              }
            }
          ],
          "window": {
            "tumbling": {
```

```
            "interval": "5m"
          }
        }
      }
    }
  },
  {
    "name": "Torque (Newton Meter)",
    "dataType": "DOUBLE",
    "unit": "Nm",
    "type": {
      "transform": {
        "expression": "knm * 1000",
        "variables": [
          {
            "name": "knm",
            "value": {
              "propertyId": "Torque (KiloNewton Meter)"
            }
          }
        ]
      }
    }
  },
  {
    "name": "Overdrive State Time",
    "dataType": "DOUBLE",
    "unit": "Seconds",
    "type": {
      "metric": {
        "expression": "statetime(overdrive_state)",
        "variables": [
          {
            "name": "overdrive_state",
            "value": {
              "propertyId": "Overdrive State"
            }
          }
        ],
        "window": {
          "tumbling": {
            "interval": "5m"
          }
        }
```

```
        }
      }
    }
  ],
  "assetModelHierarchies": []
}
```

Modello di asset centrale eolica

Il seguente modello di asset rappresenta una centrale eolica che comprende più turbine eoliche. Questo modello di asset definisce una gerarchia rispetto al modello di turbina eolica. Ciò consente al parco eolico di calcolare i valori (come la potenza media) a partire dai dati di tutte le turbine eoliche del parco eolico.

> **Note**
>
> Questo modello di esempio è simile al modello di parco eolico illustrato nella AWS IoT SiteWise demo. Per ulteriori informazioni, consulta Utilizzo della AWS IoT SiteWise demo.

Questo modello di asset dipende da Modello di asset turbina eolica. Sostituisci i valori `propertyId` e `childAssetModelId` con quelli di un modello di asset turbina eolica esistente.

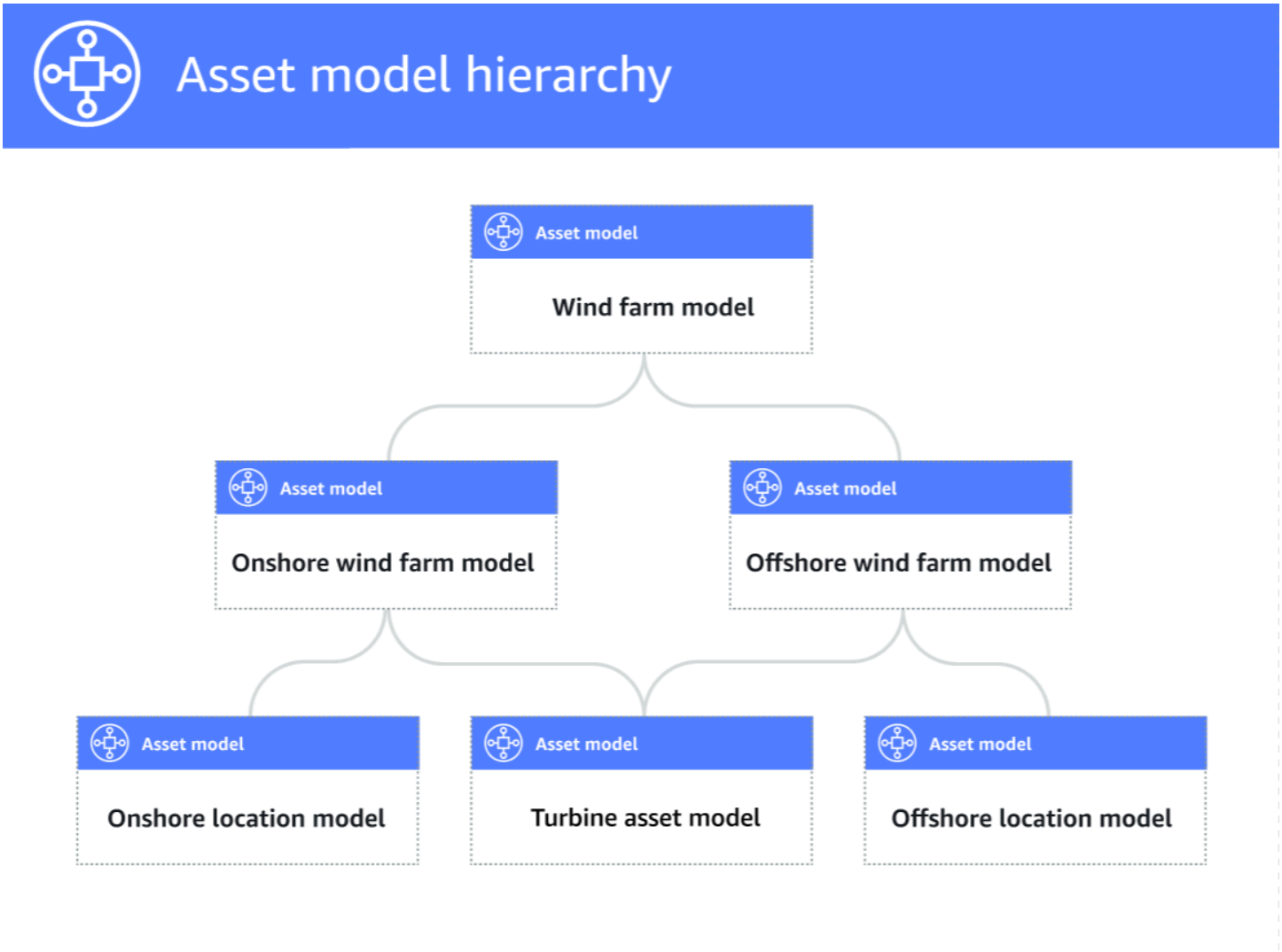
```
{
  "assetModelName": "Wind Farm Asset Model",
  "assetModelDescription": "Represents a wind farm.",
  "assetModelProperties": [
    {
      "name": "Code",
      "dataType": "INTEGER",
      "type": {
        "attribute": {
          "defaultValue": "300"
        }
      }
    },
    {
      "name": "Location",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "Renton"
```

```
        }
      }
    },
    {
      "name": "Reliability Manager",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "Mary Major"
        }
      }
    },
    {
      "name": "Total Overdrive State Time",
      "dataType": "DOUBLE",
      "unit": "seconds",
      "type": {
        "metric": {
          "expression": "sum(overdrive_state_time)",
          "variables": [
            {
              "name": "overdrive_state_time",
              "value": {
                "propertyId": "ID of Overdrive State Time property in Wind Turbine
Asset Model",
                "hierarchyId": "Turbine Asset Model"
              }
            }
          ],
          "window": {
            "tumbling": {
              "interval": "5m"
            }
          }
        }
      }
    },
    {
      "name": "Total Average Power",
      "dataType": "DOUBLE",
      "unit": "Watts",
      "type": {
        "metric": {
          "expression": "sum(turbine_avg_power)",
```

```
          "variables": [
            {
              "name": "turbine_avg_power",
              "value": {
                "propertyId": "ID of Average Power property in Wind Turbine Asset
 Model",
                "hierarchyId": "Turbine Asset Model"
              }
            }
          ],
          "window": {
            "tumbling": {
              "interval": "5m"
            }
          }
        }
      }
    }
  ],
  "assetModelHierarchies": [
    {
      "name": "Turbine Asset Model",
      "childAssetModelId": "ID of Wind Turbine Asset Model"
    }
  ]
}
```

Definizione delle gerarchie dei modelli di asset

È possibile definire gerarchie di modelli di asset per creare associazioni logiche tra i modelli di asset utilizzati nelle operazioni industriali. Ad esempio, è possibile definire un parco eolico composto da parchi eolici onshore e offshore. Un parco eolico onshore contiene una turbina e una posizione onshore. Un parco eolico offshore contiene una turbina e un'ubicazione offshore.



Quando si associa un modello di asset figlio a un modello di asset principale tramite una gerarchia, le metriche del modello di asset principale possono inserire dati dalle metriche del modello di asset figlio. È possibile utilizzare le gerarchie e le metriche dei modelli di asset per calcolare statistiche che forniscono informazioni dettagliate sulla propria operazione o su un sottoinsieme di essa. Per ulteriori informazioni, consulta Aggregazione di dati da proprietà e altre risorse (metriche).

Ogni gerarchia definisce una relazione tra un modello di asset principale e un modello di asset figlio. In un modello di asset principale, è possibile definire più gerarchie per lo stesso modello di asset figlio. Ad esempio, se nei parchi eolici sono presenti due diversi tipi di turbine eoliche, in cui tutte le turbine eoliche sono rappresentate dallo stesso modello di asset, è possibile definire una gerarchia per ogni tipo. Quindi, è possibile definire le metriche nel modello del parco eolico per calcolare statistiche indipendenti e combinate per ogni tipo di turbina eolica.

Un modello di asset principale può essere associato a più modelli di asset secondari. Ad esempio, se disponete di un parco eolico onshore e un parco eolico offshore rappresentati da due diversi modelli di asset, potete associare questi modelli di asset allo stesso modello di asset del parco eolico principale.

Un modello di asset figlio può anche essere associato a più modelli di asset principali. Ad esempio, se disponete di due diversi tipi di parchi eolici, in cui tutte le turbine eoliche sono rappresentate dallo stesso modello di asset, potete associare il modello di asset delle turbine eoliche a diversi modelli di asset di parchi eolici.

> **Note**
>
> Quando si definisce una gerarchia di modelli di asset, il modello di asset figlio deve essere `ACTIVE` o avere una versione precedente. `ACTIVE` Per ulteriori informazioni, consulta Stati di asset e modelli.

Dopo aver definito i modelli di asset gerarchici e aver creato gli asset, puoi associare gli asset per completare la relazione padre-figlio. Per ulteriori informazioni, consulta Creazione degli asset e Associazione e annullamento dell'associazione degli asset.

Argomenti

- Definizione delle gerarchie dei modelli di asset (console)
- Definizione delle gerarchie degli asset ()AWS CLI

Definizione delle gerarchie dei modelli di asset (console)

Quando si definisce una gerarchia per un modello di asset nella AWS IoT SiteWise console, si specificano i seguenti parametri:

- Nome della gerarchia: il nome della gerarchia, ad esempio. **`Wind Turbines`**
- Modello gerarchico: il modello di asset secondario.
- ID esterno della gerarchia (opzionale): si tratta di un ID definito dall'utente. Per ulteriori informazioni, consulta Riferimento a oggetti con ID esterni nella Guida per l'utente di AWS IoT SiteWise .

Per ulteriori informazioni, consulta Creazione di un modello di asset (console).

Definizione delle gerarchie degli asset ()AWS CLI

Quando definite una gerarchia per un modello di asset con l' AWS IoT SiteWise API, specificate i seguenti parametri:

- `name`— Il nome della gerarchia, ad esempio. **`Wind Turbines`**
- `childAssetModelId`— L'ID o l'ID esterno del modello di asset secondario per la gerarchia. È possibile utilizzare l'ListAssetModelsoperazione per trovare l'ID di un modello di asset esistente.

Example Definizione della gerarchia di esempio

L'esempio seguente mostra una gerarchia di modelli di asset che rappresenta la relazione tra un parco eolico e le turbine eoliche. Questo oggetto è un esempio di. AssetModelHierarchy Per ulteriori informazioni, consulta Creazione di un modello di asset (AWS CLI).

```
{
  ...
  "assetModelHierarchies": [
    {
      "name": "Wind Turbines",
      "childAssetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE"
    },
  ]
}
```

Creazione di modelli di componenti

Utilizzate i modelli di AWS IoT SiteWise componenti per definire sottoassiemi a cui potete fare riferimento dai modelli di asset o da altri modelli di componenti. In questo modo, è possibile riutilizzare la definizione del componente su più altri modelli o più volte all'interno dello stesso modello.

Il processo di definizione di un modello di componente è molto simile alla definizione di un modello di asset. Come un modello di asset, un modello di componente ha un nome, una descrizione e proprietà di asset. Tuttavia, i modelli di componenti non possono includere definizioni della gerarchia degli asset, poiché i modelli di componenti stessi non possono essere utilizzati per creare risorse direttamente. Inoltre, i modelli di componenti non possono definire allarmi.

Ad esempio, è possibile definire un componente per un servomotore con proprietà di temperatura del motore, temperatura dell'encoder e resistenza di isolamento. Quindi, potete definire un modello di asset per apparecchiature che contengono servomotori, come una macchina CNC.

> **Note**
>
> - Si consiglia di modellare l'operazione partendo dai nodi di livello inferiore. Ad esempio, create il componente del servomotore prima di creare il modello di asset della macchina CNC. I modelli di asset contengono riferimenti a modelli di componenti esistenti.
> - Non è possibile creare una risorsa direttamente da un modello di componente. Per creare una risorsa che utilizza il componente, è necessario creare un modello di risorsa per la risorsa. Quindi, create un modello composito personalizzato che faccia riferimento al componente. Per ulteriori informazioni sulla creazione di modelli di asset, consulta Creazione dei modelli di asset Per ulteriori informazioni sulla creazione di modelli compositi personalizzati, consultaCreazione di modelli compositi personalizzati (Componenti).

Le sezioni seguenti descrivono come utilizzare l' AWS IoT SiteWise API per creare modelli di componenti.

Argomenti

- Creazione di un modello di componente (AWS CLI)
- Esempio di modello di componente

Creazione di un modello di componente (AWS CLI)

È possibile utilizzare AWS Command Line Interface (AWS CLI) per creare un modello di componente.

Utilizzate l'CreateAssetModeloperazione per creare un modello di componente con proprietà. Questa operazione prevede un payload con la seguente struttura:

```
{
  "assetModelType": "COMPONENT_MODEL",
  "assetModelName": "String",
  "assetModelDescription": "String",
  "assetModelProperties": Array of AssetModelProperty,
}
```

Per creare un modello di componente ()AWS CLI

1. Create un file chiamato `component-model-payload.json` e poi copiate il seguente oggetto JSON nel file:

```
{
  "assetModelType": "COMPONENT_MODEL",
  "assetModelName": "",
  "assetModelDescription": "",
  "assetModelProperties": [

  ]
}
```

2. Utilizza l'editor di testo JSON preferito per modificare il file `component-model-payload.json` come segue:

   a. Immettete un nome (`assetModelName`) per il modello del componente, ad esempio **`Servo Motor`** o**`Servo Motor Model`**. In questo caso, questo nome deve essere univoco per tutti i modelli di asset e i modelli di componenti del tuo account Regione AWS.

   b. (Facoltativo) Inserite un ID esterno (`assetModelExternalId`) per il modello del componente. Si tratta di un ID definito dall'utente. Per ulteriori informazioni, consulta Riferimento a oggetti con ID esterni nella Guida per l'utente di AWS IoT SiteWise .

   c. (Facoltativo) Immetti una descrizione (`assetModelDescription`) per il modello di asset o rimuovi la coppia chiave-valore `assetModelDescription`.

   d. (Facoltativo) Definite le proprietà degli asset (`assetModelProperties`) per il modello del componente. Per ulteriori informazioni, consulta Definizione delle proprietà dei dati.

   e. (Facoltativo) Aggiungi i tag (`tags`) per il modello di asset. Per ulteriori informazioni, consulta Taggare le tue risorse AWS IoT SiteWise.

3. Eseguite il comando seguente per creare un modello di componente dalla definizione nel file JSON.

```
aws iotsitewise create-asset-model --cli-input-json file://component-model-
payload.json
```

   L'operazione restituisce una risposta che contiene il `assetModelId` riferimento a cui si fa riferimento quando si aggiunge un riferimento al modello di componente in un modello di asset o in un altro modello di componente. La risposta contiene anche lo stato del modello

(`assetModelStatus.state`) che inizialmente è `CREATING`. Lo stato del modello di componente è valido `CREATING` fino alla propagazione delle modifiche.

> **Note**
>
> Il processo di creazione del modello di componente può richiedere fino a qualche minuto per i modelli complessi. Per verificare lo stato corrente del modello di componente, utilizzate l'DescribeAssetModeloperazione specificando il`assetModelId`. Una volta raggiunto lo stato del modello di componente`ACTIVE`, potete aggiungere riferimenti al modello di componente nei modelli di asset o in altri modelli di componenti. Per ulteriori informazioni, consulta Stati di asset e modelli.

4. (Facoltativo) Create modelli compositi personalizzati per il modello di componente. Con i modelli compositi personalizzati, è possibile raggruppare le proprietà all'interno del modello o includere un sottoassieme facendo riferimento a un altro modello di componente. Per ulteriori informazioni, consulta Creazione di modelli compositi personalizzati (Componenti).

Esempio di modello di componente

Questa sezione contiene un esempio di definizione del modello di componente che puoi utilizzare per creare un modello di componente con gli AWS IoT SiteWise SDK AWS CLI e. Questo modello di componente rappresenta un servomotore che può essere utilizzato all'interno di un'altra apparecchiatura, ad esempio una macchina CNC.

Argomenti

- Modello di componente del servomotore

Modello di componente del servomotore

Il seguente modello di componente rappresenta un servomotore che può essere utilizzato all'interno di apparecchiature come macchine CNC. Il servomotore fornisce varie misurazioni, come temperature e resistenza elettrica. Queste misurazioni sono disponibili come proprietà sugli asset creati da modelli di asset che fanno riferimento al modello dei componenti del servomotore.

```
{
    "assetModelName": "ServoMotor",
    "assetModelType": "COMPONENT_MODEL",
    "assetModelProperties": [
```

```
        {
            "dataType": "DOUBLE",
            "name": "Servo Motor Temperature",
            "type": {
            "measurement": {}
            },
            "unit": "Celsius"
        },
        {
            "dataType": "DOUBLE",
            "name": "Spindle speed",
            "type": {
            "measurement": {}
            },
            "unit": "rpm"
        }
    ]
}
```

Definizione delle proprietà dei dati

Le proprietà degli asset sono le strutture all'interno di ogni asset che contengono i dati degli asset. Esistono vari tipi di proprietà:

- Attributi: proprietà generalmente statiche di una risorsa, come il produttore del dispositivo o l'area geografica. Per ulteriori informazioni, consulta Definizione di dati statici (attributi).
- Misurazioni: i flussi di dati dei sensori del dispositivo raw di un asset, come i valori della velocità di rotazione con data e ora o i valori di temperatura con data e ora in gradi Celsius. Una misurazione è definita da un alias del flusso di dati. Per ulteriori informazioni, consulta Definizione dei flussi di dati provenienti dalle apparecchiature (misurazioni).
- Trasformazioni: i valori delle serie temporali trasformati di una risorsa, come i valori di temperatura con data e ora in gradi Fahrenheit. Una trasformazione è definita da un'espressione con le sue variabili. Per ulteriori informazioni, consulta Trasformazione dei dati (trasformazioni).
- Metriche: i dati di una risorsa aggregati in un intervallo di tempo specificato, ad esempio la temperatura media oraria. Un parametro è definito da un intervallo di tempo e un'espressione con le sue variabili. Le espressioni metriche possono inserire le proprietà metriche degli asset associati, in modo da poter calcolare le metriche che rappresentano l'operazione o un sottoinsieme dell'operazione. Per ulteriori informazioni, consulta Aggregazione di dati da proprietà e altre risorse (metriche).

Per ulteriori informazioni, consultare Creazione dei modelli di asset.

Per un esempio di come utilizzare misurazioni, trasformazioni e parametri per calcolare l'efficienza complessiva delle apparecchiature (OEE), consulta Calcolo dell'OEE in AWS IoT SiteWise.

Argomenti

- Definizione di dati statici (attributi)
- Definizione dei flussi di dati provenienti dalle apparecchiature (misurazioni)
- Trasformazione dei dati (trasformazioni)
- Aggregazione di dati da proprietà e altre risorse (metriche)
- Utilizzo delle espressioni di formula

Definizione di dati statici (attributi)

Gli attributi delle risorse rappresentano informazioni generalmente statiche, come il produttore del dispositivo o la posizione geografica. Ogni asset include gli attributi del modello da cui è stato creato.

Argomenti

- Definizione degli attributi (console)
- Definizione degli attributi ()AWS CLI

Definizione degli attributi (console)

Quando definite un attributo per un modello di asset nella AWS IoT SiteWise console, specificate i seguenti parametri:

- Nome: il nome della proprietà.
- Valore predefinito: (Facoltativo) Il valore predefinito per questo attributo. Gli asset creati dal modello hanno questo valore per l'attributo. Per ulteriori informazioni su come sostituire il valore predefinito in un asset creato da un modello, consulta Aggiornamento dei valori degli attributi.
- Tipo di dati: il tipo di dati della proprietà, che è uno dei seguenti:
  - String: una stringa con un massimo di 1024 byte.
  - Numero intero: un numero intero con segno a 32 bit con intervallo [-2.147.483.648, 2.147.483.647].
  - Doppio: un numero in virgola mobile con intervallo [-10^100, 10^100] e precisione doppia IEEE 754.

  - **`false`**Booleano — **`true`** o.
- ID esterno: (Facoltativo) Si tratta di un ID definito dall'utente. Per ulteriori informazioni, consulta Riferimento a oggetti con ID esterni nella Guida per l'utente di AWS IoT SiteWise .

Per ulteriori informazioni, consulta Creazione di un modello di asset (console).

Definizione degli attributi ()AWS CLI

Quando definite un attributo per un modello di asset con l' AWS IoT SiteWise API, specificate i seguenti parametri:

- `name`— Il nome della proprietà.
- `defaultValue`— (Facoltativo) Il valore predefinito per questo attributo. Gli asset creati dal modello hanno questo valore per l'attributo. Per ulteriori informazioni su come sostituire il valore predefinito in un asset creato da un modello, consulta Aggiornamento dei valori degli attributi.
- `dataType`— Il tipo di dati della proprietà, che è uno dei seguenti:
  - `STRING`— Una stringa con un massimo di 1024 byte.
  - `INTEGER`— Un numero intero con segno a 32 bit con intervallo [-2.147.483.648, 2.147.483.647].
  - `DOUBLE`— Un numero in virgola mobile con intervallo [-10^100, 10^100] e precisione doppia IEEE 754.
  - `BOOLEAN`— `true` oppure. `false`
- `externalId`— (Facoltativo) Si tratta di un ID definito dall'utente. Per ulteriori informazioni, consulta Riferimento a oggetti con ID esterni nella Guida per l'utente di AWS IoT SiteWise .

Example Definizione di attributo di esempio

Nell'esempio seguente viene illustrato un attributo che rappresenta il numero di modello di un asset con un valore predefinito. Questo oggetto è un esempio di un oggetto AssetModelPropertyche contiene un attributo. È possibile specificare questo oggetto come parte del payload della CreateAssetModelrichiesta per creare una proprietà di attributo. Per ulteriori informazioni, consulta Creazione di un modello di asset (AWS CLI).

```
{
...
"assetModelProperties": [
{
```

```
  "name": "Model number",
  "dataType": "STRING",
  "type": {
    "attribute": {
      "defaultValue": "BLT123"
    }
  }
}
],
...
}
```

Definizione dei flussi di dati provenienti dalle apparecchiature (misurazioni)

Una misurazione rappresenta il flusso di dati grezzi del sensore di un dispositivo, ad esempio valori di temperatura con data e ora o valori di rotazioni al minuto (RPM).

Argomenti

- Definizione delle misurazioni (console)
- Definizione delle misurazioni ()AWS CLI

Definizione delle misurazioni (console)

Quando definite una misurazione per un modello di asset nella console, specificate i seguenti parametri: AWS IoT SiteWise

- Nome: il nome della proprietà.
- Unità — (Facoltativo) L'unità scientifica della proprietà, ad esempio mm o Celsius.
- Tipo di dati: il tipo di dati della proprietà, che è uno dei seguenti:
  - String: una stringa con un massimo di 1024 byte.
  - Numero intero: un numero intero con segno a 32 bit con intervallo [-2.147.483.648, 2.147.483.647].
  - Doppio: un numero in virgola mobile con intervallo [-10^100, 10^100] e precisione doppia IEEE 754.
  - **`false`**Booleano — **`true`** o.
- ID esterno: (Facoltativo) Si tratta di un ID definito dall'utente. Per ulteriori informazioni, consulta Riferimento a oggetti con ID esterni nella Guida per l'utente di AWS IoT SiteWise .

Per ulteriori informazioni, consulta Creazione di un modello di asset (console).

Definizione delle misurazioni ()AWS CLI

Quando definite una misurazione per un modello di asset con l' AWS IoT SiteWise API, specificate i seguenti parametri:

- `name`— Il nome della proprietà.
- `dataType`— Il tipo di dati della proprietà, che è uno dei seguenti:
  - `STRING`— Una stringa con un massimo di 1024 byte.
  - `INTEGER`— Un numero intero con segno a 32 bit con intervallo [-2.147.483.648, 2.147.483.647].
  - `DOUBLE`— Un numero in virgola mobile con intervallo [-10^100, 10^100] e precisione doppia IEEE 754.
  - `BOOLEAN`— `true` oppure. `false`
- `unit`— (Facoltativo) L'unità scientifica della proprietà, ad esempio mm o Celsius.
- `externalId`— (Facoltativo) Si tratta di un ID definito dall'utente. Per ulteriori informazioni, consulta Riferimento a oggetti con ID esterni nella Guida per l'utente di AWS IoT SiteWise .

Example Definizione di misurazione di esempio

Nell'esempio seguente viene illustrata una misurazione che rappresenta le letture del sensore di temperatura di un asset. Questo oggetto è un esempio di un oggetto AssetModelPropertyche contiene una misurazione. È possibile specificare questo oggetto come parte del payload della CreateAssetModelrichiesta per creare una proprietà di misurazione. Per ulteriori informazioni, consulta Creazione di un modello di asset (AWS CLI).

La struttura di misurazione è una struttura vuota quando si definisce un modello di asset perché in seguito si configura ogni risorsa per utilizzare flussi di dati di dispositivo unici. Per ulteriori informazioni su come collegare la proprietà di misurazione di un asset al flusso di dati dei sensori di un dispositivo, consultaMappatura dei flussi di dati industriali alle proprietà degli asset.

```
{
      ...
      "assetModelProperties": [
      {
          "name": "Temperature C",
          "dataType": "DOUBLE",
          "type": {
```

```
                "measurement": {}
            },
            "unit": "Celsius"
        }
    ],
        ...
}
```

Trasformazione dei dati (trasformazioni)

Le trasformazioni sono espressioni matematiche che mappano i punti dati delle proprietà degli asset da un modulo all'altro. Un'espressione di trasformazione è costituita da variabili di proprietà degli asset, valori letterali, operatori e funzioni. I punti dati trasformati mantengono una one-to-one relazione con i punti dati di input. AWS IoT SiteWise calcola un nuovo punto dati trasformato ogni volta che una delle proprietà di input riceve un nuovo punto dati.

Ad esempio, se l'asset ha un flusso di misurazione della temperatura denominato `Temperature_C` con unità in Celsius, è possibile convertire ogni punto dati in Fahrenheit con la formula `Temperature_F = 9/5 * Temperature_C + 32`. Ogni volta AWS IoT SiteWise che riceve un punto dati nel flusso di `Temperature_C` misurazione, il `Temperature_F` valore corrispondente viene calcolato in pochi secondi e disponibile come `Temperature_F` proprietà.

Se la trasformazione contiene più di una variabile, il punto dati che arriva prima avvia immediatamente il calcolo. Consideriamo un esempio in cui un produttore di componenti utilizza una trasformazione per monitorare la qualità del prodotto. Utilizzando uno standard diverso in base al tipo di parte, il produttore utilizza le seguenti misurazioni per rappresentare il processo:

- `Part_Number`- Una stringa che identifica il tipo di parte.
- `Good_Count`- Un numero intero che aumenta di uno se la parte soddisfa lo standard.
- `Bad_Count`- Un numero intero che aumenta di uno se la parte non soddisfa lo standard.

Il produttore crea anche una trasformazione`Quality_Monitor`, che è uguale `if(eq(Part_Number, "BLT123") and (Bad_Count / (Good_Count + Bad_Count) > 0.1), "Caution", "Normal")` a.

Questa trasformazione monitora la percentuale di parti difettose prodotte per un tipo di parte specifico. Se il numero di parte è BLT123 e la percentuale di parti difettose supera il 10 percento (0,1), la trasformazione viene restituita. `"Caution"` In caso contrario, la trasformazione viene restituita. `"Normal"`

> **Note**
>
> - Se `Part_Number` riceve un nuovo punto dati prima di altre misurazioni, la `Quality_Monitor` trasformazione utilizza il nuovo `Part_Number` valore e i `Bad_Count` valori `Good_Count` e più recenti. Per evitare errori, `Good_Count` reimpostatelo `Bad_Count` prima del successivo ciclo di produzione.
> - Utilizzate le metriche se desiderate valutare le espressioni solo dopo che tutte le variabili hanno ricevuto nuovi punti dati.

Argomenti

- Definizione delle trasformazioni (console)
- Definizione delle trasformazioni ()AWS CLI

Definizione delle trasformazioni (console)

Quando definite una trasformazione per un modello di asset nella AWS IoT SiteWise console, specificate i seguenti parametri:

- Nome: il nome della proprietà.
- Unità — (Facoltativo) L'unità scientifica della proprietà, ad esempio mm o Celsius.
- Tipo di dati: il tipo di dati della trasformazione, che può essere Double o String.
- ID esterno: (Facoltativo) Si tratta di un ID definito dall'utente. Per ulteriori informazioni, consulta Riferimento a oggetti con ID esterni nella Guida per l'utente di AWS IoT SiteWise .
- Formula: l'espressione di trasformazione. Le espressioni di trasformazione non possono utilizzare funzioni di aggregazione o funzioni temporali. Per aprire la funzione di completamento automatico, inizia a digitare o premi il tasto freccia giù. Per ulteriori informazioni, consulta Utilizzo delle espressioni di formula.

> **Important**
>
> Le trasformazioni possono immettere proprietà di tipo intero, doppio, booleano o stringa. I booleani vengono convertiti in `0` (false) e (true). `1`
> Le trasformazioni devono inserire una o più proprietà che non sono attributi e un numero qualsiasi di proprietà degli attributi. AWS IoT SiteWise calcola un nuovo punto dati

trasformato ogni volta che la proprietà di input che non è un attributo riceve un nuovo punto dati. I nuovi valori degli attributi non avviano gli aggiornamenti delle trasformazioni. La stessa frequenza di richiesta per le operazioni API relative ai dati delle proprietà degli asset si applica ai risultati del calcolo delle trasformazioni.
Le espressioni delle formule possono generare solo valori doppi o stringhe. Le espressioni annidate possono generare altri tipi di dati, ad esempio stringhe, ma la formula nel suo insieme deve restituire un numero o una stringa. È possibile utilizzare la funzione jp per convertire una stringa in un numero. Il valore booleano deve essere 1 (vero) o 0 (falso). Per ulteriori informazioni, consulta Valori indefiniti, infiniti e di overflow.

Per ulteriori informazioni, consultare Creazione di un modello di asset (console).

Definizione delle trasformazioni ()AWS CLI

Quando definite una trasformazione per un modello di asset con l' AWS IoT SiteWise API, specificate i seguenti parametri:

- `name`— Il nome della proprietà.
- `unit`— (Facoltativo) L'unità scientifica della proprietà, ad esempio mm o Celsius.
- `dataType`— Il tipo di dati della trasformazione, che deve essere `DOUBLE` o`STRING`.
- `externalId`— (Facoltativo) Si tratta di un ID definito dall'utente. Per ulteriori informazioni, consulta Riferimento a oggetti con ID esterni nella Guida per l'utente di AWS IoT SiteWise .
- `expression`— L'espressione di trasformazione. Le espressioni di trasformazione non possono utilizzare funzioni di aggregazione o funzioni temporali. Per ulteriori informazioni, consulta Utilizzo delle espressioni di formula.
- `variables`— L'elenco di variabili che definisce le altre proprietà della risorsa da utilizzare nell'espressione. Ogni struttura di variabile contiene un nome semplice da utilizzare nell'espressione e una struttura `value` che specifica la proprietà da collegare alla variabile stessa. La struttura `value` contiene le seguenti informazioni:
  - `propertyId`— L'ID della proprietà da cui immettere i valori. È possibile utilizzare il nome della proprietà anziché il relativo ID.

> **Important**
>
> Le trasformazioni possono immettere proprietà di tipo intero, doppio, booleano o stringa. I booleani vengono convertiti in `0` (false) e (true). `1`

Le trasformazioni devono inserire una o più proprietà che non sono attributi e un numero qualsiasi di proprietà degli attributi. AWS IoT SiteWise calcola un nuovo punto dati trasformato ogni volta che la proprietà di input che non è un attributo riceve un nuovo punto dati. I nuovi valori degli attributi non avviano gli aggiornamenti delle trasformazioni. La stessa frequenza di richiesta per le operazioni API relative ai dati delle proprietà degli asset si applica ai risultati del calcolo delle trasformazioni.
Le espressioni delle formule possono generare solo valori doppi o stringhe. Le espressioni annidate possono generare altri tipi di dati, ad esempio stringhe, ma la formula nel suo insieme deve restituire un numero o una stringa. È possibile utilizzare la funzione jp per convertire una stringa in un numero. Il valore booleano deve essere 1 (vero) o 0 (falso). Per ulteriori informazioni, consulta Valori indefiniti, infiniti e di overflow.

Example definizione di trasformazione

Nell'esempio seguente viene illustrata una proprietà di trasformazione che converte i dati di misurazione della temperatura di un asset da Celsius a Fahrenheit. Questo oggetto è un esempio di un oggetto AssetModelPropertyche contiene un Transform. È possibile specificare questo oggetto come parte del payload della CreateAssetModelrichiesta per creare una proprietà di trasformazione. Per ulteriori informazioni, consulta Creazione di un modello di asset (AWS CLI).

```
{
...
"assetModelProperties": [
...
{
  "name": "Temperature F",
  "dataType": "DOUBLE",
  "type": {
    "transform": {
      "expression": "9/5 * temp_c + 32",
      "variables": [
        {
          "name": "temp_c",
          "value": {
            "propertyId": "Temperature C"
          }
        }
      ]
    }
```

```
  },
  "unit": "Fahrenheit"
}
],
...
}
```

Example definizione di trasformazione che contiene tre variabili

L'esempio seguente dimostra una proprietà di trasformazione che restituisce un messaggio di avviso (`"Caution"`) se più del 10 percento delle parti BLT123 non soddisfano lo standard. Altrimenti, restituisce un messaggio informativo (). `"Normal"`

```
{
...
"assetModelProperties": [
...
{
"name": "Quality_Monitor",
"dataType": "STRING",
"type": {
    "transform": {
        "expression": "if(eq(Part_Number,"BLT123") and (Bad_Count / (Good_Count +
 Bad_Count) > 0.1), "Caution", "Normal")",
        "variables": [
            {
                "name": "Part_Number",
                "value": {
                    "propertyId": "Part Number"
                }
            },
            {
                "name": "Good_Count",
                "value": {
                    "propertyId": "Good Count"
                }
            },
            {
                "name": "Bad_Count",
                "value": {
                    "propertyId": "Bad Count"
                }
            }
```

```
        ]
    }
}
}
...
}
```

Aggregazione di dati da proprietà e altre risorse (metriche)

Le metriche sono espressioni matematiche che utilizzano funzioni di aggregazione per elaborare tutti i punti dati di input e generare un singolo punto dati per intervallo di tempo specificato. Un parametro, ad esempio, può calcolare la temperatura oraria media da un flusso di dati di temperatura.

I parametri possono immettere dati dai parametri degli asset associati, in modo da poter calcolare le statistiche che forniscono informazioni dettagliate sull'operazione o su un sottoinsieme dell'operazione. Un parametro, ad esempio, può calcolare la temperatura oraria media di tutte le turbine eoliche di una centrale eolica. Per ulteriori informazioni su come definire le associazioni tra asset, consulta Definizione delle gerarchie dei modelli di asset.

Le metriche possono anche inserire dati da altre proprietà senza aggregare i dati su ogni intervallo di tempo. Se specifichi un attributo in una formula, AWS IoT SiteWise utilizza il valore più recente per quell'attributo quando calcola la formula. Se specifichi una metrica in una formula, AWS IoT SiteWise utilizza l'ultimo valore per l'intervallo di tempo in cui calcola la formula. Ciò significa che puoi definire metriche come `OEE = Availability * Quality * Performance` `AvailabilityQuality`, dove e `Performance` sono tutte le altre metriche sullo stesso modello di asset.

AWS IoT SiteWise inoltre, calcola automaticamente un set di metriche di aggregazione di base per tutte le proprietà degli asset. Per ridurre i costi di calcolo, puoi utilizzare questi aggregati anziché definire parametri personalizzati per i calcoli di base. Per ulteriori informazioni, consulta Esecuzione di query sugli aggregati delle proprietà di asset.

Argomenti

- Definizione dei parametri (console)
- Definizione delle metriche ()AWS CLI

Definizione dei parametri (console)

Quando si definisce una metrica per un modello di asset nella AWS IoT SiteWise console, si specificano i seguenti parametri:

- Nome: il nome della proprietà.
- Tipo di dati: il tipo di dati della trasformazione, che può essere Double o String.
- ID esterno: (Facoltativo) Si tratta di un ID definito dall'utente. Per ulteriori informazioni, consulta Riferimento a oggetti con ID esterni nella Guida per l'utente di AWS IoT SiteWise .
- Formula: l'espressione metrica. Le espressioni metriche possono utilizzare funzioni di aggregazione per immettere dati da una proprietà per tutte le risorse associate in una gerarchia. Inizia a digitare o premi il tasto freccia giù per aprire la funzione di completamento automatico. Per ulteriori informazioni, consulta Utilizzo delle espressioni di formula.

  > **Important**
  >
  > Le metriche possono essere solo proprietà di tipo intero, doppio, booleano o stringa. I valori booleani vengono convertiti in `0` (false) e (true). 1
  > Le variabili di input in una espressione parametrica devono presentare lo stesso intervallo di tempo del parametro di output.
  > Le espressioni delle formule possono generare solo valori doppi o stringhe. Le espressioni annidate possono generare altri tipi di dati, ad esempio stringhe, ma la formula nel suo insieme deve restituire un numero o una stringa. È possibile utilizzare la funzione jp per convertire una stringa in un numero. Il valore booleano deve essere 1 (vero) o 0 (falso). Per ulteriori informazioni, consulta Valori indefiniti, infiniti e di overflow.

- Intervallo di tempo: l'intervallo di tempo metrico. AWS IoT SiteWise supporta i seguenti intervalli di tempo a finestra rotante, in cui ogni intervallo inizia alla fine di quello precedente:
  - da 1 minuto a 1 minuto, calcolato alla fine di ogni minuto (00:00:00, 00:01:00, 12:02:00 e così via).
  - Da 5 minuti a 5 minuti, calcolati alla fine di ogni cinque minuti a partire dall'ora (00:00:00, 12:05:00, 00:10:00 e così via).
  - da 15 minuti a 15 minuti, calcolati alla fine di ogni quindici minuti a partire dall'ora (00:00:00, 12:15:00, 00:30:00 e così via).
  - da 1 ora a 1 ora (60 minuti), calcolata alla fine di ogni ora in formato UTC (00:00:00, 01:00:00, 02:00:00 e così via).
  - 1 giorno — 1 giorno (24 ore), calcolato alla fine di ogni giornata in UTC (00:00 di lunedì, 00:00 di martedì e così via).
  - da 1 settimana a 1 settimana (7 giorni), calcolata alla fine di ogni domenica in UTC (ogni lunedì alle 00:00).

  - Intervallo personalizzato: puoi inserire qualsiasi intervallo di tempo compreso tra un minuto e una settimana.
- Data di offset: (Facoltativa) La data di riferimento a partire dalla quale aggregare i dati.
- Tempo di offset: (Facoltativo) L'ora di riferimento a partire dalla quale aggregare i dati. L'ora di offset deve essere compresa tra 00:00:00 e 23:59:59.
- Fuso orario di offset - (Facoltativo) Il fuso orario per l'offset. Se non è specificato, il fuso orario di offset predefinito è l'Universal Coordinated Time (UTC).

Fusi orari supportati

  - (UTC+ 00:00) Universal Coordinated Time
  - (UTC+ 01:00) Ora centrale europea
  - (UTC+ 02:00) Europa orientale
  - (UTC03+:00) Ora dell'Africa orientale
  - (UTC+ 04:00) Ora del Vicino Oriente
  - (UTC+ 05:00) Ora del Pakistan di Lahore
  - (UTC+ 05:30) Ora solare dell'India
  - (UTC+ 06:00) Ora solare del Bangladesh
  - (UTC+ 07:00) Ora solare del Vietnam
  -
  - (UTC+ 09:00) Ora solare del Giappone
  - (UTC+ 09:30) Ora centrale dell'Australia
  - (UTC+ 10:00) Ora orientale dell'Australia
  - (UTC+ 11:00) Ora solare delle Salomone
  - (UTC+ 12:00) Ora solare della Nuova Zelanda
  - (UTC- 11:00) Ora delle Isole Midway
  - (UTC- 10:00) Ora solare delle Hawaii
  - (UTC- 09:00) Ora solare dell'Alaska
  - (UTC- 08:00) Ora solare del Pacifico
  - (UTC- 07:00) Ora solare di Phoenix
  - (UTC- 06:00) Ora solare centrale
  - (UTC- 05:00) Ora solare orientale

- (UTC- 04:00) Ora di Porto Rico e Isole Vergini Americane
- (UTC- 03:00) Ora solare dell'Argentina
- (UTC- 02:00) Ora della Georgia del Sud
- (UTC- 01:00) Ora dell'Africa centrale

Example intervallo di tempo personalizzato con un offset (console)

L'esempio seguente mostra come definire un intervallo di tempo di 12 ore con un offset il 20 febbraio 2021 alle 18:30:30 (PST).

Per definire un intervallo personalizzato con un offset

1. Per Intervallo di tempo, scegliete Intervallo personalizzato.
2. Per Intervallo di tempo, effettuate una delle seguenti operazioni:
   - Immettete**`12`**, quindi scegliete le ore.
   - Inserisci**`720`**, quindi scegli minuti.
   - Inserisci**`43200`**, quindi scegli secondi.

   > **Important**
   > L'intervallo di tempo deve essere un numero intero indipendentemente dall'unità.

3. Per la data di offset, scegli 20/02/2021.
4. Per Tempo di offset, immettete. **`18:30:30`**
5. Per il fuso orario di Offset, scegliete (UTC- 08:00) Pacific Standard Time.

Se crei la metrica il 1° luglio 2021, prima o alle 18:30:30 (PST), otterrai il primo risultato di aggregazione il 1° luglio 2021 alle 18:30:30 (PST). Il secondo risultato di aggregazione è il 2 luglio 2021 alle 06:30:30 (PST) e così via.

Definizione delle metriche ()AWS CLI

Quando definite una metrica per un modello di asset con l' AWS IoT SiteWise API, specificate i seguenti parametri:

- `name`— Il nome della proprietà.
- `dataType`— Il tipo di dati della metrica, che può essere `DOUBLE` o`STRING`.
- `externalId`— (Facoltativo) Si tratta di un ID definito dall'utente. Per ulteriori informazioni, consulta Riferimento a oggetti con ID esterni nella Guida per l'utente di AWS IoT SiteWise .
- `expression`— L'espressione metrica. Le espressioni metriche possono utilizzare funzioni di aggregazione per immettere dati da una proprietà per tutte le risorse associate in una gerarchia. Per ulteriori informazioni, consulta Utilizzo delle espressioni di formula.
- `window`— L'intervallo di tempo e l'offset della finestra di rotazione della metrica, in cui ogni intervallo inizia quando termina quello precedente:
  - `interval`— L'intervallo di tempo per la finestra di rotazione. L'intervallo di tempo deve essere compreso tra un minuto e una settimana.
  - `offsets`— L'offset della finestra ribaltabile.

  Per ulteriori informazioni, consulta l'AWS IoT SiteWise API TumblingWindowReference.

  Example intervallo di tempo personalizzato con un offset ()AWS CLI

  L'esempio seguente mostra come definire un intervallo di tempo di 12 ore con un offset il 20 febbraio 2021 alle 18:30:30 (PST).

  ```
  {
      "window": {
          "tumbling": {
              "interval": "12h",
              "offset": " 2021-07-23T18:30:30-08"
          }
      }
  }
  ```

  Se crei la metrica il 1° luglio 2021, prima o alle 18:30:30 (PST), otterrai il primo risultato di aggregazione il 1° luglio 2021 alle 18:30:30 (PST). Il secondo risultato di aggregazione è il 2 luglio 2021 alle 06:30:30 (PST) e così via.
- `variables`— L'elenco di variabili che definisce le altre proprietà della risorsa o delle risorse secondarie da utilizzare nell'espressione. Ogni struttura di variabile contiene un nome semplice da utilizzare nell'espressione e una struttura `value` che specifica la proprietà da collegare alla variabile stessa. La struttura `value` contiene le seguenti informazioni:

- `propertyId`— L'ID della proprietà da cui estrarre i valori. È possibile utilizzare il nome della proprietà anziché il relativo ID se la proprietà è definita nel modello corrente (anziché definita in un modello da una gerarchia).
- `hierarchyId`— (Facoltativo) L'ID della gerarchia da cui interrogare gli asset secondari per la proprietà. È possibile utilizzare il nome della definizione della gerarchia anziché il relativo ID. Se omettete questo valore, AWS IoT SiteWise trova la proprietà nel modello corrente.

> **Important**
>
> Le metriche possono essere solo proprietà di tipo intero, doppio, booleano o stringa. I valori booleani vengono convertiti in `0` (false) e (true). `1`
> Le variabili di input in una espressione parametrica devono presentare lo stesso intervallo di tempo del parametro di output.
> Le espressioni delle formule possono generare solo valori doppi o stringhe. Le espressioni annidate possono generare altri tipi di dati, ad esempio stringhe, ma la formula nel suo insieme deve restituire un numero o una stringa. È possibile utilizzare la funzione jp per convertire una stringa in un numero. Il valore booleano deve essere 1 (vero) o 0 (falso). Per ulteriori informazioni, consulta Valori indefiniti, infiniti e di overflow.

- `unit`— (Facoltativo) L'unità scientifica della proprietà, ad esempio mm o Celsius.

Example Definizione del parametro di esempio

Nell'esempio seguente viene illustrata una proprietà parametro che aggrega i dati di misurazione della temperatura di un asset per calcolare la temperatura oraria massima in Fahrenheit. Questo oggetto è un esempio di un AssetModelPropertyche contiene una metrica. È possibile specificare questo oggetto come parte del payload della CreateAssetModelrichiesta per creare una proprietà metrica. Per ulteriori informazioni, consulta Creazione di un modello di asset (AWS CLI).

```
{
      ...
      "assetModelProperties": [
      ...
      {
        "name": "Max temperature",
        "dataType": "DOUBLE",
        "type": {
```

```
          "metric": {
            "expression": "max(temp_f)",
            "variables": [
              {
                "name": "temp_f",
                "value": {
                  "propertyId": "Temperature F"
                }
              }
            ],
            "window": {
              "tumbling": {
                "interval": "1h"
              }
            }
          }
        },
        "unit": "Fahrenheit"
      }
    ],
    ...
}
```

Example Esempio di definizione della metrica che immette i dati dagli asset associati

L'esempio seguente mostra una proprietà metrica che aggrega i dati sulla potenza media di più turbine eoliche per calcolare la potenza media totale di un parco eolico. Questo oggetto è un esempio di un oggetto che contiene una metrica AssetModelProperty. È possibile specificare questo oggetto come parte del payload della CreateAssetModelrichiesta per creare una proprietà metrica.

```
{
      ...
      "assetModelProperties": [
      ...
      {
          "name": "Total Average Power",
          "dataType": "DOUBLE",
          "type": {
            "metric": {
              "expression": "avg(power)",
              "variables": [
                {
                  "name": "power",
```

```
                  "value": {
                    "propertyId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
                    "hierarchyId": "Turbine Asset Model"
                  }
                }
              ],
              "window": {
                "tumbling": {
                  "interval": "5m"
                }
              }
            }
        },
        "unit": "kWh"
      }
    ],
    ...
}
```

Utilizzo delle espressioni di formula

Con le espressioni di formula, è possibile definire le funzioni matematiche per trasformare e aggregare i dati industriali grezzi e ottenere informazioni dettagliate sulla propria operazione. Le espressioni di formule combinano valori letterali, operatori, funzioni e variabili per elaborare i dati. Per ulteriori informazioni su come definire le proprietà degli asset che utilizzano espressioni di formule, consulta Trasformazione dei dati (trasformazioni) eAggregazione di dati da proprietà e altre risorse (metriche). Le trasformazioni e le metriche sono proprietà delle formule.

Argomenti

- Utilizzo di variabili nelle espressioni delle formule
- Utilizzo di valori letterali nelle espressioni delle formule
- Utilizzo degli operatori nelle espressioni delle formule
- Utilizzo delle costanti nelle espressioni delle formule
- Utilizzo delle funzioni nelle espressioni delle formule
- Tutorial sulle espressioni di formule

Utilizzo di variabili nelle espressioni delle formule

Le variabili rappresentano le proprietà AWS IoT SiteWise degli asset nelle espressioni delle formule. Utilizzate le variabili per inserire valori da altre proprietà degli asset nelle espressioni, in modo da poter elaborare i dati provenienti da proprietà costanti (attributi), flussi di dati non elaborati (misurazioni) e altre proprietà delle formule.

Le variabili possono rappresentare le proprietà degli asset dello stesso modello di asset o dei modelli di asset secondari associati. Solo le formule metriche possono inserire variabili da modelli di asset secondari.

Le variabili vengono identificate con nomi diversi nella console e nell'API.

- AWS IoT SiteWise console: utilizza i nomi delle proprietà degli asset come variabili nelle espressioni.
- AWS IoT SiteWise API (AWS CLI, AWS SDK): definisci le variabili con la ExpressionVariablestruttura, che richiede un nome di variabile e un riferimento a una proprietà dell'asset. Il nome della variabile può contenere lettere minuscole, numeri e caratteri di sottolineatura. Quindi, utilizzate i nomi delle variabili per fare riferimento alle proprietà delle risorse nelle espressioni.

I nomi delle variabili distinguono tra maiuscole e minuscole

Per ulteriori informazioni, consulta Definizione delle trasformazioni e Definizione delle metriche.

Utilizzo delle variabili per fare riferimento alle proprietà

Il valore di una variabile definisce la proprietà a cui fa riferimento. AWS IoT SiteWise offre diversi modi per eseguire questa operazione.

- Per ID della proprietà: è possibile specificare l'ID univoco della proprietà (UUID) per identificarla.
- Per nome: se la proprietà appartiene allo stesso modello di asset, è possibile specificarne il nome nel campo ID della proprietà.
- Per percorso: un valore variabile può fare riferimento a una proprietà tramite il relativo percorso. Per ulteriori informazioni, consulta Utilizzo di percorsi per fare riferimento alle proprietà personalizzate del modello composito.

> **Note**
>
> Le variabili non sono supportate dalla AWS IoT SiteWise console. Vengono utilizzate dall' AWS IoT SiteWise API, incluso il AWS Command Line Interface AWS CLI() e dagli AWS SDK.

Una variabile ricevuta in una risposta da AWS IoT SiteWise include informazioni complete sul valore, inclusi l'ID e il percorso.

Tuttavia, quando si passa una variabile a AWS IoT SiteWise (ad esempio, in una chiamata «crea» o «aggiorna»), è sufficiente specificare solo una di queste. Ad esempio, se si specifica il percorso, non è necessario fornire l'ID.

Utilizzo di valori letterali nelle espressioni delle formule

È possibile definire numeri e stringhe letterali nelle espressioni delle formule.

- Numeri

  Usa numeri e notazione scientifica per definire numeri interi e doppi. È possibile utilizzare la notazione E per esprimere numeri con notazione scientifica.

  Esempi:`1`,`,2.0`,`,.9`, `-23.1` `7.89e3` `3.4E-5`

- Stringhe

  Usa i caratteri `'` (virgolette) e `"` (virgolette doppie) per definire le stringhe. Il tipo di citazione per l'inizio e la fine devono corrispondere. Per evitare una virgoletta che corrisponde a quella utilizzata per dichiarare una stringa, includi quella virgoletta due volte. Questo è l'unico carattere di escape nelle AWS IoT SiteWise stringhe.

  Esempi: `'active'`, `"inactive"`, `'{"temp": 52}'`, `"{""temp"": ""high""}"`

Utilizzo degli operatori nelle espressioni delle formule

È possibile utilizzare i seguenti operatori comuni nelle espressioni di formule.

Operatore	Descrizione
+	Se entrambi gli operandi sono numeri, questo operatore aggiunge gli operandi sinistro e destro. Se uno degli operandi è una stringa, questo operatore concatena gli operandi sinistro e destro come stringhe. Ad esempio, l'espress ione restituisce. `1 + 2 + " is three"` `"3 is three"` La stringa concatenata può contenere fino a 1024 caratteri. Se la stringa supera i 1024 caratteri, AWS IoT SiteWise non restituisce un punto dati per quel calcolo.
-	Sottrae l'operando destro dall'operando sinistro. È possibile utilizzare questo operatore solo con operandi numerici.
/	Divide l'operando sinistro per l'operando destro. È possibile utilizzare questo operatore solo con operandi numerici.
*	Moltiplica gli operandi sinistro e destro. È possibile utilizzare questo operatore solo con operandi numerici.
^	Solleva l'operando di sinistra alla potenza dell'operando destro (esponenziazione). È possibile utilizzare questo operatore solo con operandi numerici.
%	Restituisce il resto della divisione dell'oper ando sinistro per l'operando destro. Il segno del risultato è identico a quello dell'operando

Operatore	Descrizione
	sinistro. Questo comportamento è diverso dall'operazione del modulo. È possibile utilizzare questo operatore solo con operandi numerici.
`x < y`	Restituisce 1 se x è minore diy, altrimenti. `0`
`x > y`	Restituisce 1 se x è maggiore diy, altrimenti`0`.
`x <= y`	Restituisce 1 se x è minore o uguale ay, altrimenti`0`.
`x >= y`	Restituisce 1 se x è maggiore o uguale ay, altrimenti`0`.
`x == y`	Restituisce 1 se x è uguale ay, altrimenti`0`.
`x != y`	Restituisce 1 se non x è uguale ay, altrimenti`0`.
`!x`	Restituisce 1 se x viene valutato come `0` (falso), altrimenti`0`. xviene valutato falso se: • xè un operando numerico e viene valutato in. `0` • xviene valutato in una stringa vuota. • xviene valutato in un array vuoto. • xviene valutato in. `None`

Operatore	Descrizione
`x and y`	Restituisce `0` se `x` viene valutato come `0` (false). Altrimenti, restituisce il risultato valutato di. `y` `x`o `y` viene valutato falso se: • `x`or `y` è un operando numerico e viene valutato come. `0` • `x`o `y` viene valutato in una stringa vuota. • `x`o `y` viene valutato in una matrice vuota. • `x`o `y` viene valutato in. `None`
`x or y`	Restituisce 1 se `x` viene valutato come 1 (true). Altrimenti, restituisce il risultato valutato di. `y` `x`o `y` viene valutato falso se: • `x`or `y` è un operando numerico e viene valutato come. `0` • `x`o `y` viene valutato in una stringa vuota. • `x`o `y` viene valutato in una matrice vuota. • `x`o `y` viene valutato in. `None`
`not x`	Restituisce 1 se `x` viene valutato come `0` (false), altrimenti. `0` `x`viene valutato falso se: • `x`è un operando numerico e viene valutato in. `0` • `x`viene valutato in una stringa vuota. • `x`viene valutato in un array vuoto. • `x`viene valutato in. `None`

Operatore	Descrizione

`[]`
 	
`s[index]`
	Restituisce il carattere in corrispondenza di un indice `index` della stringa`s`. È equivalente alla sintassi dell'indice in Python.
	
	Example Esempi
	
	• `"Hello!"[1]` restituisce `e`.
	• `"Hello!"[-2]` restituisce `o`.

Operatore	Descrizione

`[]`
 	
`s[start:end:step]`
	Restituisce una parte della stringa. `s` È equivalente alla sintassi slice in Python. Questo operatore ha i seguenti argomenti:
	
	• `start`— (Facoltativo) L'indice iniziale inclusivo della fetta. L'impostazione predefinita è `0`.
	• `end`— (Facoltativo) L'indice finale esclusivo della fetta. Il valore predefinito è la lunghezza della stringa.
	• `step`— (Facoltativo) Il numero da incrementare per ogni passaggio della fetta. Ad esempio, potete specificare di `2` restituire una sezione con ogni altro carattere o specificare di `-1` invertire la sezione. L'impostazione predefinita è `1`.
	
	È possibile omettere l'`step`argomento per utilizzarne il valore predefinito. Ad esempio, `s[1:4:1]` è uguale a `s[1:4]`.
	
	Gli argomenti devono essere numeri interi o la costante none. Se si specificanone, AWS IoT SiteWise utilizza il valore predefinito per quell'argomento.
	
	Example Esempi
	
	• `"Hello!"[1:4]` restituisce `"ell"`.
	• `"Hello!"[:2]` restituisce `"He"`.
	• `"Hello!"[3:]` restituisce `"lo!"`.
	• `"Hello!"[:-4]` restituisce `"He"`.
	• `"Hello!"[::2]` restituisce `"Hlo"`.
	• `"Hello!"[::-1]` restituisce `"!olleH"`.

Utilizzo delle costanti nelle espressioni delle formule

È possibile utilizzare le seguenti costanti matematiche comuni nelle espressioni. Tutte le costanti non fanno distinzione tra maiuscole e minuscole.

> **Note**
>
> Se si definisce una variabile con lo stesso nome di una costante, la variabile sostituisce la costante.

Costante	Descrizione
`pi`	Il numero pi ()π: `3.141592653589793`
`e`	Il numero e: `2.718281828459045`
`true`	Equivalente al numero 1. Nel AWS IoT SiteWise, i booleani si convertono nei loro equivalenti numerici.
`false`	Equivalente al numero 0. In AWS IoT SiteWise, i booleani vengono convertiti nei loro equivalenti numerici.
`none`	Equivalente a nessun valore. È possibile utilizzare questa costante per non restituire nulla come risultato di un'espressione condizionale.

Utilizzo delle funzioni nelle espressioni delle formule

È possibile utilizzare le seguenti funzioni per operare sui dati nelle espressioni delle formule.

Le trasformazioni e le metriche supportano diverse funzioni. La tabella seguente indica quali tipi di funzioni sono compatibili con ogni tipo di proprietà della formula.

> **Note**
>
> È possibile includere un massimo di 10 funzioni in un'espressione di formula.

Tipo di funzione	Trasformazioni	Metriche
Utilizzo di funzioni comuni nelle espressioni delle formule	 Sì	 Sì
Utilizzo delle funzioni di confronto nelle espressioni delle formule	 Sì	 Sì
Utilizzo di funzioni condizionali nelle espressioni delle formule	 Sì	 Sì
Utilizzo di funzioni di stringa nelle espressioni di formule	 Sì	 Sì
Utilizzo delle funzioni di aggregazione nelle espressioni di formule	 No	 Sì
Utilizzo di funzioni temporali nelle espressioni delle formule	 Sì	 Sì

Tipo di funzione	Trasformazioni	Metriche
Utilizzo delle funzioni di data e ora nelle espressioni di formule	 Sì	 Sì

Sintassi della funzione

È possibile utilizzare la seguente sintassi per creare funzioni:

Sintassi regolare

Con la sintassi normale, il nome della funzione è seguito da parentesi con zero o più argomenti.

`function_name``(`*`argument1, argument2, argument3, ...`*`)`. Ad esempio, le funzioni con la sintassi normale potrebbero essere simili a `log(x)` `econtains(s, substring)`.

Sintassi uniforme delle chiamate di funzione (UFCS)

UFCS consente di chiamare funzioni utilizzando la sintassi per le chiamate di metodo nella programmazione orientata agli oggetti. Con UFCS, il primo argomento è seguito da dot (`.`), quindi dal nome della funzione e dagli argomenti rimanenti (se presenti) tra parentesi.

`argument1``.`*`function_name`*`(`*`argument2, argument3, ...`*`)`. Ad esempio, le funzioni con UFCS potrebbero essere simili `x.log()` a e. `s.contains(substring)`

È inoltre possibile utilizzare UFCS per concatenare le funzioni successive. AWS IoT SiteWise utilizza il risultato della valutazione della funzione corrente come primo argomento per la funzione successiva.

Ad esempio, è possibile utilizzare `message.jp('$.status').lower().contains('fail')` invece di`contains(lower(jp(message, '$.status')),'fail')`.

Per ulteriori informazioni, visita il sito Web del linguaggio di programmazione D.

> **Note**
>
> È possibile utilizzare UFCS per tutte le AWS IoT SiteWise funzioni.

AWS IoT SiteWise le funzioni non distinguono tra maiuscole e minuscole. Ad esempio, è possibile utilizzare `lower(s)` e in modo `Lower(s)` intercambiabile.

Utilizzo di funzioni comuni nelle espressioni delle formule

Nelle trasformazioni e nelle metriche, è possibile utilizzare le seguenti funzioni per calcolare le funzioni matematiche comuni nelle trasformazioni e nelle metriche.

Funzione	Descrizione
`abs(x)`	Restituisce il valore assoluto di `x`.
`acos(x)`	Restituisce l'arccoseno di `x`.
`asin(x)`	Restituisce l'arcsine di `x`.
`atan(x)`	Restituisce l'arctangente di `x`.
`cbrt(x)`	Restituisce la radice cubica di `x`.
`ceil(x)`	Restituisce il numero intero più vicino maggiore di `x`.
`cos(x)`	Restituisce il coseno di `x`.
`cosh(x)`	Restituisce il coseno iperbolico di `x`.
`cot(x)`	Restituisce la cotangente di. `x`
`exp(x)`	Restituisce e al potere di `x`.
`expm1(x)`	Restituisce `exp(x) - 1`. Utilizzate questa funzione `exp(x) - 1` per calcolare con maggiore precisione valori piccoli di. `x`
`floor(x)`	Restituisce il numero intero più vicino inferiore a `x`.
`log(x)`	Restituisce $\log_e$ (base e) di `x`.

Funzione	Descrizione
`log10(x)`	Restituisce $\log_{10}$ (base 10) di `x`.
`log1p(x)`	Restituisce `log(1 + x)`. Utilizzare questa funzione `log(1 + x)` per calcolare con maggiore precisione valori piccoli di`x`.
`log2(x)`	Restituisce $\log_2$ (base 2) di `x`.
`pow(x, y)`	Restituisce `x` al potere di `y`. Questo è equivalen te a`x ^ y`.
`signum(x)`	Restituisce il segno di `x` (`-1` per input negativi, `0` per input pari a zero, `+1` per input positivi).
`sin(x)`	Restituisce il seno di `x`.
`sinh(x)`	Restituisce il seno iperbolico di `x`.
`sqrt(x)`	Restituisce la radice quadrata di `x`.
`tan(x)`	Restituisce la tangente di `x`.
`tanh(x)`	Restituisce la tangente iperbolica di `x`.

Utilizzo delle funzioni di confronto nelle espressioni delle formule

Nelle trasformazioni e nelle metriche, è possibile utilizzare le seguenti funzioni di confronto per confrontare due valori e ottenere un risultato `1` (vero) o `0` (falso). AWS IoT SiteWise confronta le stringhe in base all'ordine lessicografico.

Funzione	Descrizione
`gt(x, y)`	Restituisce `1` se `x` è maggiore di `y`, altrimenti `0` (`x > y`).

Funzione	Descrizione
	Questa funzione non restituisce un valore se x e y sono tipi incompatibili, come un numero e una stringa.
`gte(x, y)`	Restituisce 1 se x è maggiore o uguale a y, altrimenti `0` (`x ≥ y`). AWS IoT SiteWise considera gli argomenti uguali se rientrano in una tolleranza relativa di`1E-9`. Si comporta in modo simile alla funzione isclose in Python. Questa funzione non restituisce un valore se x e y sono tipi incompatibili, come un numero e una stringa.
`eq(x, y)`	Restituisce 1 se x è uguale a y, altrimenti `0` (`x == y`). AWS IoT SiteWise considera gli argomenti uguali se rientrano in una tolleranza relativa di`1E-9`. Si comporta in modo simile alla funzione isclose in Python. Questa funzione non restituisce un valore se x e y sono tipi incompatibili, come un numero e una stringa.
`lt(x, y)`	Restituisce 1 se x è inferiore a y, altrimenti `0` (`x < y`). Questa funzione non restituisce un valore se x e y sono tipi incompatibili, come un numero e una stringa.

Funzione	Descrizione
`lte(x, y)`	Restituisce 1 se x è minore o uguale a y, altrimenti `0` (`x ≤ y`). AWS IoT SiteWise considera gli argomenti uguali se rientrano in una tolleranza relativa di`1E-9`. Si comporta in modo simile alla funzione isclose in Python. Questa funzione non restituisce un valore se x e y sono tipi incompatibili, come un numero e una stringa.
`isnan(x)`	Restituisce 1 se x è uguale a`NaN`, altrimenti`0`. Questa funzione non restituisce un valore se x è una stringa.

Utilizzo di funzioni condizionali nelle espressioni delle formule

Nelle trasformazioni e nelle metriche, è possibile utilizzare la seguente funzione per verificare una condizione e restituire risultati diversi, indipendentemente dal fatto che la condizione restituisca vero o falso.

Funzione	Descrizione
`if(condition, result_if_true, result_if_false)`	Valuta `condition` e restituisce `result_if_true` se la condizione restituisce vero o `result_if_false` se la condizione restituisce. `false` `condition` deve essere un numero. Questa funzione considera `0` una stringa vuota come `false` e tutto il resto (incluso`NaN`) come`true`. I booleani vengono convertiti in `0` (false) e `1` (true).

Funzione	Descrizione
	È possibile restituire la costante none da questa funzione per scartare l'output per una particolare condizione. Ciò significa che puoi filtrare i punti dati che non soddisfano una condizione. Per ulteriori informazioni, consulta Filtraggio dei punti dati. Example Esempi • `if(0, x, y)`restituisce la variabiley. • `if(5, x, y)`restituisce la variabilex. • `if(gt(temp, 300), x, y)` restituisce la variabile `x` se la variabile `temp` è maggiore di`300`. • `if(gt(temp, 300), temp, none)`restituisce la variabile `temp` se è maggiore o uguale a`300`, oppure `none` (nessun valore) se `temp` è minore di`300`. Si consiglia di utilizzare UFCS per funzioni condizionali annidate in cui uno o più argomenti sono funzioni condizionali. È possibile utilizzar e `if(condition, result_if_true)` per valutare una condizione e `elif(cond ition, result_if_true, result_if _false)` valutare condizioni aggiuntive. Ad esempio, puoi usare `if(condition1, result1_if_true).elif(condi tion2, result2_if_true, result2_i f_false)` invece di`if(condition1, result1_if_true, if(condit ion2, result2_if_true, result2_i f_false))` .

Funzione	Descrizione
	È inoltre possibile concatenare funzioni condizionali intermedie aggiuntive. Ad esempio, è possibile utilizzare, `if(condition1, result1_if_true).elif(condition2, result2_if_true).elif(condition3, result3_if_true, result3_if_false)` anziché annidare, più `if` istruzioni, ad esempio. `if(condition1, result1_if_true, if(condition2, result2_if_true, if(condition3, result3_if_true result3_if_false)))` **Important** È necessario utilizzare `elif(condition, result_if_true, result_if_false)` con UFCS.

Utilizzo di funzioni di stringa nelle espressioni di formule

Nelle trasformazioni e nelle metriche, è possibile utilizzare le seguenti funzioni per operare sulle stringhe. Per ulteriori informazioni, consulta Usare le stringhe nelle formule.

Important

Le espressioni di formule possono generare solo valori doppi o stringhe. Le espressioni annidate possono generare altri tipi di dati, ad esempio stringhe, ma la formula nel suo insieme deve restituire un numero o una stringa. È possibile utilizzare la funzione jp per convertire una stringa in un numero. Il valore booleano deve essere 1 (vero) o 0 (falso). Per ulteriori informazioni, consulta Valori indefiniti, infiniti e di overflow.

Funzione	Descrizione
`len(s)`	Restituisce la lunghezza della stringa. `s`
`find(s, substring)`	Restituisce l'indice della stringa `substring` nella stringa`s`.
`contains(s, substring)`	Restituisce 1 se la stringa `s` contiene la stringa`substring` , altrimenti`0`.
`upper(s)`	Restituisce la stringa `s` in formato maiuscolo.
`lower(s)`	Restituisce la stringa `s` in formato minuscolo.
`jp(s, json_path)`	Valuta la stringa `s` con l'JsonPathespressione `json_path` e restituisce il risultato. Utilizzate questa funzione per effettuare le seguenti operazioni: • Estrai un valore, un array o un oggetto da una struttura JSON serializzata. • Converte una stringa in un numero. Ad esempio, la formula viene `jp('111', '$')` restituita 111 come numero. Per estrarre un valore di stringa da una struttura JSON e restituirlo come numero, è necessario utilizzare più funzioni annidate`jp`. La `jp` funzione esterna estrae la stringa dalla struttura JSON e la `jp` funzione interna converte la stringa in un numero. La stringa `json_path` deve contenere una stringa letterale. Ciò significa che non `json_path` può essere un'espressione che restituisce una stringa.

Funzione	Descrizione
	Example Esempi • `jp('{"status":"active","value":15}', '$.value')` restituisce 15. • `jp('{"measurement":{"reading":25,"confidence":0.95}}', '$.measurement.reading')` restituisce 25. • `jp('[2,8,23]', '$[2]')` restituisce 23. • `jp('{"values":[3,6,7]}', '$.values[1]')` restituisce 6. • `jp('111', '$')` restituisce 111. • `jp(jp('{"measurement":{"reading":25,"confidence":"0.95"}}', '$.measurement.confidence'), '$')` restituisce `0.95`.
`join(s0, s1, s2, s3, ...)`	Restituisce una stringa concatenata con un delimitatore. Questa funzione utilizza la prima stringa di input come delimitatore e unisce le stringhe di input rimanenti. Si comporta in modo simile alla funzione join (CharSequence delimiter, CharSequence... elements) in Java. Example Esempi • `join("-", "aa", "bb", "cc")`restituisce `aa-bb-cc`

Funzione	Descrizione
`format(expression: "format")` o `format("format", expression)`	Restituisce una stringa nel formato specificato. Questa funzione restituisce `expression` un valore e quindi restituisce il valore nel formato specificato. Si comporta in modo simile alla funzione format (String format, Object... args) in Java. Per ulteriori informazioni sui formati supportati, consulta Conversioni in Class Formatter nella piattaforma Java, Specifiche dell'API Standard Edition 7. Example Esempi • `format(100+1: "d")` restituisce una stringa,. `101` • `format("The result is %d", 100+1)`restituisce una stringa,`The result is 101`.

Funzione	Descrizione
`f'expression'`	Restituisce una stringa concatenata. Con questa funzione formattata, è possibile utilizzar e un'espressione semplice per concatenare e formattare stringhe. Queste funzioni possono contenere espressioni annidate. È possibile utilizzare `{}` (parentesi graffe arricciate) per interpolare le espressioni. Si comporta in modo simile alle stringhe letterali formattate in Python. Example Esempi • `f'abc{1+2: "f"}d'` restituisce `abc3.000000d` . Per valutare questa espressione di esempio, procedi come segue: 1. `format(1+2: "f")` restituisce un numero in virgola mobile,`3.000000`. 2. `join('', "abc", 1+2, 'd')`restituis ce una stringa,`abc3.000000d` . Puoi anche scrivere l'espressione nel modo seguente:`join('', "abc", format(1+ 2: "f"), 'd')` .

Utilizzo delle funzioni di aggregazione nelle espressioni di formule

Solo nelle metriche, puoi utilizzare le seguenti funzioni che aggregano i valori di input in ogni intervallo di tempo e calcolano un singolo valore di output. Le funzioni di aggregazione possono aggregare i dati dagli asset associati.

Gli argomenti delle funzioni di aggregazione possono essere variabili, numeri letterali, funzioni temporali, espressioni annidate o funzioni di aggregazione. La formula `max(latest(x), latest(y), latest(z))` utilizza una funzione di aggregazione come argomento e restituisce il valore corrente massimo delle proprietà, e. `x` `y` `z`

È possibile utilizzare espressioni annidate nelle funzioni di aggregazione. Quando si utilizzano espressioni nidificate, si applicano le seguenti regole:

- Ogni argomento può avere una sola variabile.

  Example

  Ad esempio, `avg(x*(x-1))` e `sum(x/2 )/avg(y^2 )` sono supportati.

  Ad esempio, `min(x/y)` non è supportato.
- Ogni argomento può avere espressioni annidate a più livelli.

  Example

  Ad esempio, `sum(avg(x^2 )/2)` è supportato.
- Argomenti diversi possono avere variabili diverse.

  Example

  Ad esempio, `sum(x/2, y*2)` è supportato.

> **Note**
>
> - Se le espressioni contengono misurazioni, AWS IoT SiteWise utilizza gli ultimi valori dell'intervallo di tempo corrente per le misurazioni per calcolare gli aggregati.
> - Se le espressioni contengono attributi, AWS IoT SiteWise utilizza i valori più recenti per gli attributi per calcolare gli aggregati.

Funzione	Descrizione
`avg(`x_0`, ..., `x_n`)`	Restituisce la media dei valori delle variabili date nell'intervallo di tempo specificato. Questa funzione emette un punto dati solo se le variabili specificate hanno almeno un punto dati nell'intervallo di tempo corrente.

Funzione	Descrizione
`sum(`x_0`, ..., `x_n`)`	Restituisce la somma dei valori delle variabili date nell'intervallo di tempo specificato. Questa funzione emette un punto dati solo se le variabili date hanno almeno un punto dati nell'intervallo di tempo corrente.
`min(`x_0`, ..., `x_n`)`	Restituisce il valore minimo delle variabili date nell'intervallo di tempo specificato. Questa funzione emette un punto dati solo se le variabili date hanno almeno un punto dati nell'intervallo di tempo corrente.
`max(`x_0`, ..., `x_n`)`	Restituisce il valore massimo delle variabili date nell'intervallo di tempo specificato. Questa funzione emette un punto dati solo se le variabili date hanno almeno un punto dati nell'intervallo di tempo corrente.
`count(`x_0`, ..., `x_n`)`	Restituisce il numero totale di punti di dati per le variabili date nell'intervallo di tempo corrente. Per ulteriori informazioni su come contare il numero di punti dati che soddisfano una condizione, consulta Conteggio dei punti dati che corrispondono a una condizione. Questa funzione calcola un punto dati per ogni intervallo di tempo.

Funzione	Descrizione
`stdev(x0, ..., xn)`	Restituisce la deviazione standard dei valori delle variabili specificate nell'intervallo di tempo corrente. Questa funzione emette un punto dati solo se le variabili date hanno almeno un punto dati nell'intervallo di tempo corrente.

Utilizzo di funzioni temporali nelle espressioni delle formule

Utilizza le funzioni temporali per restituire valori in base ai timestamp dei punti dati.

Utilizzo delle funzioni temporali nelle metriche

Solo nelle metriche, puoi utilizzare le seguenti funzioni che restituiscono valori in base ai timestamp dei punti dati.

Gli argomenti delle funzioni temporali devono essere proprietà del modello di asset locale o espressioni annidate. Ciò significa che non è possibile utilizzare le proprietà dei modelli di asset secondari nelle funzioni temporali.

È possibile utilizzare espressioni annidate nelle funzioni temporali. Quando si utilizzano espressioni nidificate, si applicano le seguenti regole:

- Ogni argomento può avere una sola variabile.

  Ad esempio, `latest( t*9/5 + 32 )` è supportato.
- Gli argomenti non possono essere funzioni di aggregazione.

  Ad esempio, `first( sum(x) )` non è supportato.

Funzione	Descrizione
`first(x)`	Restituisce il valore con il primo timestamp delle variabili date nell'intervallo di tempo specificato.

Funzione	Descrizione
`last(x)`	Restituisce il valore con l'ultimo timestamp delle variabili date nell'intervallo di tempo specificato.
`earliest(x)`	Restituisce l'ultimo valore della variabile specificata prima dell'inizio dell'intervallo di tempo corrente. Questa funzione calcola un punto dati per ogni intervallo di tempo, se la proprietà di input ha almeno un punto dati nella cronologia. Per informazioni dettagliate, vedi time-range-definition.
`latest(x)`	Restituisce l'ultimo valore della variabile specificata con l'ultimo timestamp prima della fine dell'intervallo di tempo corrente. Questa funzione calcola un punto dati per ogni intervallo di tempo, se la proprietà di input ha almeno un punto dati nella cronologia. Per informazioni dettagliate, vedi time-range-definition.

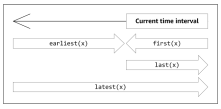
Funzione	Descrizione
`statetime(x)`	Restituisce la quantità di tempo in secondi in cui le variabili date sono risultate positive nell'intervallo di tempo specificato. È possibile utilizzare le funzioni di confronto per creare una proprietà di trasformazione da utilizzare per la `statetime` funzione. Ad esempio, se si dispone di una proprietà `Idle`, cioè `0` o `1`, è possibile calcolare la durata dell'inattività nell'intervallo di tempo con questa espressione: `IdleTime = statetime (Idle)` . Per ulteriori informazioni, vedere lo scenario statetime di esempio. La funzione non supporta le proprietà dei parametri come variabili di input. Questa funzione calcola un punto dati per ogni intervallo di tempo, se la proprietà di input ha almeno un punto dati nella cronologia.

Funzione	Descrizione
`TimeWeightedAvg(x, [interpolation])`	Restituisce la media dei dati di input ponderata con gli intervalli di tempo tra i punti. Vedi Parametri delle funzioni ponderate nel tempo per i dettagli del calcolo e degli intervalli. L'argomento opzionale `interpolaton` deve essere una costante di stringa: • `locf`— Questa è l'impostazione predefinita. Il calcolo utilizza l'algoritmo di calcolo Last Observed Carry Forward per gli intervalli tra i punti dati. In questo approccio, il punto dati viene calcolato come ultimo valore osservato fino al successivo timestamp del punto dati di input. Il valore dopo un buon punto dati viene estrapolato come valore fino al successivo timestamp del punto dati. • `linear`— Il calcolo utilizza l'algoritmo di calcolo dell'interpolazione lineare per gli intervalli tra i punti dati. Il valore tra due punti dati validi viene estrapolato come interpolazione lineare tra i valori di tali punti dati. Il valore tra punti dati buoni e cattivi o il valore dopo l'ultimo punto dati valido verrà estrapolato come punto dati valido.

Funzione	Descrizione
`TimeWeightedStDev(x, [algo])`	Restituisce la deviazione standard dei dati di input ponderata con gli intervalli di tempo tra i punti. Vedi Parametri delle funzioni ponderate nel tempo per i dettagli del calcolo e degli intervalli. Il calcolo utilizza l'algoritmo di calcolo Last Observed Carry Forward per gli intervalli tra i punti dati. In questo approccio, il punto dati viene calcolato come ultimo valore osservato fino al successivo timestamp del punto dati di input. Il peso viene calcolato come intervallo di tempo in secondi tra i punti dati o i confini della finestra. L'argomento opzionale `algo` deve essere una costante di stringa: • `f`— Questa è l'impostazione predefinita. Restituisce una varianza campionaria ponderata imparziale con pesi di frequenza , calcolata in TimeWeight secondi. Questo algoritmo viene generalmente assunto in base alla deviazione standard ed è noto come correzione di Bessel della deviazione standard per campioni ponderati. • `p`— Restituisce la varianza del campione ponderata e distorta, nota anche come varianza della popolazione. Le seguenti formule vengono utilizzate per il calcolo nei casi in cui: • S_p = deviazione standard della popolazione

Funzione	Descrizione
	• S_f = deviazione standard di frequenza • X_i = dati in entrata • ω_i = peso che equivale all'intervallo di tempo in secondi • μ* = media ponderata dei dati in entrata Equazione per la deviazione standard della popolazione: $$S_p^2 = \frac{\sum_{i=1}^{N} \omega_i (x_i - \mu^*)^2}{\sum_{i=1}^{N} \omega_i}$$ Equazione per la deviazione standard di frequenza: $$S_f^2 = \frac{\sum_{i=1}^{N} \omega_i (x_i - \mu^*)^2}{\sum_{i=1}^{N} \omega_i - 1}$$

Il diagramma seguente mostra come AWS IoT SiteWise calcola le funzioni temporali,, e `first` `last` `earliest``latest`, rispetto all'intervallo di tempo corrente.



Note

- L'intervallo di tempo per`first(x)`, `last(x)` è (inizio finestra corrente, fine finestra corrente].
- L'intervallo di tempo per `latest(x)` è (inizio dell'ora, fine della finestra corrente].
- L'intervallo di tempo per `earliest(x)` è (inizio dell'ora, fine della finestra precedente].

Parametri delle funzioni ponderati nel tempo

Le funzioni ponderate in base al tempo calcolate per la finestra aggregata tengono conto di quanto segue:

- Punti dati all'interno della finestra
- Intervalli di tempo tra i punti dati
- Ultimo punto dati prima della finestra
- Primo punto dati dopo la finestra (per alcuni algoritmi)

Termini:

- Punto dati errato: qualsiasi punto dati con qualità o valore non numerico non buono. Questo non viene considerato nel calcolo dei risultati di una finestra.
- Intervallo errato: l'intervallo dopo un punto dati errato. Anche l'intervallo precedente al primo punto dati noto è considerato un intervallo errato.
- Buon punto dati: qualsiasi punto dati con buona qualità e valore numerico.

> **Note**
>
> - AWS IoT SiteWise consuma dati di `GOOD` qualità solo quando calcola trasformazioni e metriche. Ignora e fornisce dati`UNCERTAIN`. `BAD`
> - L'intervallo precedente al primo punto dati noto è considerato un intervallo errato. Per ulteriori informazioni, consulta the section called “Tutorial sulle espressioni di formule”.

L'intervallo dopo l'ultimo punto dati noto continua all'infinito e influisce su tutte le finestre successive. Quando arriva un nuovo punto dati, la funzione ricalcola l'intervallo.

Seguendo le regole precedenti, il risultato aggregato della finestra viene calcolato e limitato ai limiti delle finestre. Per impostazione predefinita, la funzione invia il risultato della finestra solo se l'intera finestra è un intervallo adeguato.

Se l'intervallo di validità della finestra è inferiore alla lunghezza della finestra, la funzione non invia la finestra.

Quando i punti dati che influiscono sul risultato della finestra cambiano, la funzione ricalcola la finestra, anche se i punti dati si trovano all'esterno della finestra.

Se la proprietà di input ha almeno un punto dati nella sua cronologia ed è stato avviato un calcolo, la funzione calcola le funzioni aggregate ponderate nel tempo per ogni intervallo di tempo.

Example Esempio di scenario statetime

Si consideri un esempio in cui si dispone di una risorsa con le seguenti proprietà:

- `Idle`— Una misurazione che è o. `0` `1` Quando il valore è `1`, la macchina è inattiva.
- `Idle Time`— Una metrica che utilizza la formula `statetime(Idle)` per calcolare la quantità di tempo in secondi in cui la macchina è inattiva, per intervallo di 1 minuto.

La proprietà `Idle` ha i seguenti punti dati.

Time stamp	2:00:00 PM	2:00:30 PM	2:01:15 PM	2:02:45 PM	2:04:00 PM
Idle	0	1	1	0	0

AWS IoT SiteWise calcola la `Idle Time` proprietà ogni minuto in base ai valori di. `Idle` Al termine di questo calcolo, la proprietà `Idle Time` ha i seguenti punti dati.

Time stamp	2:00:00 PM	2:01:00 PM	2:02:00 PM	2:03:00 PM	2:04:00 PM
Idle Time	N/D	30	60	45	0

AWS IoT SiteWise esegue i seguenti calcoli `Idle Time` alla fine di ogni minuto.

- Alle 2:00 PM (dall'1:59 PM alle 2:00 PM)
  - Non ci sono dati per `Idle` prima delle 2:00 PM, quindi nessun punto dati viene calcolato.
- Alle 2:01 PM (dalle 2:00 PM alle 2:01 PM)
  - Alle 2:00:00 PM, la macchina è attiva (`Idle` è `0`).
  - Alle 2:00:30 PM, la macchina è inattiva (`Idle` è `1`).
  - `Idle` non cambia di nuovo prima della fine dell'intervallo alle 2:01:00 PM, quindi `Idle Time` è 30 secondi.

- Alle 2:02 PM (da 2:01 PM alle 2:02 PM)
  - Alle 2:01:00 PM, la macchina è inattiva (con l'ultimo punto dati alle 2:00:30 PM).
  - Alle 2:01:15, la macchina è ancora inattiva.
  - `Idle` non cambia di nuovo prima della fine dell'intervallo alle 2:02:00 PM, quindi `Idle Time` è 60 secondi.
- Alle 2:03 PM (dalle 2:02 PM fino 2:03 PM)
  - Alle 2:02:00 PM, la macchina è inattiva (per l'ultimo punto dati alle 2:01:15 PM).
  - Alle 2:02:45 PM, la macchina è attiva.
  - `Idle` non cambia di nuovo prima della fine dell'intervallo alle 2:03:00 PM, quindi `Idle Time` è 45 secondi.
- Alle 2:04 PM (dalle 2:03 PM fino alle 2:04 PM)
  - Alle 2:03:00 PM, la macchina è attiva (per l'ultimo punto dati alle 2:02:45 PM).
  - `Idle` non cambia di nuovo prima della fine dell'intervallo alle 2:04:00 PM, quindi `Idle Time` è 0 secondi.

Example Esempio TimeWeightedAvg e TimeWeightedStDev scenario

Le tabelle seguenti forniscono input e output di esempio per queste metriche della finestra di un minuto:. `Avg(x)`, `TimeWeightedAvg(x)`, `TimeWeightedAvg(x, "linear")`, `stDev(x)`, `timeWeightedStDev(x)`, `timeWeightedStDev(x, 'p')`

Esempio di input per una finestra aggregata di un minuto:

> **Note**
>
> Questi punti dati sono tutti di qualità. `GOOD`

03:00:00	4.0
03:01:00	2.0
03:01:10	8.0
03:01:50	20.0

03:02:00	14,0
03:02:05	10,0
03:02:10	3.0
03:02:30	20.0
03:03:30	0,0

Risultati aggregati in uscita:

> **Note**
>
> Nessuno: risultato non prodotto per questa finestra.

Orario	`Avg(x)`	`TimeWeighted Avg(x)`	`TimeWeighted Avg(X, "linear")`	`stDev(X)`	`timeWeighted StDev(x)`	`timeWeighted StDev(x, 'p')`
3:00:00	4	Nessuno	Nessuno	0	Nessuno	Nessuno
3:01:00	2	4	3	0	0	0
3:02:00	14	9	13	6	5,4306100415817 75	5,385164807134504
3:03:00	11	13	12,875	8,54400374531753	7,724054437220943	7,659416862050705
3:04:00	0	10	2.5	0	10,084389681792215	10
3:05:00	Nessuno	0	0	Nessuno	0	0

Uso delle funzioni temporali nelle trasformazioni

Solo nelle trasformazioni, è possibile utilizzare la `pretrigger()` funzione per recuperare il valore di `GOOD` qualità di una variabile prima dell'aggiornamento della proprietà che ha avviato il calcolo della trasformazione corrente.

Consideriamo un esempio in cui un produttore monitora AWS IoT SiteWise lo stato di una macchina. Il produttore utilizza le seguenti misurazioni e trasformazioni per rappresentare il processo:

- Una misurazione`current_state`, che può essere 0 o 1.
  - Se la macchina è in stato di pulizia, è `current_state` uguale a 1.
  - Se la macchina è in stato di produzione, è `current_state` uguale a 0.
- Una trasformazione, che `cleaning_state_duration` equivale a. `if(pretrigger(current_state) == 1, timestamp(current_state) - timestamp(pretrigger(current_state)), none)` Questa trasformazione restituisce per quanto tempo la macchina è rimasta nello stato di pulizia, in secondi, nel formato Unix epoch. Per ulteriori informazioni, vedere Utilizzo di funzioni condizionali nelle espressioni delle formule e la funzione timestamp ().

Se la macchina rimane in stato di pulizia più a lungo del previsto, il produttore potrebbe esaminare la macchina.

È possibile utilizzare la `pretrigger()` funzione anche in trasformazioni multivariate. Ad esempio, avete due misure denominate x and e y una trasformazione uguale a. `z x + y + pretrigger(y)` La tabella seguente mostra i valori per x e z dalle 9:00 alle 9:15. y

> **Note**
>
> - Questo esempio presuppone che i valori delle misurazioni arrivino in ordine cronologico. Ad esempio, il valore di x per 09:00 AM arriva prima del valore di x 09:05.
> - Se i punti dati per le 9:05 arrivano prima dei punti dati per le 9:00, z non viene calcolato alle 9:05.
> - Se il valore di x 9:05 AM arriva prima del valore di 09:00 AM e i valori di arrivano in x ordine cronologico, è uguale alle 9:05. y z `22 = 20 + 1 + 1`

	09:00	09:05	09:10	09:15
x	10	20		30
y	1	2	3	
`z = x + y + pretrigger(y)`	ynon riceve alcun punto dati prima delle 09:00. Pertanto, z non viene calcolato alle 09:00.	23 = 20 + 2 + 1 `pretrigger(y)` è uguale a 1.	25 = 20 + 3 + 2 xnon riceve un nuovo punto dati. `pretrigger(y)` è uguale a 2.	36 = 30 + 3 + 3 ynon riceve un nuovo punto dati. Pertanto, è `pretrigger(y)` uguale a 3 alle 09:15.

Utilizzo delle funzioni di data e ora nelle espressioni di formule

Nelle trasformazioni e nelle metriche, puoi utilizzare le funzioni di data e ora nei seguenti modi:

- Recupera il timestamp corrente di un punto dati in UTC o nel fuso orario locale.
- Costruisci timestamp con argomenti, come, e. `year` `month` `day_of_month`
- Estrai un periodo di tempo, ad esempio un anno o un mese, con l'argomento. `unix_time`

Funzione	Descrizione
`now()`	Restituisce la data e l'ora correnti, in secondi, nel formato Unix epoch.
`timestamp()`	• Nelle trasformazioni, la funzione restituisce il timestamp, in secondi, del messaggio di input nel formato Unix epoch. Solo nelle trasformazioni, puoi eseguire una delle seguenti operazioni: • Fornite una variabile come argomento della funzione. La `timestamp ( variable-name )` funzione restituisce

Funzione	Descrizione
	il timestamp, in secondi, del valore di `GOOD` qualità più recente per la variabile specifica ta nel formato Unix epoch. Ad esempio, se la risorsa ha una proprietà di trasformazione denominata `Temperatu re_F` che utilizza la `9/5 * Temperatu re_C` formula per convertire ogni punto di dati di temperatura da Celsius a Fahrenheit, potete utilizzare la `timestamp (Temperature_F)` funzione per ottenere il timestamp del valore di qualità più recente per la proprietà. `GOOD` `Temperature_F` • Utilizzate la `pretrigger()` funzione come argomento della funzione. La `timestamp(pretrigger(` *`variable-name`* `))` funzione restituisce il timestamp , in secondi, del valore di `GOOD` qualità per la variabile specificata prima dell'aggi ornamento della proprietà che ha avviato il calcolo della trasformazione corrente nel formato Unix epoch. Per ulteriori informazi oni, consulta Uso delle funzioni temporali nelle trasformazioni. • Nelle metriche, la funzione restituisce il timestamp recuperato alla fine della finestra corrente, in secondi, nel formato Unix epoch.

Funzione	Descrizione
`mktime(time_zone, year, month, day_of_month, hour, minute, second)`	Restituisce il tempo di input in secondi, nel formato Unix epoch. Per l'utilizzo di questa funzione si applicano i seguenti requisiti: • L'argomento del fuso orario deve essere una stringa tra virgolette (`'UTC'`). Se non specificato, il fuso orario predefinito è UTC. L'argomento del fuso orario può essere il primo o l'ultimo argomento. • L'anno, il mese, il giorno del mese, l'ora, il minuto e il secondo argomento devono essere in ordine. • Gli argomenti anno, mese e data sono obbligatori. Per l'utilizzo di questa funzione si applicano i seguenti limiti: • `year`- I valori validi sono compresi tra 1970 e 2250. • `month`- I valori validi sono compresi tra 1 e 12. • `day-of-month` - I valori validi sono compresi tra 1 e 31. • `hour`- I valori validi sono compresi tra 0 e 23. • `minute`- I valori validi sono compresi tra 0 e 59. • `second`- I valori validi sono compresi tra 0 e 60. Può essere un numero in virgola mobile. Esempi:

Funzione	Descrizione
	• `mktime(2020, 2, 29)` • `mktime('UTC+3', 2021, 12, 31, 22)` • `mktime(2022, 10, 13, 2, 55, 13.68, 'PST')`

Funzione	Descrizione
`localtime(unix_time, time_zone)`	Restituisce l'anno, il giorno del mese, il giorno della settimana, il giorno dell'anno, l'ora, il minuto o il secondo nel fuso orario specificato dall'ora Unix. Per l'utilizzo di questa funzione si applicano i seguenti requisiti: • L'argomento del fuso orario deve essere una stringa tra virgolette (`'UTC'`). Se non specificato, il fuso orario predefinito è UTC. • L'argomento Unix time è l'ora in secondi, nel formato Unix epoch. L'intervallo valido è 1-31556889864403199. Può essere un numero a virgola mobile. Esempio di risposta: `2007-12-03T10:15:30+01:00[Europe/Paris]` `localtime(unix_time, time_zone)` non è una funzione autonoma. Le `sec()` funzioni `year()mon()`,`mday`,`wday()`, `yday()hour()`,`minute()`,, e prendono `localtime(unix_time, time_zone)` come argomento. Esempi: • `year(localtime('GMT', 1605898608.8113723))` • `now().localtime().year()` • `timestamp().localtime('PST').year()`

Funzione	Descrizione
	• `localtime(1605289736, 'Europe/London').year()`
`year(localtime(unix_time, time_zone)`	Restituisce l'anno da`localtime(unix_time, time_zone)` .
`mon(localtime(unix_time, time_zone))`	Restituisce il mese da`localtime(unix_time, time_zone)` .
`mday(localtime(unix_time, time_zone))`	Restituisce il giorno del mese da`localtime(unix_time, time_zone)` .
`wday(localtime(unix_time, time_zone))`	Restituisce il giorno della settimana da`localtime(unix_time, time_zone)` .
`yday(localtime(unix_time, time_zone))`	Restituisce il giorno dell'anno da`localtime(unix_time, time_zone)` .
`hour(localtime(unix_time, time_zone))`	Restituisce l'ora da`localtime(unix_time, time_zone)` .
`minute(localtime(unix_time, time_zone))`	Restituisce il minuto da`localtime(unix_time, time_zone)` .
`sec(localtime(unix_time, time_zone))`	Restituisce il secondo da`localtime(unix_time, time_zone)` .

Formati di fuso orario supportati

È possibile specificare l'argomento del fuso orario nei seguenti modi:

- Scostamento del fuso orario: specifica `'Z'` l'UTC o un offset (`'+2'`o). `'-5'`
- ID di offset: combinano un'abbreviazione del fuso orario e un offset. Ad esempio `'GMT+2'` e `'UTC-01:00'`. L'abbreviazione del fuso orario deve contenere solo tre lettere.
- ID basati sulla regione: ad esempio, `'Etc/GMT+12'` e`'Pacific/Pago_Pago'`.

Abbreviazioni dei fusi orari supportate

Le funzioni di data e ora supportano le seguenti abbreviazioni del fuso orario di tre lettere:

- EST - - 05:00
- SAB -- 10:00
- SAB - 07:00
- ACT - Australia/Darwin
- AET - Australia/Sydney
- AGT - America/Argentina/Buenos Aires
- ARTE - Africa/Cairo
- AST - America/Anchorage
- BET - America/San Paolo
- BST - Asia/Dacca
- CAT - Africa/Harare
- CET - Europa/Parigi
- CNT - America/St. Johns
- CST - America/Chicago
- CTT - Asia/Shanghai
- EAT - Africa/Addis_Abeba
- IET - America/Indiana/Indianapolis
- IST - Asia/Calcutta
- JST - Asia/Tokyo
- MIT - Pacifico/Apia
- NET - Asia/Yerevan
- NST - Pacifico/Auckland
- PLT - Asia/Karachi
- PRT - America/Portorico
- PST - America/Los Angeles
- SST - Pacifico/Guadalcanal
- VST - Asia/Ho_Chi_Minh

ID basati sulla regione supportati

Le funzioni di data e ora supportano i seguenti ID basati sulla regione, organizzati in base alla loro relazione con UTC+ 00:00:

- ETC/GMT+12 (UTC- 12:00)
- Pacifico/Pago_Pago (UTC- 11:00)
- Pacifico/Samoa (UTC- 11:00)
- Pacifico/Niue (UTC- 11:00)
- Stati Uniti/Samoa (UTC- 11:00)
- ETC/GMT+11 (UTC- 11:00)
- Pacifico/Midway (UTC- 11:00)
- Pacifico/Honolulu (UTC- 10:00)
- Pacifico/Rarotonga (UTC- 10:00)
- Pacifico/Tahiti (UTC- 10:00)
- Pacifico/Johnston (UTC- 10:00)
- Stati Uniti/Hawaii (UTC- 10:00)
- Sistema V/HST10 (UTC- 10:00)
- ETC/GMT+10 (UTC- 10:00)
- Pacifico/Marchesi (UTC- 09:30)
- ETC/GMT+9 (UTC- 09:00)
- Pacifico/Gambier (UTC- 09:00)
- America/Atka (UTC- 09:00)
- Sistema V/YST9 (UTC- 09:00)
- America/Adak (UTC- 09:00)
- Stati Uniti/Aleutine (UTC- 09:00)
- ETC/GMT+8 (UTC- 08:00)
- Stati Uniti/Alaska (UTC- 08:00)
- America/Juneau (UTC- 08:00)
- America/Metlakatla (UTC- 08:00)
- America/Yakutat (UTC- 08:00)

- Pacifico/Pitcairn (UTC- 08:00)
- America/Sitka (UTC- 08:00)
- America/Anchorage (UTC- 08:00)
- Sistema V/PST 8 (UTC- 08:00)
- America/Nome (UTC- 08:00)
- Sistema V/YST9YDT (UTC- 08:00)
- Canada/Yukon (UTC- 07:00)
- Stati Uniti/Pacifico - Nuovo (UTC- 07:00)
- ETC/GMT+7 (UTC- 07:00)
- Stati Uniti/Arizona (UTC- 07:00)
- America/Dawson_Creek (UTC- 07:00)
- Canada/Pacifico (UTC- 07:00)
- PST 8 PDT (UTC- 07:00)
- Sistema V/MST7 (UTC- 07:00)
- America/Dawson (UTC- 07:00)
- Messico/ (UTC- 07:00) BajaNorte
- America/Tijuana (UTC- 07:00)
- America/Creston (UTC- 07:00)
- America/Hermosillo (UTC- 07:00)
- America/Santa Isabel (UTC- 07:00)
- America/Vancouver (UTC- 07:00)
- America/Ensenada (UTC- 07:00)
- America/Phoenix (UTC- 07:00)
- America/Whitehorse (UTC- 07:00)
- America/Fort_Nelson (UTC- 07:00)
- Sistema V/PST 8 PDT (UTC- 07:00)
- America/Los Angeles (UTC- 07:00)
- Stati Uniti/Pacifico (UTC- 07:00)
- America/El Salvador (UTC- 06:00)

- America/Guatemala (UTC- 06:00)
- America/Belize (UTC- 06:00)
- America/Managua (UTC- 06:00)
- America/Tegucigalpa (UTC- 06:00)
- ETC/GMT+6 (UTC- 06:00)
- Pacifico/Pasqua (UTC- 06:00)
- Messico/ BajaSur (UTC- 06:00)
- America/Regina (UTC- 06:00)
- America/Denver (UTC- 06:00)
- Pacifico/Galapagos (UTC- 06:00)
- America/Yellowknife (UTC- 06:00)
- America/Swift_Current (UTC- 06:00)
- America/Inuvik (UTC- 06:00)
- America/Mazatlán (UTC- 06:00)
- America/Boise (UTC- 06:00)
- America/Costa-Rica (UTC- 06:00)
- MST 07:00 (UTC- 06:00)
- Sistema V/CST6 (UTC- 06:00)
- America/Chihuahua (UTC- 06:00)
- America/Ojinaga (UTC- 06:00)
- Cile/ (UTC- 06:00) EasterIsland
- Stati Uniti/Mountain (UTC- 06:00)
- America/Edmonton (UTC- 06:00)
- Canada/Montagna (UTC- 06:00)
- America/Cambridge_Bay (UTC- 06:00)
- Navajo (UTC- 06:00)
- Sistema V/MST7MDT (UTC- 06:00)
- Canada/Saskatchewan (UTC- 06:00)
- America/Shiprock (UTC- 06:00)

- America/Panama (UTC- 05:00)
- America/Chicago (UTC- 05:00)
- America/Eirunepé (UTC- 05:00)
- ETC/GMT+5 (UTC- 05:00)
- Messico/Generale (UTC- 05:00)
- America/Porto_Acre (UTC- 05:00)
- America/Guayaquil (UTC- 05:00)
- America/Rankin_Inlet (UTC- 05:00)
- Stati Uniti/Central (UTC- 05:00)
- America/Rainy_River (UTC- 05:00)
- America/Indiana/Knox (UTC- 05:00)
- America/Dakota del Nord/Beulah (UTC- 05:00)
- America/Monterrey (UTC- 05:00)
- America/Giamaica (UTC- 05:00)
- America/Atikokan (UTC- 05:00)
- America/Coral_Harbour (UTC- 05:00)
- America/Dakota del Nord/Centro (UTC- 05:00)
- America/Cayman (UTC- 05:00)
- America/Indiana/Tell_City (UTC- 05:00)
- America/Città del Messico (UTC- 05:00)
- America/Matamoros (UTC- 05:00)
- CST 6 CDT (UTC- 05:00)
- America/Knox_in (UTC- 05:00)
- America/Bogotà (UTC- 05:00)
- America/Menominee (UTC- 05:00)
- America/Resolute (UTC- 05:00)
- Sistema V/EST 5 (UTC- 05:00)
- Canada/Central (UTC- 05:00)
- Brasile/Acre (UTC- 05:00)

- America/Cancún (UTC- 05:00)
- America/Lima (UTC- 05:00)
- America/Bahia Banderas (UTC- 05:00)
- Stati Uniti/Indiana-Starke (UTC- 05:00)
- America/Rio_Branco (UTC- 05:00)
- Sistema V/CST6CDT (UTC- 05:00)
- Giamaica (UTC- 05:00)
- America/Mérida (UTC- 05:00)
- America/North Dakota/New_Salem (UTC- 05:00)
- America/Winnipeg (UTC- 05:00)
- America/Cuiabá (UTC- 04:00)
- America/Marigot (UTC- 04:00)
- America/Indiana/Petersburg (UTC- 04:00)
- Cile/Continentale (UTC- 04:00)
- America/Grand_Turk (UTC- 04:00)
- Cuba (UTC- 04:00)
- ETC/GMT+4 (UTC- 04:00)
- America/Manaus (UTC- 04:00)
- America/Fort_Wayne (UTC- 04:00)
- America/Saint Thomas (UTC- 04:00)
- America/Anguilla (UTC- 04:00)
- America/L'Avana (UTC- 04:00)
- Stati Uniti/Michigan (UTC- 04:00)
- America/Barbados (UTC- 04:00)
- America/Louisville (UTC- 04:00)
- America/Curacao (UTC- 04:00)
- America/Guyana (UTC- 04:00)
- America/Martinica (UTC- 04:00)
- America/Porto_Rico (UTC- 04:00)

- America/Port_of_Spain (UTC- 04:00)
- Sistema V/AST 4 (UTC- 04:00)
- America/Indiana/Vevay (UTC- 04:00)
- America/Indiana/Vincennes (UTC- 04:00)
- America/Kralendijk (UTC- 04:00)
- America/Antigua (UTC- 04:00)
- America/Indianapolis (UTC- 04:00)
- America/Iqaluit (UTC- 04:00)
- America/Saint Vincent (UTC- 04:00)
- America/Kentucky/Louisville (UTC- 04:00)
- America/Dominica (UTC- 04:00)
- America/Asunción (UTC- 04:00)
- EST 5 EDT (UTC- 04:00)
- America/Nassau (UTC- 04:00)
- America/Kentucky/Monticello (UTC- 04:00)
- Brasile/Ovest (UTC- 04:00)
- America/Aruba (UTC- 04:00)
- America/Indiana/Indianapolis (UTC- 04:00)
- America/Santiago (UTC- 04:00)
- America/La_Paz (UTC- 04:00)
- America/Thunder_Bay (UTC- 04:00)
- America/Indiana/Marengo (UTC- 04:00)
- America/Blanc Sablon (UTC- 04:00)
- America/Santo Domingo (UTC- 04:00)
- Stati Uniti/Orientali (UTC- 04:00)
- Canada/Est (UTC- 04:00)
- America/Port-au-Prince (UTC- 04:00)
- America/Saint Barthelemy (UTC- 04:00)
- America/Nipigon (UTC- 04:00)

- Stati Uniti/Indiana orientale (UTC- 04:00)
- America/Saint Lucia (UTC- 04:00)
- America/Montserrat (UTC- 04:00)
- America/Lower_Princes (UTC- 04:00)
- America/Detroit (UTC- 04:00)
- America/Tortola (UTC- 04:00)
- America/Porto_Velho (UTC- 04:00)
- America/Campo_Grande (UTC- 04:00)
- America/Isole Vergini (UTC- 04:00)
- America/Pangnirtung (UTC- 04:00)
- America/Montréal (UTC- 04:00)
- America/Indiana/Winamac (UTC- 04:00)
- America/Boa Vista (UTC- 04:00)
- America/Grenada (UTC- 04:00)
- America/New York (UTC- 04:00)
- America/Saint Kitts (UTC- 04:00)
- America/Caracas (UTC- 04:00)
- America/Guadalupa (UTC- 04:00)
- America/Toronto (UTC- 04:00)
- Sistema V/EST 5 EDT (UTC- 04:00)
- America/Argentina/Catamarca (UTC- 03:00)
- Canada/Atlantico (UTC- 03:00)
- America/Argentina/Córdoba (UTC- 03:00)
- America/Araguaina (UTC- 03:00)
- America/Argentina/Salta (UTC- 03:00)
- ETC/GMT+3 (UTC- 03:00)
- America/Montevideo (UTC- 03:00)
- Brasile/Est (UTC- 03:00)
- America/Argentina/Mendoza (UTC- 03:00)
- America/Argentina/Rio_Gallegos (UTC- 03:00)

- America/Catamarca (UTC- 03:00)
- America/Córdoba (UTC- 03:00)
- America/San Paolo (UTC- 03:00)
- America/Argentina/Jujuy (UTC- 03:00)
- America/Cayenne (UTC- 03:00)
- America/Recife (UTC- 03:00)
- America/Buenos Aires (UTC- 03:00)
- America/Paramaribo (UTC- 03:00)
- America/Moncton (UTC- 03:00)
- America/Mendoza (UTC- 03:00)
- America/Santarem (UTC- 03:00)
- Atlantico/Bermuda (UTC- 03:00)
- America/Maceió (UTC- 03:00)
- Atlantico/Stanley (UTC- 03:00)
- America/Halifax (UTC- 03:00)
- Antartide/Rothera (UTC- 03:00)
- America/Argentina/San_Luis (UTC- 03:00)
- America/Argentina/Ushuaia (UTC- 03:00)
- Antartide/Palmer (UTC- 03:00)
- America/Punta_Arenas (UTC- 03:00)
- America/Glace_Bay (UTC- 03:00)
- America/Fortaleza (UTC- 03:00)
- America/Thule (UTC- 03:00)
- America/Argentina/La_Rioja (UTC- 03:00)
- America/Belém (UTC- 03:00)
- America/Jujuy (UTC- 03:00)
- America/Bahia (UTC- 03:00)
- America/Goose_Bay (UTC- 03:00)
- America/Argentina/San_Juan (UTC- 03:00)
- America/Argentina/ ComodRivadavia (UTC- 03:00)

- America/Argentina/Tucumán (UTC- 03:00)
- America/Rosario (UTC- 03:00)
- Sistema V/AST 4ADT (UTC- 03:00)
- America/Argentina/Buenos Aires (UTC- 03:00)
- America/St. Johns (UTC- 02:30)
- Canada/Terranova (UTC- 02:30)
- America/Miquelon (UTC- 02:00)
- ETC/GMT+2 (UTC- 02:00)
- America/Godthab (UTC- 02:00)
- America/Norfolk (UTC- 02:00)
- Brasile/ (UTC- 02:00) DeNoronha
- Atlantico/Georgia del Sud (UTC- 02:00)
- ETC/GMT+1 (UTC- 01:00)
- Atlantico/Capo Verde (UTC- 01:00)
- Pacifico/Kiritimati (UTC+ 14:00)
- ETC/GMT-14 (UTC+ 14:00)
- Pacifico/Fakaofo (UTC+ 13:00)
- Pacifico/Enderbury (UTC+ 13:00)
- Pacifico/Apia (UTC+ 13:00)
- Pacifico/Tongatapu (UTC+ 13:00)
- Etc/GMT-13 (UTC+ 13:00)
- NZ-CHAT (UTC+ 12:45)
- Pacifico/Chatham (UTC+ 12:45)
- Pacifico/Kwajalein (UTC+ 12:00)
- Antartide/ McMurdo (UTC+ 12:00)
- Pacifico/Wallis (UTC+ 12:00)
- Pacifico/Figi (UTC+ 12:00)
- Pacifico/Funafuti (UTC+ 12:00)
- Pacifico/Nauru (UTC+ 12:00)
- Kwajalein (UTC+ 12:00)

- NZ (UTC+ 12:00)
- Pacifico/Wake (UTC+ 12:00)
- Antartide/South_Pole (UTC+ 12:00)
- Pacifico/Tarawa (UTC+ 12:00)
- Pacifico/Auckland (UTC+ 12:00)
- Asia/Kamchatka (UTC+ 12:00)
- Etc/GMT-12 (UTC+ 12:00)
- Asia/Anadyr (UTC+ 12:00)
- Pacifico/Majuro (UTC+ 12:00)
- Pacifico/Ponape (UTC+ 11:00)
- Pacifico/Bougainville (UTC+ 11:00)
- Antartide/Macquarie (UTC+ 11:00)
- Pacifico/Pohnpei (UTC+ 11:00)
- Pacifico/Efate (UTC+ 11:00)
- Pacifico/Norfolk (UTC+ 11:00)
- Asia/Magadan (UTC+ 11:00)
- Pacifico/Kosrae (UTC+ 11:00)
- Asia/Sakhalin (UTC+ 11:00)
- Pacifico/Noumea (UTC+ 11:00)
- ETC/GMT-11 (UTC+ 11:00)
- Asia/Srednekolymsk (UTC+ 11:00)
- Pacifico/Guadalcanal (UTC+ 11:00)
- Australia/Lord_Howe (UTC+ 10:30)
- Australia/LHI (UTC+ 10:30)
- Australia/Hobart (UTC+ 10:00)
- Pacifico/Yap (UTC+ 10:00)
- Australia/Tasmania (UTC+ 10:00)
- Pacifico/Port_Moresby (UTC+ 10:00)
- Australia/ACT (UTC+ 10:00)
- Australia/Victoria (UTC+ 10:00)

- Pacifico/Chuuk (UTC+ 10:00)
- Australia/Queensland (UTC+ 10:00)
- Australia/Canberra (UTC+ 10:00)
- Australia/Currie (UTC+ 10:00)
- Pacifico/Guam (UTC+ 10:00)
- Pacifico/Truk (UTC+ 10:00)
- Australia/Nuovo Galles del Sud (UTC+ 10:00)
- Asia/Vladivostok (UTC+ 10:00)
- Pacifico/Saipan (UTC+ 10:00)
- Antartide/Dumontdurville (UTC+ 10:00)
- Australia/Sydney (UTC+ 10:00)
- Australia/Brisbane (UTC+ 10:00)
- Etc/GMT-10 (UTC+ 10:00)
- Asia/Ust-Nera (UTC+ 10:00)
- Australia/Melbourne (UTC+ 10:00)
- Australia/Lindeman (UTC+ 10:00)
- Australia/Nord (UTC+ 09:30)
- Australia/Yancowinna (UTC+ 09:30)
- Australia/Adelaide (UTC+ 09:30)
- Australia/Broken_Hill (UTC+ 09:30)
- Australia/Sud (UTC+ 09:30)
- Australia/Darwin (UTC+ 09:30)
- ETC/GMT-9 (UTC+ 09:00)
- Pacifico/Palau (UTC+ 09:00)
- Asia/Chita (UTC+ 09:00)
- Asia/Dili (UTC+ 09:00)
- Asia/Jayapura (UTC+ 09:00)
- Asia/Yakutsk (UTC+ 09:00)
- Asia/Pyongyang (UTC+ 09:00)
- MERCOLEDÌ (UTC+ 09:00)

- Asia/Seul (UTC+ 09:00)
- Asia/Khandyga (UTC+ 09:00)
- Giappone (UTC+ 09:00)
- Asia/Tokyo (UTC+ 09:00)
- Australia/Eucla (UTC+ 08:45)
- Asia/Kuching (UTC+ 08:00)
- Asia/Chungking (UTC+ 08:00)
- ETC/GMT-8 (UTC+ 08:00)
- Australia/Perth (UTC+ 08:00)
- Asia/Macao (UTC+ 08:00)
- Asia/Macao (UTC+ 08:00)
- Asia/Choibalsan (UTC+ 08:00)
- Asia/Shanghai (UTC+ 08:00)
- Antartide/Casey (UTC+ 08:00)
- Asia/Ulan_Bator (UTC+ 08:00)
- Asia/Chongqing (UTC+ 08:00)
- Asia/Ulan Bator (UTC+ 08:00)
- Asia/Taipei (UTC+ 08:00)
- Asia/Manila (UTC+ 08:00)
- PRC (UTC+ 08:00)
- Asia/Ujung-Pandang (UTC+ 08:00)
- Asia/Harbin (UTC+ 08:00)
- Singapore (UTC+ 08:00)
- Asia/Brunei (UTC+ 08:00)
- Australia/Ovest (UTC+ 08:00)
- Asia/Hong Kong (UTC+ 08:00)
- Asia/Makassar (UTC+ 08:00)
- Hong Kong (UTC+ 08:00)
- Asia/Kuala Lumpur (UTC+ 08:00)
- Asia/Irkutsk (UTC+ 08:00)

- Asia/Singapore (UTC+ 08:00)
- Asia/Pontianak (UTC+ 07:00)
- ETC/GMT-7 (UTC+ 07:00)
- Asia/Phnom_Penh (UTC+ 07:00)
- Asia/Novosibirsk (UTC+ 07:00)
- Antartide/Davis (UTC+ 07:00)
- Asia/Tomsk (UTC+ 07:00)
- Asia/Giacarta (UTC+ 07:00)
- Asia/Barnaul (UTC+ 07:00)
- Indiano/Natale (UTC+ 07:00)
- Asia/Ho Chi Minh (UTC+ 07:00)
- Asia/Hovd (UTC+ 07:00)
- Asia/Bangkok (UTC+ 07:00)
- Asia/Vientiane (UTC+ 07:00)
- Asia/Novokuzneck (UTC+ 07:00)
- Asia/Krasnoyarsk (UTC+ 07:00)
- Asia/Saigon (UTC+ 07:00)
- Asia/Yangon (UTC+ 06:30)
- Asia/Yangon (UTC+ 06:30)
- Indiana/Cocos (UTC+ 06:30)
- Asia/Kashgar (UTC+ 06:00)
- ETC/GMT-6 (UTC+ 06:00)
- Asia/Almaty (UTC+ 06:00)
- Asia/Dacca (UTC+ 06:00)
- Asia/Omsk (UTC+ 06:00)
- Asia/Dacca (UTC+ 06:00)
- Indiana/Chagos (UTC+ 06:00)
- Asia/Qyzylorda (UTC+ 06:00)
- Asia/Bishkek (UTC+ 06:00)
- Antartide/Vostok (UTC+ 06:00)

- Asia/Urumqi (UTC+ 06:00)
- Asia/Thimbu (UTC+ 06:00)
- Asia/Thimphu (UTC+ 06:00)
- Asia/Kathmandu (UTC+ 05:45)
- Asia/Kathmandu (UTC+ 05:45)
- Asia/Calcutta (UTC+ 05:30)
- Asia/Colombo (UTC+ 05:30)
- Asia/Calcutta (UTC+ 05:30)
- Asia/Aqtau (UTC+ 05:00)
- ETC/GMT-5 (UTC+ 05:00)
- Asia/Samarcanda (UTC+ 05:00)
- Asia/Karachi (UTC+ 05:00)
- Asia/Ekaterinburg (UTC+ 05:00)
- Asia/Dushanbe (UTC+ 05:00)
- Indiana/Maldive (UTC+ 05:00)
- Asia/Orale (UTC+ 05:00)
- Asia/Taskent (UTC+ 05:00)
- Antartide/Mawson (UTC+ 05:00)
- Asia/Aktobe (UTC+ 05:00)
- Asia/Ashkhabad (UTC+ 05:00)
- Asia/Ashgabat (UTC+ 05:00)
- Asia/Atyrau (UTC+ 05:00)
- Indiana/Kerguelen (UTC+ 05:00)
- Iran (UTC+ 04:30)
- Asia/Teheran (UTC+ 04:30)
- Asia/Kabul (UTC+ 04:30)
- Asia/Yerevan (UTC+ 04:00)
- ETC/GMT-4 (UTC+ 04:00)
- Etc/GMT-4 (UTC+ 04:00)
- Asia/Dubai (UTC+ 04:00)

- Indiana/Riunione (UTC+ 04:00)
- Europa/Saratov (UTC+ 04:00)
- Europa/Samara (UTC+ 04:00)
- Indiana/Mahé (UTC+ 04:00)
- Asia/Baku (UTC+ 04:00)
- Asia/Muscat (UTC+ 04:00)
- Europa/Volgograd (UTC+ 04:00)
- Europa/Astrakhan (UTC+ 04:00)
- Asia/Tbilisi (UTC+ 04:00)
- Europa/Ulyanovsk (UTC+ 04:00)
- Asia/Aden (UTC+ 03:00)
- Africa/Nairobi (UTC+ 03:00)
- Europa/Istanbul (UTC+ 03:00)
- ETC/GMT-3 (UTC+ 03:00)
- Europa/Zaporozhye (UTC+ 03:00)
- Israele (UTC+ 03:00)
- Indiana/Comore (UTC+ 03:00)
- Antartide/Syowa (UTC+ 03:00)
- Africa/Mogadiscio (UTC+ 03:00)
- Europa/Bucarest (UTC+ 03:00)
- Africa/Asmeria (UTC+ 03:00)
- Europa/Mariehamn (UTC+ 03:00)
- Asia/Istanbul (UTC+ 03:00)
- Europa/Tiraspol (UTC+ 03:00)
- Europa/Mosca (UTC+ 03:00)
- Europa/Chisinau (UTC+ 03:00)
- Europa/Helsinki (UTC+ 03:00)
- Asia/Beirut (UTC+ 03:00)
- Asia/Tel Aviv (UTC+ 03:00)
- Africa/Gibuti (UTC+ 03:00)

- Europa/Simferopol (UTC+ 03:00)
- Europa/Sofia (UTC+ 03:00)
- Asia/Gaza (UTC+ 03:00)
- Africa/Asmara (UTC+ 03:00)
- Europa/Riga (UTC+ 03:00)
- Asia/Bagdad (UTC+ 03:00)
- Asia/Damasco (UTC+ 03:00)
- Africa/Dar_es_Salaam (UTC+ 03:00)
- Africa/Addis_Abeba (UTC+ 03:00)
- Europa/Uzhgorod (UTC+ 03:00)
- Asia/Gerusalemme (UTC+ 03:00)
- Asia/Riyad (UTC+ 03:00)
- Asia/Kuwait (UTC+ 03:00)
- Europa/Kirov (UTC+ 03:00)
- Africa/Kampala (UTC+ 03:00)
- Europa/Minsk (UTC+ 03:00)
- Asia/Qatar (UTC+ 03:00)
- Europa/Kiev (UTC+ 03:00)
- Asia/Bahrein (UTC+ 03:00)
- Europa/Vilnius (UTC+ 03:00)
- Indiana/Antananarivo (UTC+ 03:00)
- Indiana/Mayotte (UTC+ 03:00)
- Europa/Tallinn (UTC+ 03:00)
- Turchia (UTC+ 03:00)
- Africa/Juba (UTC+ 03:00)
- Asia/Nicosia (UTC+ 03:00)
- Asia/Famagosta (UTC+ 03:00)
- S-DOM (UTC+ 03:00)
- EET (UTC+ 03:00)
- Asia/Hebron (UTC+ 03:00)

- Asia/Amman (UTC+ 03:00)
- Europa/Nicosia (UTC+ 03:00)
- Europa/Atene (UTC+ 03:00)
- Africa/Cairo (UTC+ 02:00)
- Africa/Mbabane (UTC+ 02:00)
- Europa/Bruxelles (UTC+ 02:00)
- Europa/Varsavia (UTC+ 02:00)
- CET (UTC+ 02:00)
- Europa/Lussemburgo (UTC+ 02:00)
- ETC/GMT-2 (UTC+ 02:00)
- Libia (UTC+ 02:00)
- Africa/Kigali (UTC+ 02:00)
- Africa/Tripoli (UTC+ 02:00)
- Europa/Kaliningrad (UTC+ 02:00)
- Africa/Windhoek (UTC+ 02:00)
- Europa/Malta (UTC+ 02:00)
- Europa/Busingen (UTC+ 02:00)
-
- Europa/Skopje (UTC+ 02:00)
- Europa/Sarajevo (UTC+ 02:00)
- Europa/Roma (UTC+ 02:00)
- Europa/Zurigo (UTC+ 02:00)
- Europa/Gibilterra (UTC+ 02:00)
- Africa/Lubumbashi (UTC+ 02:00)
- Europa/Vaduz (UTC+ 02:00)
- Europa/Lubiana (UTC+ 02:00)
- Europa/Berlino (UTC+ 02:00)
- Europa/Stoccolma (UTC+ 02:00)
- Europa/Budapest (UTC+ 02:00)
- Europa/Zagabria (UTC+ 02:00)

- Europa/Parigi (UTC+ 02:00)
- Africa/Ceuta (UTC+ 02:00)
- Europa/Praga (UTC+ 02:00)
- Antartide/Troll (UTC+ 02:00)
- Africa/Gaborone (UTC+ 02:00)
- Europa/Copenaghen (UTC+ 02:00)
- Europa/Vienna (UTC+ 02:00)
- Europa/Tirana (UTC+ 02:00)
- INCONTRATO (UTC+ 02:00)
- Europa/Amsterdam (UTC+ 02:00)
- Africa/Maputo (UTC+ 02:00)
- Europa/San_Marino (UTC+ 02:00)
- Polonia (UTC+ 02:00)
- Europa/Andorra (UTC+ 02:00)
- Europa/Oslo (UTC+ 02:00)
- Europa/Podgorica (UTC+ 02:00)
- Africa/Bujumbura (UTC+ 02:00)
- Atlantico/Jan_Mayen (UTC+ 02:00)
- Africa/Maseru (UTC+ 02:00)
- Europa/Madrid (UTC+ 02:00)
- Africa/Blantyre (UTC+ 02:00)
- Africa/Lusaka (UTC+ 02:00)
- Africa/Harare (UTC+ 02:00)
- Africa/Khartum (UTC+ 02:00)
- Africa/Johannesburg (UTC+ 02:00)
- Europa/Belgrado (UTC+ 02:00)
- Europa/Bratislava (UTC+ 02:00)
- Artico/Longyearbyen (UTC+ 02:00)
- Egitto (UTC+ 02:00)
- Europa/Vaticano (UTC+ 02:00)

- Europa/Monaco (UTC+ 02:00)
- Europa/Londra (UTC+ 01:00)
- Etc/GMT-1 (UTC+ 01:00)
- Europa/Jersey (UTC+ 01:00)
- Europa/Guernsey (UTC+ 01:00)
- Europa/Isle_of_Man (UTC+ 01:00)
- Africa/Tunisi (UTC+ 01:00)
- Africa/Malabo (UTC+ 01:00)
- GB-Irlanda (UTC+ 01:00)
- Africa/Lagos (UTC+ 01:00)
- Africa/Algeri (UTC+ 01:00)
- IT (UTC+ 01:00)
- Portogallo (UTC+ 01:00)
- Africa/Sao_Tomé (UTC+ 01:00)
- Africa/N' Djamena (UTC+ 01:00)
- Atlantico/Fær Øer (UTC+ 01:00)
- Irlanda (UTC+ 01:00)
- Atlantico/Faroe (UTC+ 01:00)
- Europa/Dublino (UTC+ 01:00)
- Africa/Libreville (UTC+ 01:00)
- Africa/El_Aaiun (UTC+ 01:00)
- Africa/El_Aaiun (UTC+ 01:00)
- Africa/Douala (UTC+ 01:00)
- Africa/Brazzaville (UTC+ 01:00)
- Africa/Porto-Novo (UTC+ 01:00)
- Atlantico/Madeira (UTC+ 01:00)
- Europa/Lisbona (UTC+ 01:00)
- Atlantico/Canarie (UTC+ 01:00)
- Africa/Casablanca (UTC+ 01:00)

- Europa/Belfast (UTC+ 01:00)
- Africa/Luanda (UTC+ 01:00)
- Africa/Kinshasa (UTC+ 01:00)
- Africa/Bangui (UTC+ 01:00)
- UMIDO (UTC+ 01:00)
- Africa/Niamey (UTC+ 01:00)
- GMT (UTC+ 00:00)
- etc/GMT-0 (UTC+ 00:00)
- Atlantic/Sant' Elena (UTC+ 00:00)
- Etc/GMT+0 (UTC+ 00:00)
- Africa/Banjul (UTC+ 00:00)
- ETC/GMT (UTC+ 00:00)
- Africa/Freetown (UTC+ 00:00)
- Africa/Bamako (UTC+ 00:00)
- Africa/Conakry (UTC+ 00:00)
- Universale (UTC+ 00:00)
- Africa/Nouakchott (UTC+ 00:00)
- UTC (UTC+ 00:00)
- Etc/Universal (UTC+ 00:00)
- Atlantico/Azzorre (UTC+ 00:00)
- Africa/Abidjan (UTC+ 00:00)
- Africa/Accra (UTC+ 00:00)
- ETC/UTC (UTC+ 00:00)
- GMT0 (UTC+ 00:00)
- Zulu (UTC+ 00:00) Zulu (UTC+ 00:00)
- Africa/Ouagadougou (UTC+ 00:00)
- Atlantico/Reykjavík (UTC+ 00:00)
- Etc/Zulu (UTC+ 00:00)
- Islanda (UTC+ 00:00)

- Africa/Lomé (UTC+ 00:00)
- Greenwich (UTC+ 00:00)
- etc/GMT0 (UTC+ 00:00)
- America/Danmarkshavn (UTC+ 00:00)
- Africa/Dakar (UTC+ 00:00)
- Africa/Bissau (UTC+ 00:00)
- Etc/Greenwich (UTC+ 00:00)
- Africa/Timbuctù (UTC+ 00:00)
- UTC (UTC+ 00:00)
- Africa/Monrovia (UTC+ 00:00)
- ETC/UTC (UTC+ 00:00)

Tutorial sulle espressioni di formule

Puoi seguire questi tutorial per utilizzare le espressioni delle formule in. AWS IoT SiteWise

Argomenti

Usare le stringhe nelle formule

È possibile utilizzare le stringhe nelle espressioni delle formule. È inoltre possibile inserire stringhe da variabili che fanno riferimento alle proprietà degli attributi e delle misurazioni.

> **Important**
>
> Le espressioni delle formule possono generare solo valori doppi o stringhe. Le espressioni annidate possono generare altri tipi di dati, ad esempio stringhe, ma la formula nel suo

insieme deve restituire un numero o una stringa. È possibile utilizzare la funzione jp per convertire una stringa in un numero. Il valore booleano deve essere 1 (vero) o 0 (falso). Per ulteriori informazioni, consulta Valori indefiniti, infiniti e di overflow.

AWS IoT SiteWise fornisce le seguenti funzionalità di espressione delle formule che è possibile utilizzare per operare sulle stringhe:

- Stringhe letterali
- L'operatore di indice () `s[index]`
- L'operatore slice () `s[start:end:step]`
- Funzioni di confronto, che è possibile utilizzare per confrontare le stringhe in base all'ordine lessicografico
- Funzioni di stringa, che includono la `jp` funzione in grado di analizzare oggetti JSON serializzati e convertire stringhe in numeri

Filtraggio dei punti dati

È possibile utilizzare la funzione if per filtrare i punti dati che non soddisfano una condizione. La `if` funzione valuta una condizione e restituisce valori `true` e `false` risultati diversi. È possibile utilizzare la costante none come output per un caso di una `if` funzione per scartare il punto dati relativo a quel caso.

Per filtrare i punti dati che corrispondono a una condizione

- Crea una trasformazione che utilizzi la `if` funzione per definire una condizione che verifichi se una condizione è soddisfatta e la restituisca none come `result_if_false` valore `result_if_true` or.

Example Esempio: filtra i punti dati in cui l'acqua non bolle

Prendiamo in considerazione uno scenario in cui si esegue `temp_c` una misurazione che fornisce la temperatura (in gradi Celsius) dell'acqua in una macchina. Puoi definire la seguente trasformazione per filtrare i punti dati in cui l'acqua non bolle:

- Trasforma: `boiling_temps = if(gte(temp_c, 100), temp_c, none)` — Restituisce la temperatura se è maggiore o uguale a 100 gradi Celsius, altrimenti non restituisce alcun punto dati.

Conteggio dei punti dati che corrispondono a una condizione

È possibile utilizzare le funzioni di confronto e sum () per contare il numero di punti dati per i quali una condizione è vera.

Per contare i punti dati che corrispondono a una condizione

1. Crea una trasformazione che utilizza una funzione di confronto per definire una condizione di filtro su un'altra proprietà.
2. Creare un parametro che sommi i punti dati in cui tale condizione è soddisfatta.

Example Esempio: contare il numero di punti dati in cui l'acqua è in ebollizione.

Prendiamo in considerazione uno scenario in cui si esegue `temp_c` una misurazione che fornisce la temperatura (in gradi Celsius) dell'acqua in una macchina. È possibile definire le seguenti proprietà di trasformazione e parametro per contare il numero di punti dati in cui l'acqua è in ebollizione:

- Trasforma: `is_boiling = gte(temp_c, 100)` — Restituisce 1 se la temperatura è maggiore o uguale a 100 gradi Celsius, altrimenti restituisce. `0`
- Metrica: `boiling_count = sum(is_boiling)` — Restituisce il numero di punti dati in cui l'acqua bolle.

Dati tardivi nelle formule

AWS IoT SiteWise supporta l'inserimento tardivo di dati risalenti fino a 7 giorni fa. Quando AWS IoT SiteWise riceve dati in ritardo, ricalcola i valori esistenti per qualsiasi metrica che inserisce i dati in ritardo in una finestra precedente. Questi ricalcoli comportano costi di elaborazione dei dati.

> **Note**
>
> Quando AWS IoT SiteWise calcola proprietà che immettono dati tardivi, utilizza l'espressione della formula corrente di ogni proprietà.

Dopo aver AWS IoT SiteWise ricalcolato una finestra precedente per una metrica, sostituisce il valore precedente per quella finestra. Se hai abilitato le notifiche per quella metrica, emette AWS IoT SiteWise anche una notifica del valore della proprietà. Ciò significa che è possibile ricevere una nuova notifica di aggiornamento del valore della proprietà per la stessa proprietà e timestamp per cui

è stata precedentemente ricevuta una notifica. Se le applicazioni o i data lake utilizzano notifiche sui valori delle proprietà, devi aggiornare il valore precedente con il nuovo valore in modo che i dati siano accurati.

Qualità dei dati nelle formule

In AWS IoT SiteWise, ogni punto dati ha un codice di qualità, che può essere uno dei seguenti:

- `GOOD`— I dati non sono interessati da alcun problema.
- `BAD`— I dati sono interessati da un problema come il guasto del sensore.
- `UNCERTAIN`— I dati sono influenzati da un problema come l'imprecisione del sensore.

AWS IoT SiteWise utilizza solo dati `GOOD` di qualità quando calcola trasformazioni e metriche. AWS IoT SiteWise restituisce solo dati di `GOOD` qualità per calcoli di successo. Se un calcolo non ha esito positivo, AWS IoT SiteWise non emette un punto dati per quel calcolo. Ciò può verificarsi se un calcolo genera un valore indefinito, infinito o di overflow.

Per ulteriori informazioni su come eseguire query sui dati e filtrare in base alla qualità dei dati, vedere Interroga dati da AWS IoT SiteWise.

Valori indefiniti, infiniti e di overflow

Alcune espressioni di formule (ad esempio `x / 0`, `sqrt(-1)`, `olog(0)`) calcolano valori non definiti in un sistema numerico reale, infiniti o al di fuori dell'intervallo supportato da. AWS IoT SiteWise Quando l'espressione di una proprietà di asset calcola un valore indefinito, infinito o di overflow, AWS IoT SiteWise non genera un punto dati per quel calcolo.

AWS IoT SiteWise inoltre non emette un punto dati se calcola un valore non numerico come risultato di un'espressione di formula. Ciò significa che se definisci una formula che calcola una stringa, una matrice o la costante none, AWS IoT SiteWise non genera un punto dati per quel calcolo.

Example Esempi

Ciascuna delle seguenti espressioni di formula restituisce un valore che non AWS IoT SiteWise può essere rappresentato come numero. AWS IoT SiteWise non genera un punto dati quando calcola queste espressioni di formule.

- `x / 0`non è definito.
- `log(0)`non è definito.
- `sqrt(-1)`non è definito in un sistema numerico reale.

- `"hello" + " world"`è una stringa.
- `jp('{"values":[3,6,7]}', '$.values')`è un array.
- `if(gte(temp, 300), temp, none)`è none quando `temp` è inferiore a`300`.

Creazione di modelli compositi personalizzati (Componenti)

I modelli compositi personalizzati, o i componenti, se utilizzi la console, forniscono un altro livello di organizzazione per i modelli di asset e i modelli di componenti. Puoi usarli per strutturare i tuoi modelli raggruppando le proprietà o facendo riferimento ad altri modelli. Per ulteriori informazioni sull'utilizzo di modelli compositi personalizzati, consulta. Modelli compositi personalizzati (componenti)

È possibile creare un modello composito personalizzato all'interno di un modello di asset o di componenti esistente. Esistono due tipi di modelli compositi personalizzati. Per raggruppare le proprietà correlate all'interno di un modello, è possibile creare un modello composito personalizzato in linea. Per fare riferimento a un modello di componente all'interno del vostro modello di asset o modello di componente, potete creare un modello composito component-model-basedpersonalizzato.

Le sezioni seguenti descrivono come utilizzare l' AWS IoT SiteWise API per creare modelli compositi personalizzati.

Argomenti

- Creazione di un componente in linea (console)
- Creazione di un modello composito personalizzato in linea ()AWS CLI
- Creazione di un component-model-based componente (console)
- Creazione di un modello composito component-model-based personalizzato (AWS CLI)

Creazione di un componente in linea (console)

È possibile utilizzare la AWS IoT SiteWise console per creare un componente in linea che definisce le proprie proprietà.

> **Note**
>
> Poiché si tratta di un componente in linea, queste proprietà si applicano solo al modello di asset corrente e non sono condivise altrove.
> Se avete bisogno di produrre un modello riutilizzabile (ad esempio, per condividerlo tra più modelli di asset o per includere più istanze all'interno di un modello di asset), dovreste

invece creare un componente basato su un modello di componente. Per i dettagli, consulta la sezione seguente.

Per creare un componente (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione selezionare Models (Modelli).
3. Scegliete il modello di asset a cui desiderate aggiungere un componente.
4. Nella scheda Proprietà, scegliete Componenti.
5. Scegli Crea componente.
6. Nella pagina Crea componente, procedi come segue:

   a. Immettete un nome per il componente, ad esempio **`ServoMotor`** o**`ServoMotor Model`**. Questo nome deve essere univoco per tutti i componenti del tuo account in questa regione.

   b. (Facoltativo) Aggiungi le definizioni attributi per il modello. Gli attributi rappresentano informazioni che vengono modificate raramente. Per ulteriori informazioni, consulta Definizione di dati statici (attributi).

   c. (Facoltativo) Aggiungi le definizioni misurazione per il modello. Le misurazioni rappresentano flussi di dati provenienti dall'apparecchiatura. Per ulteriori informazioni, consulta Definizione dei flussi di dati provenienti dalle apparecchiature (misurazioni).

   d. (Facoltativo) Aggiungi le definizioni di trasformazione per il modello. Le trasformazioni sono formule che mappano i dati da un modulo all'altro. Per ulteriori informazioni, consulta Trasformazione dei dati (trasformazioni).

   e. (Facoltativo) Aggiungi le definizioni parametro per il modello. Le metriche sono formule che aggregano i dati su intervalli di tempo. Le metriche possono inserire dati dalle risorse associate, in modo da poter calcolare valori che rappresentano l'operazione o un sottoinsieme dell'operazione. Per ulteriori informazioni, consulta Aggregazione di dati da proprietà e altre risorse (metriche).

   f. Scegliete Crea componente.

Creazione di un modello composito personalizzato in linea ()AWS CLI

È possibile utilizzare il AWS Command Line Interface (AWS CLI) per creare un modello composito personalizzato in linea che definisce le proprie proprietà.

Utilizzate l'CreateAssetModelCompositeModeloperazione per creare un modello in linea con proprietà. Questa operazione prevede un payload con la seguente struttura.

> **Note**
>
> Poiché si tratta di un modello composito in linea, queste proprietà si applicano solo al modello di asset corrente e non sono condivise altrove. Ciò che lo rende «in linea» è che non fornisce un valore per il `composedAssetModelId` campo.
> Se avete bisogno di produrre un modello riutilizzabile (ad esempio, da condividere tra più modelli di asset o per includere più istanze all'interno di un unico modello di asset), dovreste invece creare un modello component-model-basedcomposito. Per i dettagli, consultate la sezione seguente.

```
{
    "assetModelCompositeModelName": "CNCLathe_ServoMotorA",
    "assetModelCompositeModelType": "CUSTOM",
    "assetModelCompositeModelProperties": [
        {
            "dataType": "DOUBLE",
            "name": "Servo Motor Temperature",
            "type": {
            "measurement": {}
            },
            "unit": "Celsius"
        },
        {
            "dataType": "DOUBLE",
            "name": "Spindle speed",
            "type": {
            "measurement": {}
            },
            "unit": "rpm"
        }
    ]
}
```

Creazione di un component-model-based componente (console)

È possibile utilizzare la AWS IoT SiteWise console per creare un componente basato su un modello di componente.

Per creare un component-model-based componente (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione selezionare Models (Modelli).
3. Scegliete il modello di asset a cui desiderate aggiungere un componente.
4. Nella scheda Proprietà, scegliete Componenti.
5. Scegli Crea componente.
6. Nella pagina Crea componente, procedi come segue:

    a. Seleziona il modello di componente su cui vuoi basare il componente.

    b. Immettete un nome per il componente, ad esempio **`ServoMotor`** o**`ServoMotor Model`**. Questo nome deve essere univoco per tutti i componenti del tuo account in questa regione.

    c. Scegli Crea componente.

Creazione di un modello composito component-model-based personalizzato (AWS CLI)

Puoi utilizzarli AWS CLI per creare un modello composito component-model-based personalizzato all'interno del tuo modello di asset. Un modello composito component-model-based personalizzato è un riferimento a un modello di componente che hai già definito altrove.

Utilizzate l'CreateAssetModelCompositeModeloperazione per creare un modello composito component-model-based personalizzato. Questa operazione prevede un payload con la seguente struttura.

> **Note**
>
> In questo esempio, il valore di `composedAssetModelId` è l'ID del modello di asset o l'ID esterno di un modello di componente esistente. Per ulteriori informazioni, consulta Riferimento a oggetti con ID esterni nella Guida per l'utente di AWS IoT SiteWise . Per un esempio di come creare un modello di componente, vedeteCreazione di un modello di componente (AWS CLI).

```
{
    "assetModelCompositeModelName": "CNCLathe_ServoMotorA",
```

```
    "assetModelCompositeModelType": "CUSTOM",
    "composedAssetModelId": component model ID
]
```

Poiché si tratta solo di un riferimento, un modello composito component-model-based personalizzato non ha proprietà proprie, a parte un nome.

Se desiderate aggiungere più istanze dello stesso componente al vostro modello di asset (ad esempio, una macchina CNC con più servomotori), potete aggiungere più modelli compositi component-model-based personalizzati che hanno ciascuno il proprio nome ma che fanno tutti lo stesso riferimento. `composedAssetModelId`

È possibile annidare i componenti all'interno di altri componenti. A tale scopo, puoi aggiungere un modello component-model-based composito, come mostrato in questo esempio, a uno dei tuoi modelli di componenti.

Creazione degli asset

È possibile creare un asset partendo da un modello. Devi avere un modello di asset prima di poter creare un asset. Se non hai creato nessun modello di asset, consulta Creazione dei modelli di asset.

> **Note**
>
> È possibile creare asset solo da modelli `ACTIVE`. Se lo stato del modello non fosse `ACTIVE`, bisognerà attendere qualche minuto per poter creare degli asset correlati. Per ulteriori informazioni, consulta Stati di asset e modelli.

Argomenti

- Creazione di un asset (console)
- Creare una risorsa (AWS CLI)
- Configurazione di un nuovo asset

Creazione di un asset (console)

È possibile utilizzare la AWS IoT SiteWise console per creare una risorsa.

Per creare un asset (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Asset.
3. Selezionare Create asset (Crea asset).
4. Nella pagina Crea asset, esegui le operazioni seguenti:

   a. Per Modello, scegli il modello di asset da cui creare un asset.

   > **Note**
   >
   > Se il modello non è ATTIVO, è necessario attendere che diventi attivo oppure risolvere i problemi se è NON RIUSCITO.

   b. Immetti un nome per l'asset.

   c. (Facoltativo) Aggiungi i tag per l'asset. Per ulteriori informazioni, consulta Taggare le tue risorse AWS IoT SiteWise.

   d. Selezionare Create asset (Crea asset).

   Quando crei una risorsa, la AWS IoT SiteWise console accede alla pagina della nuova risorsa. In questa pagina puoi vedere lo stato dell'asset che inizialmente è CREAZIONE IN CORSO. Questa pagina si aggiorna automaticamente, quindi attendi l'aggiornamento dello stato dell'asset.

   > **Note**
   >
   > Il processo di creazione di un asset può richiedere fino a un minuto. Dopo che lo Stato è ATTIVO, potete eseguire operazioni di aggiornamento sulla risorsa. Per ulteriori informazioni, consulta Stati di asset e modelli.

Dopo aver creato un asset, consulta Configurazione di un nuovo asset.

Creare una risorsa (AWS CLI)

È possibile utilizzare AWS Command Line Interface (AWS CLI) per creare una risorsa a partire da un modello di asset.

Per creare un asset, è necessario disporre di un `assetModelId`. Se avete creato un modello di asset, ma non lo conosceteassetModelId, utilizzate l'ListAssetModelsAPI per visualizzare tutti i vostri modelli di asset.

Per creare una risorsa da un modello di asset, utilizzate l'CreateAssetAPI con i seguenti parametri:

- `assetName`— Il nome della nuova risorsa. Assegna un nome alla risorsa per aiutarti a identificarla.
- `assetModelId`— L'ID della risorsa. Questo è l'ID effettivo in formato UUID, o `externalId:myExternalId` se ne ha uno. Per ulteriori informazioni, consulta Riferimento a oggetti con ID esterni nella Guida per l'utente di AWS IoT SiteWise .

Per creare una risorsa ()AWS CLI

- Esegui il comando seguente per creare un asset. Sostituite *`asset-name`* con un nome per l'asset e *`asset-model-id`*con l'ID o l'ID esterno del modello di asset.

```
aws iotsitewise create-asset \
  --asset-name asset-name \
  --asset-model-id asset-model-id
```

L'azione restituisce una risposta contenente lo stato e i dettagli del nuovo asset nel formato seguente.

```
{
  "assetId": "String",
  "assetArn": "String",
  "assetStatus": {
    "state": "String",
    "error": {
      "code": "String",
      "message": "String"
    }
  }
}
```

L'elemento `state` è `CREATING` fino a quando l'asset non viene creato.

> **Note**
>
> Il processo di creazione di un asset può richiedere fino a un minuto. Per verificare lo stato della risorsa, utilizzate l'DescribeAssetoperazione con l'ID della risorsa come parametro. `assetId` Dopo che la risorsa `state` è `ACTIVE` pronta, potete eseguire operazioni di aggiornamento sulla risorsa. Per ulteriori informazioni, consulta Stati di asset e modelli.

Dopo aver creato un asset, consulta Configurazione di un nuovo asset.

Configurazione di un nuovo asset

Completa la configurazione dell'asset con le seguenti operazioni facoltative:

- Mappatura dei flussi di dati industriali alle proprietà degli asset se l'asset ha proprietà di misurazione.
- Aggiornamento dei valori degli attributi se l'asset ha valori di attributo univoci.
- Associazione e annullamento dell'associazione degli asset se l'asset è padre.

Ricerca di risorse

Utilizza la funzionalità Console AWS IoT SiteWise di ricerca per trovare risorse in base ai metadati e ai filtri dei valori delle proprietà in tempo reale.

Prerequisiti

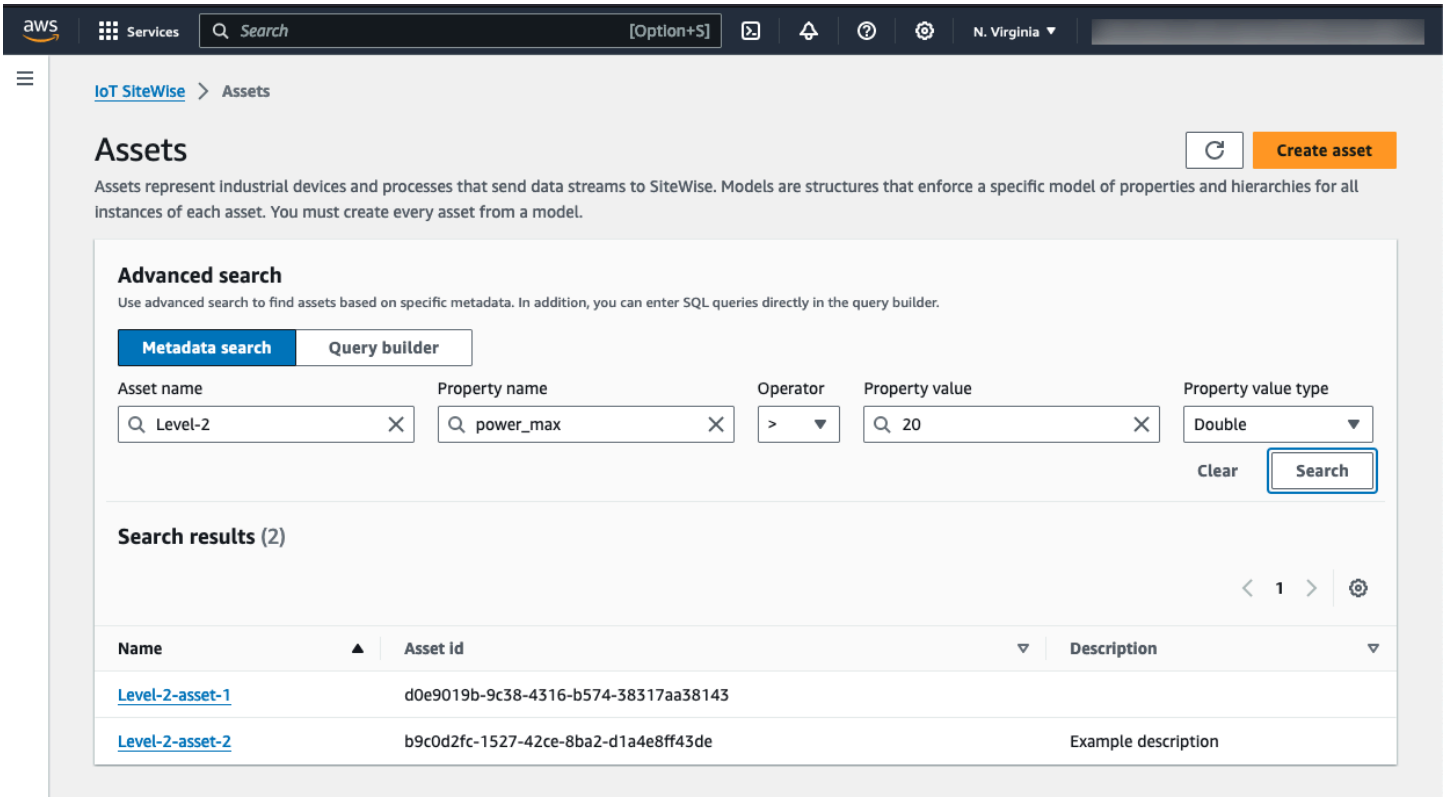
AWS IoT SiteWise richiede autorizzazioni per l'integrazione per organizzare e AWS IoT TwinMaker modellare meglio i dati industriali. Se hai concesso le autorizzazioni a AWS IoT SiteWise, utilizza l'ExecuteQueryAPI. Se non hai concesso le autorizzazioni e hai bisogno di assistenza per AWS IoT SiteWise iniziare, consulta. Integrazione di AWS IoT SiteWise e AWS IoT TwinMaker

Ricerca avanzata su Console AWS IoT SiteWise

Ricerca di metadati

1. Passare alla console AWS IoT SiteWise.

2. Nel riquadro di navigazione, scegli Ricerca avanzata in Risorse.
3. In Ricerca avanzata, scegliete l'opzione di ricerca dei metadati.
4. Compila i parametri. Compila il maggior numero possibile di campi per una ricerca efficiente.
    a. Nome della risorsa: inserisci un nome completo della risorsa o un nome parziale per una ricerca ampia.
    b. Nome della proprietà: inserisci il nome completo della proprietà o un nome parziale per una ricerca ampia.
    c. Operatore: scegli un operatore tra:
        - **=**
        - **<**
        - **>**
        - **<=**
        - **>=**
    d. Valore della proprietà: questo valore viene confrontato con il valore più recente della proprietà.
    e. Tipo di valore della proprietà: il tipo di dati della proprietà. Scegli tra le seguenti opzioni:
        - Doppio
        - Numero intero
        - Stringa
        - Booleano
5. Selezionare Search (Cerca).
6. Nella tabella dei risultati della ricerca, scegliete la risorsa dalla colonna Nome. Verrà visualizzata la pagina dettagliata della risorsa.



Ricerca parziale

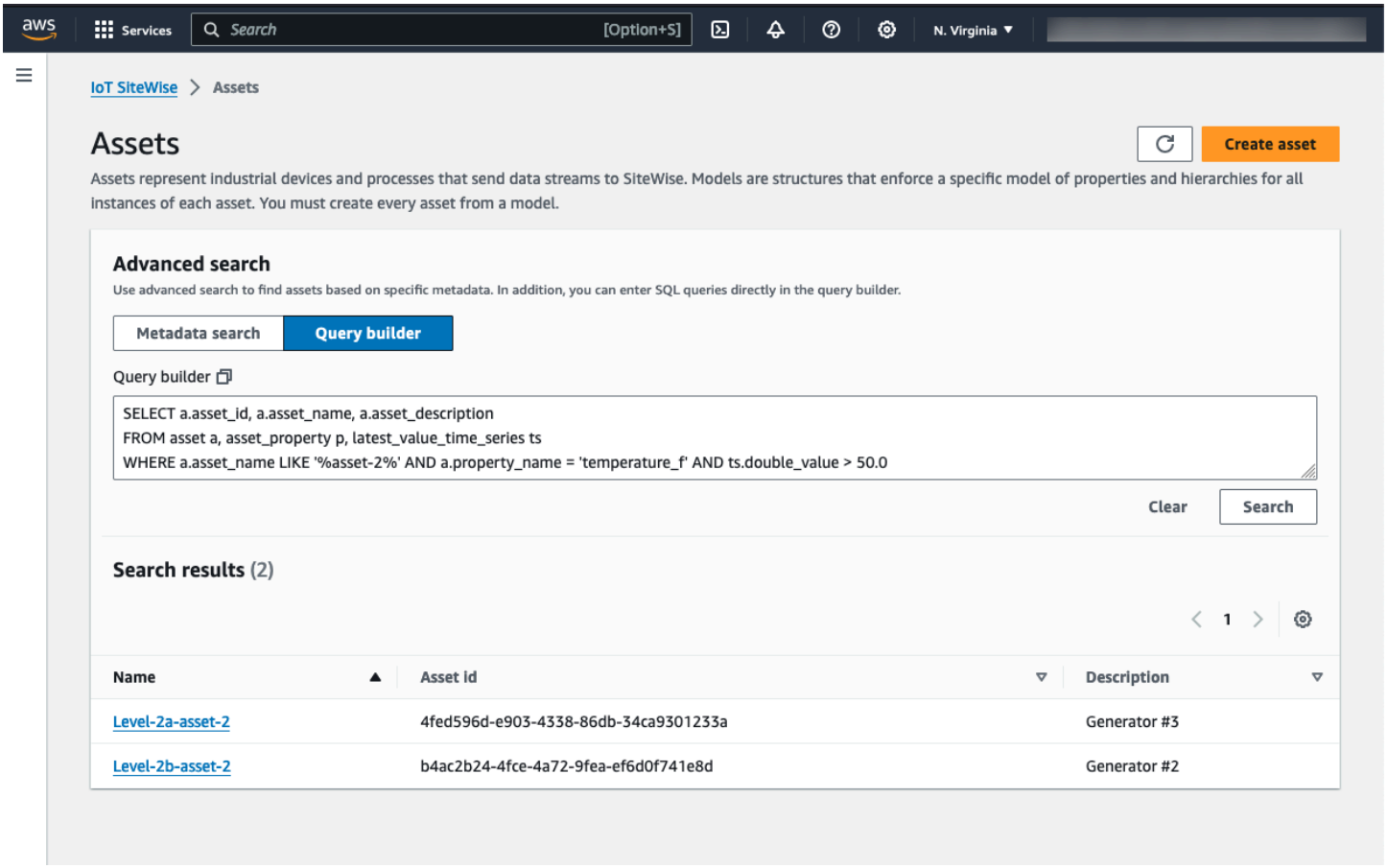
Non è necessario fornire tutti i parametri per la ricerca di risorse. Ecco alcuni esempi di ricerche parziali che utilizzano l'opzione di ricerca Metadati:

- Trova le risorse in base al loro nome:
  - Inserisci un valore solo nel campo Nome risorsa.
  - I campi Nome della proprietà e Valore della proprietà sono vuoti.
- Trova risorse contenenti proprietà con un nome specifico:
  - Immettete un valore solo nel campo Nome della proprietà.
  - I campi Nome della risorsa e Valore della proprietà sono vuoti.
- Trova le risorse in base ai valori più recenti delle loro proprietà:
  - Immettete i valori nei campi Nome della proprietà e Valore della proprietà.
  - Seleziona un tipo di valore dell'operatore e della proprietà.

Ricerca con Query Builder

1. Passare alla Console AWS IoT SiteWise.

2. Nel riquadro di navigazione, scegli Ricerca avanzata in Risorse.
3. In Ricerca avanzata scegli l'opzione Query builder.
4. Nel riquadro Query Builder, scrivi la tua query SQL per recuperare un`asset_name`, e. `asset_id` `asset_description`
5. Selezionare Search (Cerca).
6. Dalla tabella dei risultati della ricerca, scegliete la risorsa dalla colonna Nome. Verrà visualizzata la pagina dettagliata della risorsa.



Note

- La `SELECT` clausola della query SQL deve includere i `asset_id` campi `asset_name` and per garantire una risorsa valida nella tabella dei risultati della ricerca.

- Il generatore di query visualizza solo il nome, l'ID della risorsa e la descrizione nella tabella dei risultati. L'aggiunta di altri campi alla `SELECT` clausola non aggiunge altre colonne alla tabella dei risultati

Mappatura dei flussi di dati industriali alle proprietà degli asset

È possibile definire un alias di proprietà sulla proprietà dell'asset. Questo vi aiuta a identificare la proprietà di un asset quando inserite o recuperate i dati di un asset. Se la risorsa ha proprietà di misurazione, è possibile definire gli alias delle proprietà per mappare i flussi di dati a tali proprietà di misurazione.

Questo processo richiede che tu conosca l'alias della tua proprietà.

- Se si importano dati da server OPC-UA utilizzando un'origine dati OPC-UA in un gateway SiteWise Edge, l'alias di proprietà è il percorso di una variabile nel nodo Oggetti, a partire da. `/`

  Example

  Se il percorso della variabile è, allora l'alias della proprietà è`company/windfarm/3/turbine/7/temperature`. `/company/windfarm/3/turbine/7/temperature`

  Per ulteriori informazioni sull'architettura delle informazioni OPC-UA, vedere Information Model and Address Spacing mapping nell'OPC UA Online Reference.

  > **Note**
  >
  > - Se si configura un prefisso del flusso di dati per l'origine OPC-UA, è necessario includere tale prefisso nell'alias di proprietà per tutti i flussi di dati di tale origine.
  >
  >   Example
  >
  >   Se `/RentonWA` è un prefisso, l'alias precedente è. `/RentonWA/company/windfarm/3/turbine/7/temperature`
  > - Gli alias di proprietà possono contenere fino a 1.000 byte. I percorsi delle variabili OPC-UA possono contenere fino a 4.096 byte. Attualmente, AWS IoT SiteWise non supporta l'acquisizione di dati da variabili OPC-UA con percorsi lunghi.

- Se si importano dati da server Modbus utilizzando una sorgente dati Modbus TCP in un SiteWise gateway Edge, l'alias della proprietà è:

  Modbus `register set tag name`

  Utilizzate questo valore per inviare dati da questo set di registri a una proprietà dell'asset.
- Se importate dati da altre fonti, ad esempio utilizzando AWS IoT le regole o l'API, dovete definire gli alias delle proprietà. È possibile definire un sistema di denominazione degli alias di proprietà applicabile alla configurazione del dispositivo. Ad esempio, se si inseriscono dati da oggetti AWS IoT , è possibile includere il nome dell'oggetto negli alias di proprietà per identificare in modo univoco i flussi di dati. Per ulteriori informazioni su questo esempio, consulta il tutorial Ingesting data from things. AWS IoT

Gli alias di proprietà devono essere univoci all'interno di una regione e di un account. AWS AWS IoT SiteWise restituisce un errore se si imposta un alias di proprietà su uno che esiste già su un'altra proprietà dell'asset.

Se disponi di più sorgenti OPC-UA con percorsi di flusso di dati identici, aggiungi un prefisso ai percorsi di ciascuna fonte per formare alias unici. Per ulteriori informazioni, consulta Configurazione delle origini dati.

> **Note**
>
> Questa sezione descrive come impostare gli alias di proprietà per le proprietà di misurazione. Per ulteriori informazioni su come impostare gli alias di proprietà per le proprietà degli stati di allarme esterni, vedere. Mappatura dei flussi di stato di allarme esterni

Argomenti

- Impostazione di un alias di proprietà (console)
- Impostazione di un alias di proprietà ()AWS CLI

Impostazione di un alias di proprietà (console)

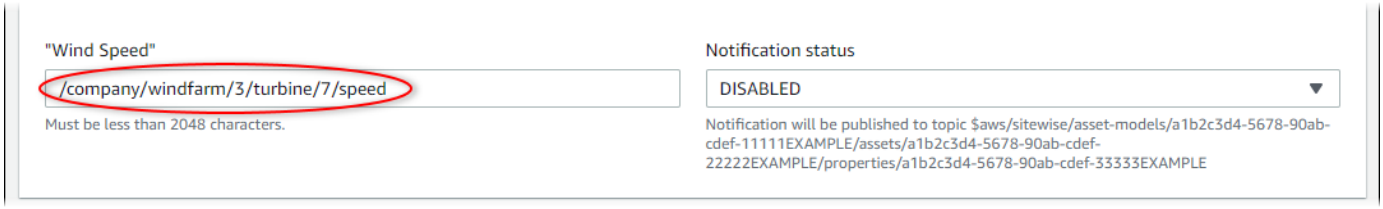
È possibile utilizzare la AWS IoT SiteWise console per impostare un alias per una proprietà dell'asset.

Per impostare un alias di proprietà (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Asset.
3. Scegli l'asset per cui vuoi impostare un alias di proprietà.

> **Tip**
>
> Puoi scegliere l'icona a forma di freccia per espandere una gerarchia di asset e trovare il tuo asset.

4. Scegli Modifica.
5. Individua la proprietà per cui vuoi impostare un alias e quindi immetti l'alias di proprietà.



6. Selezionare Salva.

Impostazione di un alias di proprietà ()AWS CLI

Utilizzate il AWS Command Line Interface (AWS CLI) per impostare un alias per una proprietà dell'asset.

Per completare questa procedura, è necessario conoscere l'elemento `assetId` dell'asset e l'elemento `propertyId` della proprietà. Puoi anche usare l'ID esterno. Se hai creato una risorsa e non la conosci`assetId`, utilizza l'ListAssetsAPI per elencare tutte le risorse per un modello specifico. Utilizzate l'DescribeAssetoperazione per visualizzare le proprietà della risorsa, compresi gli ID delle proprietà.

Utilizzate l'UpdateAssetPropertyoperazione per mappare un flusso di dati alla proprietà della risorsa. Specifica i seguenti parametri:

- `assetId`— L'ID o l'ID esterno della risorsa. Per ulteriori informazioni, consulta Riferimento a oggetti con ID esterni nella Guida per l'utente di AWS IoT SiteWise .
- `propertyId`— L'ID o l'ID esterno della proprietà della risorsa.

- `propertyAlias`— Il percorso del flusso di dati verso l'alias della proprietà.
- `propertyNotificationState`— Lo stato di notifica del valore della proprietà: `ENABLED` o`DISABLED`. Specifica lo stato di notifica esistente della proprietà quando aggiorni l'alias della proprietà. È possibile recuperare lo stato di notifica esistente con l'DescribeAssetPropertyoperazione.

  Se ometti questo parametro, il nuovo stato di notifica è `DISABLED`. Per ulteriori informazioni sulle notifiche delle proprietà, consulta Interazione con altri servizi AWS.

Per impostare un alias di proprietà ()AWS CLI

1. Esegui il comando seguente per recuperare lo stato di notifica corrente della proprietà. Sostituisci *`asset-id`* e *`property-id`* con gli ID della proprietà di asset.

   ```
   aws iotsitewise describe-asset-property \
     --asset-id asset-id \
     --property-id property-id
   ```

   L'operazione restituisce una risposta contenente i dettagli della proprietà di asset nel formato seguente. Lo stato di notifica della proprietà si trova in `assetProperty.notification.state` nell'oggetto JSON.

   ```
   {
     "assetId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
     "assetName": "Wind Turbine 7",
     "assetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
     "assetProperty": {
       "id": "a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
       "name": "Wind Speed",
       "notification": {
         "topic": "$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/
   assets/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE/properties/a1b2c3d4-5678-90ab-
   cdef-33333EXAMPLE",
         "state": "ENABLED"
       },
       "dataType": "DOUBLE",
       "unit": "m/s",
       "type": {
         "measurement": {}
       }
   ```

```
  }
}
```

2. Esegui il comando seguente per impostare l'alias della proprietà di asset. Sostituisci *property-alias* con l'alias di proprietà e *notification-state* con lo stato di notifica oppure ometti `--property-notification-state` per disabilitare le notifiche. Facoltativamente, potete aggiornare l'unità dell'asset con una nuova *unità* e. `--property-unit`

```
aws iotsitewise update-asset-property \
  --asset-id asset-id \
  --property-id property-id \
  --property-alias property-alias \
  --property-notification-state notification-state \
  --property-unit unit
```

3. Per verificare che l'alias sia stato impostato, esegui il comando seguente per recuperare i dettagli della proprietà. Sostituisci *asset-id* e *property-id* con gli ID della proprietà di asset.

```
aws iotsitewise describe-asset-property \
  --asset-id asset-id \
  --property-id property-id
```

L'operazione restituisce una risposta contenente i dettagli della proprietà di asset nel formato seguente. L'alias della proprietà si trova `assetProperty.alias` nell'oggetto JSON ed è impostato su in questo esempio. `myAlias`

```
{
  "assetId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
  "assetName": "Wind Turbine 7",
  "assetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
  "assetProperty": {
    "alias": "myAlias",
    "id": "a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
    "name": "Wind Speed",
    "notification": {
      "topic": "$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/
assets/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE/properties/a1b2c3d4-5678-90ab-
cdef-33333EXAMPLE",
      "state": "ENABLED"
    },
    "dataType": "DOUBLE",
```

```
    "unit": "m/s",
    "type": {
      "measurement": {}
    }
  }
}
```

Aggiornamento dei valori degli attributi

Gli asset ereditano gli attributi del proprio modello con i relativi valori predefiniti. In alcuni casi, è consigliabile mantenere l'attributo predefinito del modello di asset; ad esempio, per la proprietà del produttore di un asset. In altri casi, invece, occorre aggiornare l'attributo ereditato; ad esempio, per la latitudine e la longitudine di un asset.

Updating an attribute value (console)

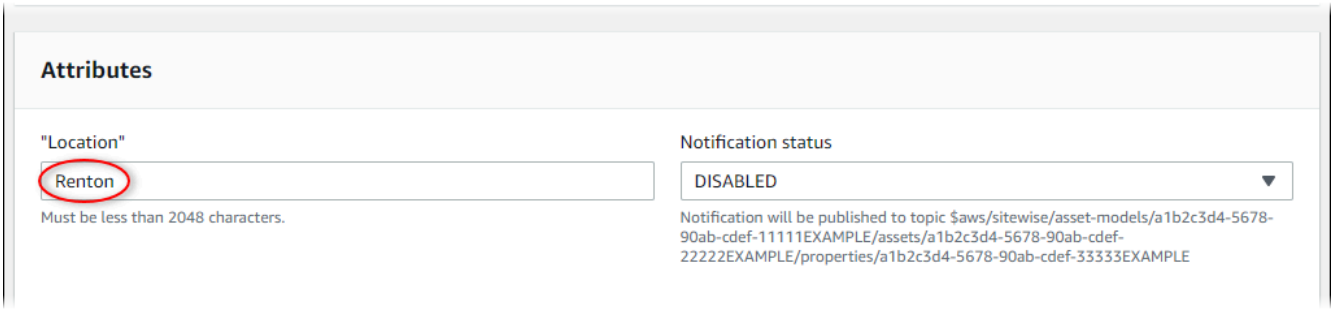
È possibile utilizzare la AWS IoT SiteWise console per aggiornare il valore di una proprietà di un asset attributo.

Per aggiornare il valore di un attributo (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Asset.
3. Scegli l'asset per cui vuoi aggiornare un attributo.

   > **Tip**
   >
   > Puoi scegliere l'icona a forma di freccia per espandere una gerarchia di asset e trovare il tuo asset.

4. Scegli Modifica.
5. Individua l'attributo da aggiornare e quindi immetti il nuovo valore.



6. Selezionare Salva.

Updating an attribute value (AWS CLI)

È possibile utilizzare AWS Command Line Interface (AWS CLI) per aggiornare il valore di un attributo.

Per completare questa procedura, è necessario conoscere l'elemento `assetId` dell'asset e l'elemento `propertyId` della proprietà. Puoi anche usare l'ID esterno. Se hai creato una risorsa e non la conosci`assetId`, utilizza l'ListAssetsAPI per elencare tutte le risorse per un modello specifico. Utilizzate l'DescribeAssetoperazione per visualizzare le proprietà della risorsa, compresi gli ID delle proprietà.

Utilizzate l'BatchPutAssetPropertyValueoperazione per assegnare i valori degli attributi alla risorsa. È possibile utilizzare questa operazione per impostare più attributi contemporaneamente. Il payload di questa operazione include un elenco di voci, ciascuna delle quali contenente l'ID asset, l'ID proprietà e il valore dell'attributo.

Per aggiornare il valore di un attributo ()AWS CLI

1. Crea un file denominato `batch-put-payload.json` e copia il seguente oggetto JSON nel file. Questo esempio di payload mostra come impostare la latitudine e la longitudine di una turbina eolica. Aggiorna gli ID, i valori e i timestamp per modificare il payload per il tuo caso d'uso.

```
{
  "entries": [
    {
      "entryId": "windfarm3-turbine7-latitude",
      "assetId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
      "propertyId": "a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
      "propertyValues": [
```

```
        {
          "value": {
            "doubleValue": 47.6204
          },
          "timestamp": {
            "timeInSeconds": 1575691200
          }
        }
      ]
    },
    {
      "entryId": "windfarm3-turbine7-longitude",
      "assetId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
      "propertyId": "a1b2c3d4-5678-90ab-cdef-55555EXAMPLE",
      "propertyValues": [
        {
          "value": {
            "doubleValue": 122.3491
          },
          "timestamp": {
            "timeInSeconds": 1575691200
          }
        }
      ]
    }
  ]
}
```

- Ogni voce nel payload contiene un `entryId` che è possibile definire come una qualsiasi stringa univoca. Se una richiesta non riesce, ciascun errore conterrà l'`entryId` della richiesta corrispondente in modo che sia possibile sapere quale richiesta riprovare.
- Per impostare il valore di un attributo, è possibile includere una struttura timestamp-quality-value (TQV) nell'elenco di ogni proprietà dell'`propertyValues`attributo. Questa struttura deve contenere il nuovo `value` e il `timestamp` corrente.
  - `value`— Una struttura che contiene uno dei seguenti campi, a seconda del tipo di proprietà impostata:
    - `booleanValue`
    - `doubleValue`
    - `integerValue`
    - `stringValue`

- `timestamp`— Una struttura che contiene l'ora attuale dell'epoca Unix in secondi,. `timeInSeconds` AWS IoT SiteWise rifiuta tutti i punti dati con timestamp che esistevano da più di 7 giorni nel passato o più recenti di 5 minuti nelle future.

Per ulteriori informazioni su come preparare un payload per, consulta. BatchPutAssetPropertyValueAcquisizione di dati tramite l'API AWS IoT SiteWise

2. Eseguite il comando seguente per inviare i valori degli attributi a AWS IoT SiteWise:

```
aws iotsitewise batch-put-asset-property-value -\-cli-input-json file://batch-put-payload.json
```

Associazione e annullamento dell'associazione degli asset

Se il modello di asset li prevede nelle proprie gerarchie, è possibile associare asset figlio all'asset padre. Gli asset padre possono accedere e aggregare i dati dagli asset associati. Per ulteriori informazioni sui modelli di asset gerarchici, consulta Definizione delle gerarchie dei modelli di asset.

Argomenti

- Associazione e annullamento dell'associazione degli asset (console)
- Associazione e dissociazione delle risorse ()AWS CLI

Associazione e annullamento dell'associazione degli asset (console)

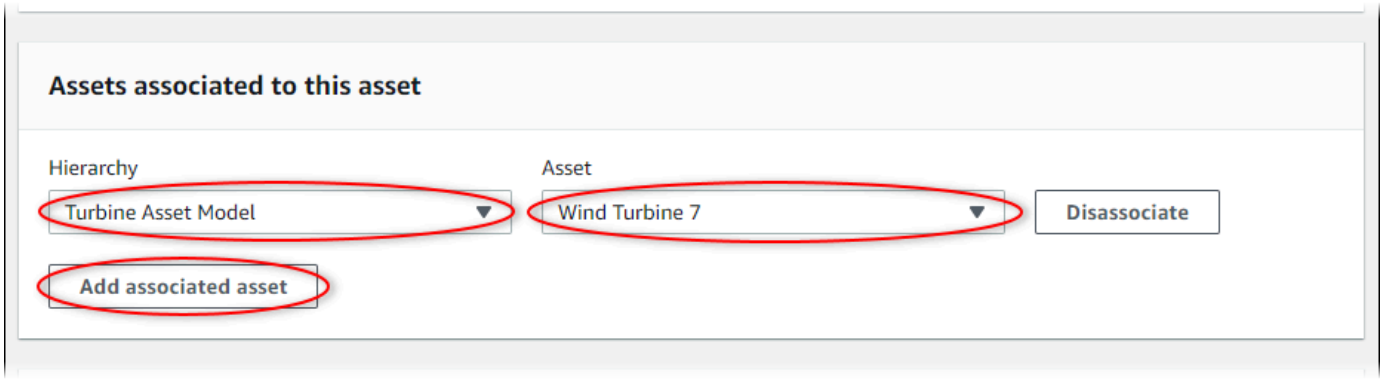
È possibile utilizzare la AWS IoT SiteWise console per associare e dissociare gli asset.

Per associare un asset (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Asset.
3. Scegli l'asset padre a cui vuoi associare un asset figlio.

> **Tip**
>
> Puoi scegliere l'icona a forma di freccia per espandere una gerarchia di asset e trovare il tuo asset.

4. Scegli Modifica.
5. In Asset associati a questo asset scegli Aggiungi asset associato.



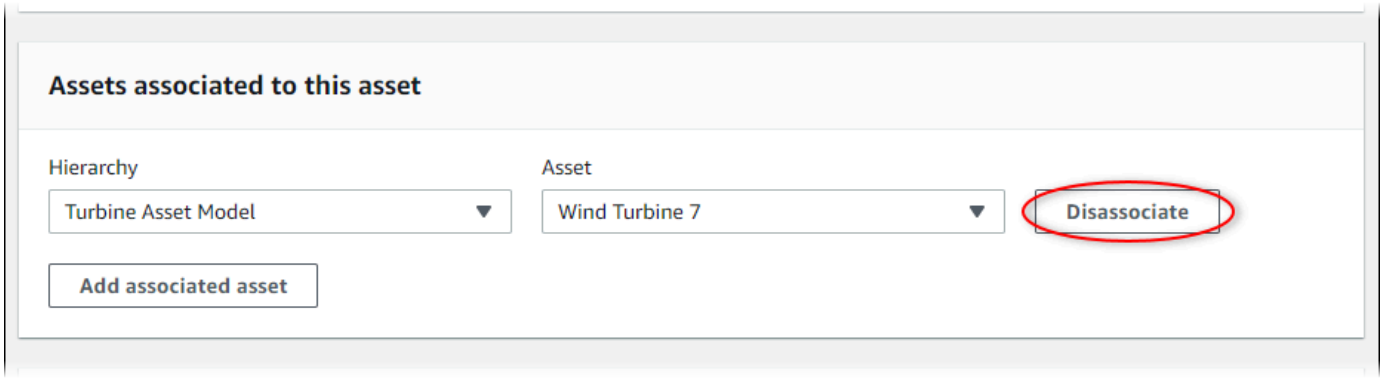
6. Per Gerarchia, scegli la gerarchia che definisce la relazione tra l'asset padre e l'asset figlio.
7. Per Asset, scegli l'asset figlio da associare.
8. Selezionare Salva.

Per annullare l'associazione di un asset (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Asset.
3. Scegli l'asset padre per cui vuoi annullare l'associazione di un asset figlio.

> **Tip**
>
> Puoi scegliere l'icona a forma di freccia per espandere una gerarchia di asset e trovare il tuo asset.

4. Scegli Modifica.
5. In Asset associati a questo asset scegli Annulla associazione.



6. Selezionare Salva.

Associazione e dissociazione delle risorse ()AWS CLI

È possibile utilizzare AWS Command Line Interface (AWS CLI) per associare e dissociare gli asset.

Per questa procedura, devi conoscere l'ID della gerarchia (`hierarchyId`) presente nel modello di asset padre che definisce la relazione con il modello di asset figlio. Utilizzate l'DescribeAssetoperazione per trovare l'ID della gerarchia nella risposta.

Per trovare un ID gerarchia

- Esegui il comando seguente per descrivere l'asset padre. Sostituisci *`parent-asset-id`*con l'ID o l'ID esterno della risorsa principale.

  ```
  aws iotsitewise describe-asset --asset-id parent-asset-id
  ```

  L'operazione restituisce una risposta contenente i dettagli dell'asset. La risposta contiene un `assetHierarchies` elenco con la seguente struttura:

  ```
  {
    ...
    "assetHierarchies": [
      {
        "id": "String",
        "name": "String"
      }
    ],
    ...
  }
  ```

  L'ID gerarchia è il valore `id` di una gerarchia nell'elenco delle gerarchie di asset.

Una volta ottenuto l'ID gerarchia puoi associare o annullare l'associazione di un asset alla gerarchia.

Per associare una risorsa secondaria a una risorsa principale, utilizzate l'AssociateAssetsoperazione. Per dissociare una risorsa secondaria da una risorsa principale, utilizzate l'DisassociateAssetsoperazione. Specifica i seguenti parametri, che sono gli stessi per entrambe le operazioni:

- `assetId`— L'ID o l'ID esterno della risorsa principale.
- `hierarchyId`— L'ID della gerarchia o l'ID esterno nella risorsa principale.
- `childAssetId`— L'ID o l'ID esterno della risorsa secondaria.

Per associare una risorsa (AWS CLI)

- Esegui il comando seguente per associare un asset figlio a un asset padre. Replace *`parent-asset-id`*, *`hierarchy-id`* e *`child-asset-id`*con i rispettivi ID:

```
aws iotsitewise associate-assets \
  --asset-id parent-asset-id \
  --hierarchy-id hierarchy-id \
  --child-asset-id child-asset-id
```

Per dissociare un asset ()AWS CLI

- Esegui il comando seguente per annullare l'associazione di un asset figlio a un asset padre. Replace *`parent-asset-id`*, *`hierarchy-id`* e *`child-asset-id`*con i rispettivi ID:

```
aws iotsitewise disassociate-assets \
  --asset-id parent-asset-id \
  --hierarchy-id hierarchy-id \
  --child-asset-id child-asset-id
```

Aggiornamento di asset e modelli

È possibile aggiornare gli asset, i modelli di asset e i modelli dei componenti AWS IoT SiteWise per modificarne i nomi e le definizioni. Queste operazioni di aggiornamento sono asincrone e richiedono tempo per essere propagate. AWS IoT SiteWise Controllate lo stato della risorsa o del modello prima di apportare ulteriori modifiche. È necessario attendere la propagazione delle modifiche prima di poter continuare a utilizzare l'asset o il modello aggiornato.

Argomenti

Aggiornamento degli asset

Puoi utilizzare la AWS IoT SiteWise console o l'API per aggiornare il nome di una risorsa.

Quando aggiorni una risorsa, lo stato della risorsa rimane invariato `UPDATING` fino alla propagazione delle modifiche. Per ulteriori informazioni, consulta Stati di asset e modelli.

Argomenti

- Aggiornamento di un asset (console)
- Aggiornamento di una risorsa (AWS CLI)

Aggiornamento di un asset (console)

Puoi utilizzare la AWS IoT SiteWise console per aggiornare i dettagli della risorsa.

Per aggiornare un asset (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Asset.
3. Scegli l'asset da aggiornare.

   > **Tip**
   >
   > Puoi scegliere l'icona a forma di freccia per espandere una gerarchia di asset e trovare il tuo asset.

4. Scegli Modifica.
5. Aggiorna il nomedell'asset.
6. (Facoltativo) In questa pagina aggiorna altre informazioni relative all'asset. Per ulteriori informazioni, consulta gli argomenti seguenti:
   - Mappatura dei flussi di dati industriali alle proprietà degli asset
   - Aggiornamento dei valori degli attributi
   - Interazione con altri servizi AWS
7. Selezionare Salva.

Aggiornamento di una risorsa (AWS CLI)

Puoi usare il AWS Command Line Interface (AWS CLI) per aggiornare il nome di una risorsa.

Utilizzate l'UpdateAssetoperazione per aggiornare una risorsa. Specifica i seguenti parametri:

- `assetId`— L'ID della risorsa. Questo è l'ID effettivo in formato UUID, o `externalId:myExternalId` se ne ha uno. Per ulteriori informazioni, consulta Riferimento a oggetti con ID esterni nella Guida per l'utente di AWS IoT SiteWise .
- `assetName`— Il nuovo nome della risorsa.

Per aggiornare il nome di una risorsa (AWS CLI)

- Esegui il comando seguente per aggiornare il nome di un asset. Sostituisci *`asset-id`* con l'ID o l'ID esterno della risorsa. Aggiorna il nome dell'*`asset con il nuovo nome`* dell'asset.

```
aws iotsitewise update-asset \
  --asset-id asset-id \
  --asset-name asset-name
```

Aggiornamento dei modelli di asset e dei modelli dei componenti

È possibile utilizzare la AWS IoT SiteWise console o l'API per aggiornare un modello di asset o un modello di componente.

Non puoi modificare il tipo o il tipo di dati di una proprietà esistente o la finestra di una metrica esistente. Inoltre, non è possibile modificare il tipo di modello da modello di asset a modello di componenti o viceversa.

> **Important**
>
> - Se rimuovete una proprietà da un modello di asset o da un modello di componente, AWS IoT SiteWise elimina tutti i dati precedenti relativi a quella proprietà. Per quanto riguarda i modelli a componenti, ciò influisce su tutti i modelli di asset che utilizzano quel modello di componenti, quindi prestate particolare attenzione a capire in che misura la modifica può essere applicata.

- Se rimuovete una definizione di gerarchia da un modello di asset, AWS IoT SiteWise dissocia tutti gli asset in quella gerarchia.

Quando aggiorni un modello, anche gli asset basati su quel modello assimilano le modifiche apportate. Fino a quando le modifiche non si propagano, ogni asset ha lo stato `UPDATING`. È necessario attendere fino a quando gli asset ritornano nello stato `ACTIVE` prima di poter interagire con loro. In questo lasso di tempo, lo stato del modello di asset aggiornato sarà `PROPAGATING`.

Quando aggiornate un modello di componente, ogni modello di asset che incorpora quel modello di componente riflette le modifiche. Fino a quando le modifiche al modello di componente non si propagano, ogni modello di asset interessato presenta `UPDATING` lo stato, seguito dall'`PROPAGATING`aggiornamento degli asset associati, come descritto nel paragrafo precedente. È necessario attendere che tali modelli di asset tornino allo `ACTIVE` stato precedente prima di interagire con essi. Durante questo periodo, lo stato del modello di componente aggiornato sarà`PROPAGATING`.

Per ulteriori informazioni, consulta Stati di asset e modelli.

Argomenti

- Aggiornamento di un modello di asset o componente (console)
- Aggiornamento di un modello di asset o componente ()AWS CLI

Aggiornamento di un modello di asset o componente (console)

È possibile utilizzare la AWS IoT SiteWise console per aggiornare un modello di asset o un modello di componente.

Per aggiornare un modello di asset o un modello di componente (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione selezionare Models (Modelli).
3. Scegliete il modello di asset o il modello di componente da aggiornare.
4. Scegli Modifica.
5. Nella pagina Modifica modello esegui una delle operazioni seguenti:
   - In Dettagli del modello modifica il nome del modello.
   - Modifica una delle definizioni degli attributi. Non è possibile modificare il tipo di dati degli attributi esistenti. Per ulteriori informazioni, consulta Definizione di dati statici (attributi).

- Modifica una delle definizioni di misurazione. Non è possibile modificare il tipo di dati delle misurazioni esistenti. Per ulteriori informazioni, consulta Definizione dei flussi di dati provenienti dalle apparecchiature (misurazioni).
- Modifica una delle definizioni di trasformazione. Per ulteriori informazioni, consulta Trasformazione dei dati (trasformazioni).
- Modifica una delle definizioni di parametro. Non è possibile modificare l'intervallo di tempo dei parametri esistenti. Per ulteriori informazioni, consulta Aggregazione di dati da proprietà e altre risorse (metriche).
- (Solo modelli di asset) Modificate una qualsiasi definizione della gerarchia. Non è possibile modificare il modello di gerarchia delle gerarchie esistenti. Per ulteriori informazioni, consulta Definizione delle gerarchie dei modelli di asset.

6. Seleziona Save (Salva.

Aggiornamento di un modello di asset o componente ()AWS CLI

È possibile utilizzare AWS Command Line Interface (AWS CLI) per aggiornare un modello di asset o un modello di componente.

Utilizzate l'UpdateAssetModelAPI per aggiornare il nome, la descrizione e le proprietà di un modello di asset o di un modello di componente. Solo per i modelli di asset, puoi aggiornare le gerarchie. Specifica i seguenti parametri:

- `assetModelId`— L'ID della risorsa. Questo è l'ID effettivo in formato UUID, o `externalId:myExternalId` se ne ha uno. Per ulteriori informazioni, consulta Riferimento a oggetti con ID esterni nella Guida per l'utente di AWS IoT SiteWise .

Specificate il modello aggiornato nel payload. Per maggiori informazioni sul formato previsto di un modello di asset o di un modello di componente, consultaCreazione dei modelli di asset.

> **Warning**
>
> L'UpdateAssetModelAPI sovrascrive il modello esistente con il modello fornito nel payload. Per evitare di eliminare le proprietà o le gerarchie del modello, è necessario includerne gli ID e le definizioni nel payload del modello aggiornato. Per informazioni su come interrogare la struttura esistente del modello, consultate l'operazione. DescribeAssetModel

> **Note**
>
> La procedura seguente può aggiornare solo modelli compositi di tipo`AWS/ALARM`. Se desideri aggiornare i modelli `CUSTOM` compositi, usa UpdateAssetModelCompositeModelinvece. Per ulteriori informazioni, consulta Aggiornamento di modelli compositi personalizzati (Componenti).

Per aggiornare un modello di asset o un modello di componente (AWS CLI)

1. Eseguite il comando seguente per recuperare la definizione del modello esistente. *asset-model-id*Sostituitelo con l'ID o l'ID esterno del modello di asset o del modello di componente da aggiornare.

   ```
   aws iotsitewise describe-asset-model --asset-model-id asset-model-id
   ```

   L'operazione restituisce una risposta che contiene i dettagli del modello. La risposta ha la seguente struttura.

   ```
   {
     "assetModelId": "String",
     "assetModelArn": "String",
     "assetModelName": "String",
     "assetModelDescription": "String",
     "assetModelProperties": Array of AssetModelProperty,
     "assetModelHierarchies": Array of AssetModelHierarchyDefinition,
     "assetModelCompositeModels": Array of AssetModelCompositeModel,
     "assetModelCompositeModelSummaries": Array of AssetModelCompositeModelSummary,
     "assetModelCreationDate": "String",
     "assetModelLastUpdateDate": "String",
     "assetModelStatus": {
       "state": "String",
       "error": {
         "code": "String",
         "message": "String"
       },
     "assetModelType": "String"
     }
   }
   ```

Per ulteriori informazioni, vedete l'DescribeAssetModeloperazione.

2. Crea un file denominato `update-asset-model.json` e copia la risposta del comando precedente nel file.
3. Rimuovi le seguenti coppie chiave-valore dall'oggetto JSON in `update-asset-model.json`:

   - `assetModelId`
   - `assetModelArn`
   - `assetModelCompositeModelSummaries`
   - `assetModelCreationDate`
   - `assetModelLastUpdateDate`
   - `assetModelStatus`
   - `assetModelType`

   L'UpdateAssetModeloperazione prevede un carico utile con la seguente struttura:

   ```
   {
     "assetModelName": "String",
     "assetModelDescription": "String",
     "assetModelProperties": Array of AssetModelProperty,
     "assetModelHierarchies": Array of AssetModelHierarchyDefinition,
     "assetModelCompositeModels": Array of AssetModelCompositeModel
   }
   ```

4. In `update-asset-model.json`, effettua una delle seguenti operazioni:

   - Modifica il nome del modello di asset (`assetModelName`).
   - Modifica, aggiungi o rimuovi la descrizione del modello di asset (`assetModelDescription`).
   - Modifica, aggiungi o rimuovi qualsiasi proprietà del modello di asset (`assetModelProperties`). Non è possibile modificare l'elemento `dataType` delle proprietà esistenti o l'elemento `window` dei parametri esistenti. Per ulteriori informazioni, consulta Definizione delle proprietà dei dati.
   - Modifica, aggiungi o rimuovi una delle gerarchie del modello di asset (`assetModelHierarchies`). Non è possibile modificare l'elemento `childAssetModelId` delle gerarchie esistenti. Per ulteriori informazioni, consulta Definizione delle gerarchie dei modelli di asset.

- Modifica, aggiungi o rimuovi uno qualsiasi dei modelli compositi di type `AWS/ALARM` () `assetModelCompositeModels` del modello di asset. Gli allarmi monitorano altre proprietà in modo da poter identificare quando le apparecchiature o i processi richiedono attenzione. Ogni definizione di allarme è un modello composito che standardizza l'insieme di proprietà utilizzate dall'allarme. Per ulteriori informazioni, consulta Monitoraggio dei dati con allarmi e Definizione degli allarmi sui modelli di asset.

5. Esegui il comando seguente per aggiornare il modello di asset con la definizione memorizzata in `update-asset-model.json`. Sostituisci *`asset-model-id`*con l'ID del modello di asset:

```
aws iotsitewise update-asset-model \
  --asset-model-id asset-model-id \
  --cli-input-json file://model-payload.json
```

Aggiornamento di modelli compositi personalizzati (Componenti)

È possibile utilizzare l' AWS IoT SiteWise API per aggiornare un modello composito personalizzato o la AWS IoT SiteWise console per aggiornare i componenti.

Argomenti

- Aggiornamento di un componente (console)
- Aggiornamento di un modello composito personalizzato (AWS CLI)

Aggiornamento di un componente (console)

È possibile utilizzare la AWS IoT SiteWise console per aggiornare un componente.

Per aggiornare un componente (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione selezionare Models (Modelli).
3. Scegliete il modello di asset in cui si trova il componente.
4. Nella scheda Proprietà, scegliete Componenti.
5. Scegliete il componente che desiderate aggiornare.
6. Scegli Modifica.
7. Nella pagina Modifica componente, effettuate una delle seguenti operazioni:

- In Dettagli del modello modifica il nome del modello.
- Modifica una delle definizioni degli attributi. Non è possibile modificare il tipo di dati degli attributi esistenti. Per ulteriori informazioni, consulta Definizione di dati statici (attributi).
- Modifica una delle definizioni di misurazione. Non è possibile modificare il tipo di dati delle misurazioni esistenti. Per ulteriori informazioni, consulta Definizione dei flussi di dati provenienti dalle apparecchiature (misurazioni).
- Modifica una delle definizioni di trasformazione. Per ulteriori informazioni, consulta Trasformazione dei dati (trasformazioni).
- Modifica una delle definizioni di parametro. Non è possibile modificare l'intervallo di tempo dei parametri esistenti. Per ulteriori informazioni, consulta Aggregazione di dati da proprietà e altre risorse (metriche).

8. Seleziona Save (Salva.

Aggiornamento di un modello composito personalizzato (AWS CLI)

È possibile utilizzare AWS Command Line Interface (AWS CLI) per aggiornare un modello composito personalizzato.

Per aggiornare il nome o la descrizione, utilizzate l'UpdateAssetModelCompositeModeloperazione. Solo per i modelli compositi personalizzati in linea, puoi anche aggiornare le proprietà. Non è possibile aggiornare le proprietà di un modello composito component-model-based personalizzato, poiché il modello di componente a cui fa riferimento fornisce le proprietà associate.

> **Important**
>
> Se rimuovete una proprietà da un modello composito personalizzato, AWS IoT SiteWise elimina tutti i dati precedenti relativi a quella proprietà. Non è possibile modificare il tipo o il tipo di dati di una proprietà esistente.
> Per sostituire una proprietà esistente del modello composito con una nuova con la stessa proprietà`name`, procedi come segue:
>
> 1. Inviate una `UpdateAssetModelCompositeModel` richiesta con l'intera proprietà esistente rimossa.
> 2. Invia una seconda `UpdateAssetModelCompositeModel` richiesta che includa la nuova proprietà. La nuova proprietà dell'asset avrà la `name` stessa di quella precedente e AWS IoT SiteWise genererà una nuova proprietà univoca`id`.

Per aggiornare un modello composito personalizzato (AWS CLI)

1. Per recuperare la definizione del modello composito esistente, eseguite il comando seguente. Sostituitelo *composite-model-id*con l'ID o l'ID esterno del modello composito personalizzato da aggiornare e *asset-model-id*con il modello di asset a cui è associato il modello composito personalizzato. Per ulteriori informazioni, consultate la Guida AWS IoT SiteWise per l'utente.

   ```
   aws iotsitewise describe-asset-model-composite-model \
   --asset-model-composite-model-id composite-model-id \
   --asset-model-id asset-model-id
   ```

   Per ulteriori informazioni, vedere l'DescribeAssetModelCompositeModeloperazione.

2. Crea un file chiamatoupdate-custom-composite-model.json, quindi copia la risposta del comando precedente nel file.

3. Rimuovi ogni coppia chiave-valore dall'oggetto JSON ad update-custom-composite-model.json eccezione dei seguenti campi:

   - assetModelCompositeModelName
   - assetModelCompositeModelDescription(se presente)
   - assetModelCompositeModelProperties(se presente)

4. In update-custom-composite-model.json, effettua una delle seguenti operazioni:

   - Modificare il valore diassetModelCompositeModelName.
   - Aggiungi o assetModelCompositeModelDescription rimuovi o modificane il valore.
   - Solo per i modelli compositi personalizzati in linea: modifica, aggiungi o rimuovi qualsiasi proprietà del modello di asset inassetModelCompositeModelProperties.

   Per ulteriori informazioni sul formato richiesto per questo file, consultate la sintassi della richiesta per. UpdateAssetModelCompositeModel

5. Eseguite il comando seguente per aggiornare il modello composito personalizzato con la definizione memorizzata inupdate-custom-composite-model.json. Sostituiscilo *composite-model-id*con l'ID del modello composito e *asset-model-id*con l'ID del modello di asset in cui si trova.

   ```
   aws iotsitewise update-asset-model-composite-model \
   --asset-model-composite-model-id composite-model-id \
   ```

```
--asset-model-id asset-model-id \
--cli-input-json file://update-custom-composite-model.json
```

Eliminazione di asset e modelli

Puoi eliminare le tue risorse e i tuoi modelli una AWS IoT SiteWise volta che hai finito di utilizzarli. Le operazioni di eliminazione sono asincrone e richiedono tempo per essere propagate. AWS IoT SiteWise

Argomenti

- Eliminazione degli asset
- Eliminazione dei modelli di asset

Eliminazione degli asset

Puoi utilizzare la AWS IoT SiteWise console o l'API per eliminare una risorsa.

Prima di eliminare un asset, è necessario innanzitutto annullare l'associazione degli asset figlio all'asset padre. Per ulteriori informazioni, consulta Associazione e annullamento dell'associazione degli asset. Se utilizzate il AWS Command Line Interface (AWS CLI), potete utilizzare l'ListAssociatedAssetsoperazione per elencare i figli di una risorsa.

Quando elimini un asset, lo stato dell'asset è `DELETING` fino a quando le modifiche non vengono propagate. Per ulteriori informazioni, consulta Stati di asset e modelli. Non è possibile eseguire query su un asset eliminato. Se lo facessi, l'API restituirebbe una risposta HTTP 404.

> **Important**
>
> AWS IoT SiteWise elimina tutti i dati delle proprietà degli asset eliminati.

Argomenti

- Eliminazione di un asset (console)
- Eliminazione di una risorsa ()AWS CLI

Eliminazione di un asset (console)

È possibile utilizzare la AWS IoT SiteWise console per eliminare una risorsa.

Per eliminare un asset (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Asset.
3. Scegli l'asset da eliminare.

   > **Tip**
   >
   > Puoi scegliere l'icona a forma di freccia per espandere una gerarchia di asset e trovare il tuo asset.

4. Se l'asset ha asset associati, elimina ogni asset associato. Puoi scegliere il nome di un asset per aprire la relativa pagina in cui è possibile eliminarlo.
5. Nella pagina dell'asset, scegli Elimina.
6. Nella finestra di dialogo Elimina risorsa, effettuate le seguenti operazioni:

   a. Immetti **`Delete`** per confermare l'eliminazione.

   b. Scegli Elimina.

Eliminazione di una risorsa ()AWS CLI

È possibile utilizzare AWS Command Line Interface (AWS CLI) per eliminare una risorsa.

Utilizzate l'DeleteAssetoperazione per eliminare una risorsa. Specifica il parametro seguente:

- `assetId`— L'ID della risorsa. Questo è l'ID effettivo in formato UUID, o `externalId:myExternalId` se ne ha uno. Per ulteriori informazioni, consulta Riferimento a oggetti con ID esterni nella Guida per l'utente di AWS IoT SiteWise .

Per eliminare una risorsa ()AWS CLI

1. Esegui il comando seguente per elencare le gerarchie dell'asset. Sostituisci *`asset-id`* con l'ID o l'ID esterno dell'asset:

```
aws iotsitewise describe-asset --asset-id asset-id
```

L'operazione restituisce una risposta contenente i dettagli dell'asset. La risposta contiene un `assetHierarchies` elenco con la seguente struttura:

```
{
  ...
  "assetHierarchies": [
    {
      "id": "String",
      "name": "String"
    }
  ],
  ...
}
```

Per ulteriori informazioni, vedere l'DescribeAssetoperazione.

2. Per ogni gerarchia, esegui il comando seguente per elencare gli elementi figlio dell'asset associati alla gerarchia. Sostituisci *asset-id* con l'ID o l'ID esterno dell'asset e *hierarchy-id con l'ID* o l'ID esterno della gerarchia.

```
aws iotsitewise list-associated-assets \
  --asset-id asset-id \
  --hierarchy-id hierarchy-id
```

Per ulteriori informazioni, vedete l'operazione. ListAssociatedAssets

3. Esegui il comando seguente per eliminare ogni asset associato e quindi eliminare l'asset. Sostituisci *asset-id* con l'ID o l'ID esterno della risorsa.

```
aws iotsitewise delete-asset --asset-id asset-id
```

Eliminazione dei modelli di asset

È possibile utilizzare la AWS IoT SiteWise console o l'API per eliminare un modello di asset.

Prima di poter eliminare un modello di asset, è necessario eliminare tutte le risorse che sono state create dal modello di asset.

Quando elimini un modello di asset, lo stato del modello di asset è `DELETING` fino a quando le modifiche non vengono propagate. Per ulteriori informazioni, consulta Stati di asset e modelli. Non è possibile eseguire query su un modello di asset eliminato. Se lo facessi, l'API restituirebbe una risposta HTTP 404.

Argomenti

- Eliminazione di un modello di asset (console)
- Eliminazione di un modello di asset ()AWS CLI

Eliminazione di un modello di asset (console)

È possibile utilizzare la AWS IoT SiteWise console per eliminare un modello di asset.

Per eliminare un modello di asset (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione selezionare Models (Modelli).
3. Scegli il modello di asset da eliminare.
4. Se il modello include asset, elimina ogni asset. Scegli il nome di un asset per aprire la relativa pagina in cui è possibile eliminarlo. Per ulteriori informazioni, consulta Eliminazione di un asset (console).
5. Nella pagina del modello, scegli Elimina.
6. Nella finestra di dialogo Elimina modello, effettuate le seguenti operazioni:
   a. Immetti **`Delete`** per confermare l'eliminazione.
   b. Scegli Elimina.

Eliminazione di un modello di asset ()AWS CLI

È possibile utilizzare AWS Command Line Interface (AWS CLI) per eliminare un modello di asset.

Utilizzate l'DeleteAssetModeloperazione per eliminare un modello di asset. Specifica il parametro seguente:

- `assetModelId`— L'ID della risorsa. Questo è l'ID effettivo in formato UUID, o `externalId:myExternalId` se ne ha uno. Per ulteriori informazioni, consulta Riferimento a oggetti con ID esterni nella Guida per l'utente di AWS IoT SiteWise .

Per eliminare un modello di asset ()AWS CLI

1. Esegui il comando seguente per elencare tutti gli asset creati dal modello. *asset-model-id*Sostituitelo con l'ID o l'ID esterno del modello di asset.

   ```
   aws iotsitewise list-assets --asset-model-id asset-model-id
   ```

   Per ulteriori informazioni, vedete l'ListAssetsoperazione.

2. Se il comando precedente restituisce asset dal modello, elimina ogni asset. Per ulteriori informazioni, consulta Eliminazione di una risorsa ()AWS CLI.

3. Esegui il comando seguente per eliminare il modello di asset. Sostituisci *asset-model-id*con l'ID o l'ID esterno del modello di asset.

   ```
   aws iotsitewise delete-asset-model --asset-model-id asset-model-id
   ```

Operazioni in blocco con risorse e modelli

Per lavorare con un gran numero di asset o modelli di asset, utilizzate le operazioni in blocco per importare ed esportare in massa le risorse in una posizione diversa. Ad esempio, puoi creare un file di dati che definisce asset o modelli di asset in un bucket Amazon S3 e utilizzare l'importazione in blocco per crearli o aggiornarli. AWS IoT SiteWise In alternativa, se disponi di un gran numero di asset o modelli di asset AWS IoT SiteWise, puoi esportarli in Amazon S3.

> **Note**
>
> Puoi eseguire operazioni di massa AWS IoT SiteWise chiamando le operazioni nell' AWS IoT TwinMaker API. Puoi farlo senza configurare AWS IoT TwinMaker o creare un' AWS IoT TwinMaker area di lavoro. Tutto ciò di cui hai bisogno è un bucket Amazon S3 in cui inserire i tuoi contenuti. AWS IoT SiteWise

Argomenti

- Concetti e terminologia chiave
- Funzionalità supportate
- Prerequisiti per le operazioni in blocco

- Esecuzione di un processo di importazione in blocco
- Esecuzione di un processo di esportazione in blocco
- Monitoraggio dell'avanzamento dei lavori e gestione degli errori
- Importa esempi di metadati
- Esporta esempi di metadati
- AWS IoT SiteWise schema del processo di trasferimento dei metadati

Concetti e terminologia chiave

AWS IoT SiteWise le funzionalità di importazione ed esportazione in blocco si basano sui seguenti concetti e terminologia:

- Importazione: l'azione di spostare risorse o modelli di asset da un file in un bucket Amazon S3 a. AWS IoT SiteWise
- Esportazione: l'azione di spostare risorse o modelli di asset AWS IoT SiteWise da un bucket Amazon S3.
- Fonte: la posizione di partenza da cui desideri spostare i contenuti.

  Ad esempio, un bucket Amazon S3 è una fonte di importazione ed AWS IoT SiteWise è una fonte di esportazione.
- Destinazione: la posizione desiderata in cui desideri spostare i tuoi contenuti.

  Ad esempio, un bucket Amazon S3 è una destinazione di esportazione ed AWS IoT SiteWise è una destinazione di importazione.
- AWS IoT SiteWise Schema: questo schema viene utilizzato per importare ed esportare metadati da. AWS IoT SiteWise
- Risorsa di primo livello: una AWS IoT SiteWise risorsa che è possibile creare o aggiornare singolarmente, ad esempio una risorsa o un modello di risorsa.
- Risorsa secondaria: una risorsa annidata all'interno di una AWS IoT SiteWise risorsa di primo livello. Gli esempi includono proprietà, gerarchie e modelli compositi.
- Metadati: informazioni chiave necessarie per importare o esportare correttamente le risorse. Esempi di metadati sono le definizioni degli asset e i modelli di asset.
- metadataTransferJob: L'oggetto creato durante l'esecuzione`CreateMetadataTransferJob`.

Funzionalità supportate

Questo argomento spiega cosa è possibile fare quando si esegue un'operazione in blocco. Le operazioni in blocco supportano le seguenti funzionalità:

- Creazione di risorse di primo livello: quando importate una risorsa o un modello di asset che non definisce un ID o il cui ID non corrisponde a quello di uno esistente, verrà creato come nuova risorsa.
- Sostituzione di risorse di primo livello: quando importate una risorsa o un modello di risorsa il cui ID corrisponde a uno già esistente, sostituirà la risorsa esistente.
- Creazione, sostituzione o eliminazione di sottorisorse: quando l'importazione sostituisce una risorsa di primo livello come una risorsa o un modello di risorsa, la nuova definizione sostituisce tutte le risorse secondarie, come proprietà, gerarchie o modelli compositi.

  Ad esempio, se aggiorni un modello di asset durante un'importazione in blocco e la versione aggiornata definisce una proprietà che non era presente nell'originale, viene creata una nuova proprietà. Se definisce una proprietà già esistente, la proprietà esistente verrà aggiornata. Se il modello di asset aggiornato omette una proprietà che era presente nell'originale, la proprietà viene eliminata.
- Nessuna eliminazione di risorse di primo livello: le operazioni in blocco non eliminano una risorsa o un modello di asset. Le operazioni in blocco si limitano a crearli o aggiornarli.

Prerequisiti per le operazioni in blocco

Questa sezione illustra i prerequisiti per le operazioni in blocco, incluse le autorizzazioni AWS Identity and Access Management (IAM) per lo scambio di risorse tra e il computer locale. Servizi AWS Prima di iniziare un'operazione in blocco, completa il seguente prerequisito:

- Crea un bucket Amazon S3 per archiviare le risorse. Per ulteriori informazioni sull'uso di Amazon S3, consulta Che cos'è Amazon S3?

Autorizzazioni IAM

Per eseguire operazioni in blocco, è necessario creare una policy AWS Identity and Access Management (IAM) con autorizzazioni che consentano lo scambio di AWS risorse tra Amazon S3 e il AWS IoT SiteWise computer locale. Per ulteriori informazioni sulla creazione di policy IAM, consulta la sezione relativa alla creazione delle policy IAM.

Per eseguire operazioni in blocco, sono necessarie le seguenti politiche.

AWS IoT SiteWise politica

Questa policy consente l'accesso alle azioni AWS IoT SiteWise API richieste per le operazioni in blocco:

```
{
    "Sid": "SiteWiseApiAccess",
    "Effect": "Allow",
    "Action": [
        "iotsitewise:CreateAsset",
        "iotsitewise:CreateAssetModel",
        "iotsitewise:UpdateAsset",
        "iotsitewise:UpdateAssetModel",
        "iotsitewise:UpdateAssetProperty",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssetProperties",
        "iotsitewise:ListAssetModelProperties",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeAssetProperty",
        "iotsitewise:AssociateAssets",
        "iotsitewise:DisassociateAssets",
        "iotsitewise:AssociateTimeSeriesToAssetProperty",
        "iotsitewise:DisassociateTimeSeriesFromAssetProperty",
        "iotsitewise:BatchPutAssetPropertyValue",
        "iotsitewise:BatchGetAssetPropertyValue",
        "iotsitewise:TagResource",
        "iotsitewise:UntagResource",
        "iotsitewise:ListTagsForResource",
        "iotsitewise:CreateAssetModelCompositeModel",
        "iotsitewise:UpdateAssetModelCompositeModel",
        "iotsitewise:DescribeAssetModelCompositeModel",
        "iotsitewise:DeleteAssetModelCompositeModel",
        "iotsitewise:ListAssetModelCompositeModels",
        "iotsitewise:ListCompositionRelationships",
        "iotsitewise:DescribeAssetCompositeModel"
    ],
    "Resource": "*"
}
```

AWS IoT TwinMaker politica

Questa politica consente l'accesso alle operazioni AWS IoT TwinMaker API utilizzate per lavorare con operazioni di massa:

```
{
    "Sid": "MetadataTransferJobApiAccess",
    "Effect": "Allow",
    "Action": [
        "iottwinmaker:CreateMetadataTransferJob",
        "iottwinmaker:CancelMetadataTransferJob",
        "iottwinmaker:GetMetadataTransferJob",
        "iottwinmaker:ListMetadataTransferJobs"
    ],
    "Resource": "*"
}
```

Politica di Amazon S3

Questa policy fornisce l'accesso ai bucket Amazon S3 per il trasferimento di metadati per operazioni di massa.

For a specific Amazon S3 bucket

Se utilizzi un bucket specifico per lavorare con i metadati delle tue operazioni di massa, questa policy fornisce l'accesso a quel bucket:

```
{
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:AbortMultipartUpload",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
    ],
    "Resource": [
        "arn:aws:s3:::bucket name",
        "arn:aws:s3:::bucket name/*"
    ]
```

```
}
```

To allow any Amazon S3 bucket

Se utilizzerai molti bucket diversi per lavorare con i metadati delle operazioni di massa, questa policy fornisce l'accesso a qualsiasi bucket:

```
{
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:AbortMultipartUpload",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
    ],
    "Resource": "*"
}
```

Per informazioni sulla risoluzione dei problemi relativi alle operazioni di importazione ed esportazione, consulta. Risoluzione dei problemi di importazione ed esportazione in blocco

Esecuzione di un processo di importazione in blocco

L'importazione in blocco è l'azione di spostare i metadati in un'area di lavoro. AWS IoT SiteWise Ad esempio, l'importazione in blocco può spostare i metadati da un file locale o da un file in un bucket Amazon S3 a un'area di lavoro. AWS IoT SiteWise

Passaggio 1: preparare il file da importare

Scaricate il file in formato AWS IoT SiteWise nativo per importare gli asset e i relativi modelli. Per ulteriori dettagli, consulta AWS IoT SiteWise schema del processo di trasferimento dei metadati.

Passaggio 2: carica il file preparato su Amazon S3

Carica il file su Amazon S3. Per ulteriori informazioni, consulta Caricamento di un file su Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service.

Importa metadati (console)

Puoi utilizzare il Console AWS IoT SiteWise per importare in blocco i metadati. Segui Passaggio 1: preparare il file da importare e Passaggio 2: carica il file preparato su Amazon S3 prepara un file pronto per essere importato.

Importa dati da Amazon S3 a Console AWS IoT SiteWise

1. Passare alla console AWS IoT SiteWise.
2. Scegli Bulk operations New dal pannello di navigazione.
3. Scegli Nuova importazione per avviare il processo di importazione.
4. Nella pagina Importa metadati:
   - Scegli Browse Amazon S3 per visualizzare il bucket e i file Amazon S3.
   - Passa al bucket Amazon S3 che contiene il file di importazione preparato.
   - Seleziona il file da importare.
   - Esaminate il file selezionato e scegliete Importa.
5. La pagina Operazioni in blocco sui SiteWise metadati di Console AWS IoT SiteWise mostra il processo di importazione appena creato nella tabella di avanzamento dei lavori.

Importa metadati ()AWS CLI

Per eseguire un'azione di importazione, utilizzate la procedura seguente:

Importa dati da Amazon S3 a AWS CLI

1. Crea un file di metadati che specifichi le risorse che desideri importare, seguendo il. AWS IoT SiteWise schema del processo di trasferimento dei metadati Archivia questo file nel tuo bucket Amazon S3.

   Per esempi di file di metadati da importare, consulta. Importa esempi di metadati
2. Ora create un file JSON con il corpo della richiesta. Il corpo della richiesta specifica l'origine e la destinazione del processo di trasferimento. Questo file è separato dal file del passaggio precedente. Assicurati di specificare il tuo bucket Amazon S3 come origine e `iotsitewise` come destinazione.

   L'esempio seguente mostra il corpo della richiesta:

```
{
      "metadataTransferJobId": "your-transfer-job-Id",
      "sources": [{
          "type": "s3",
          "s3Configuration": {
              "location": "arn:aws:s3:::your-S3-bucket-name/
your_import_metadata.json"
          }
      }],
      "destination": {
          "type": "iotsitewise"
      }
  }
```

3. Invoca il `CreateMetadataTransferJob` eseguendo il AWS CLI comando seguente. In questo esempio, viene denominato `createMetadataTransferJobExport.json` il file del corpo della richiesta del passaggio precedente.

   ```
   aws iottwinmaker create-metadata-transfer-job --region us-east-1 \
     --cli-input-json file://createMetadataTransferJobImport.json
   ```

   Questo creerà un processo di trasferimento dei metadati e inizierà il processo di trasferimento delle risorse selezionate.

Esecuzione di un processo di esportazione in blocco

L'esportazione in blocco è l'azione di spostare i metadati da un' AWS IoT SiteWise area di lavoro a un bucket Amazon S3.

Quando esegui un'esportazione in blocco dei tuoi AWS IoT SiteWise contenuti su Amazon S3, puoi specificare filtri per limitare i modelli e gli asset specifici che desideri esportare.

I filtri devono essere specificati in una `iotSiteWiseConfiguration` sezione all'interno della sezione delle fonti della richiesta JSON.

> **Note**
>
> Puoi includere più filtri nella tua richiesta. L'operazione in blocco esporterà modelli di asset e asset che corrispondono a uno qualsiasi dei filtri.

Se non fornite alcun filtro, l'operazione in blocco esporta tutti i modelli e gli asset degli asset.

Example corpo della richiesta con filtri

```
{
      "metadataTransferJobId": "your-transfer-job-id",
      "sources": [
       {
        "type": "iotsitewise",
        "iotSiteWiseConfiguration": {
          "filters": [
           {
              "filterByAssetModel": {
                  "assetModelId": "asset model ID"
              }
            },
            {
              "filterByAssetModel": {
                  "assetModelId": "asset model ID",
                  "includeAssets": true
              }
            },
            {
              "filterByAssetModel": {
                  "assetModelId": "asset model ID",
                  "includeOffspring": true
               }
             }
           ]
          }
        }
       ],
       "destination": {
          "type": "s3",
          "s3Configuration": {
            "location": "arn:aws:s3:::your-S3-bucket-location"
          }
      }
}
```

Esporta metadati (console)

La procedura seguente spiega l'azione di esportazione della console:

Creare un processo di esportazione in Console AWS IoT SiteWise

1. Passare alla console AWS IoT SiteWise.
2. Scegli Operazioni in blocco Nuove dal pannello di navigazione.
3. Scegli Nuova esportazione per avviare il processo di esportazione.
4. Nella pagina Esporta metadati:
   - Immettete un nome per il processo di esportazione. Questo è il nome usato per il file esportato nel tuo bucket Amazon S3.
   - Scegli le risorse da esportare, che imposta i filtri per il lavoro:
     - Esporta tutti gli asset e i modelli di asset. Utilizza i filtri sugli asset e sui modelli di asset.
     - Esporta risorse. Filtra in base alle tue risorse.
       - Seleziona la risorsa da utilizzare per il filtro di esportazione.
       - (Facoltativo) Aggiungete la progenie o il modello di asset associato.
     - Esporta modelli di asset. Filtra i tuoi modelli di asset.
       - Seleziona il modello di asset da utilizzare per il filtro di esportazione.
       - (Facoltativo) Aggiungi la progenie, l'asset associato o entrambi.
     - Seleziona Successivo.
   - Passa al bucket Amazon S3:
     - Scegli Browse Amazon S3 per visualizzare il bucket e i file Amazon S3.
     - Passa al bucket Amazon S3 in cui deve essere inserito il file.
     - Seleziona Successivo.
   - Controlla il processo di esportazione e scegli Esporta.
5. La pagina Operazioni in blocco sui SiteWise metadati di Console AWS IoT SiteWise mostra il processo di importazione appena creato nella tabella di avanzamento dei lavori.

Per i diversi modi di utilizzare i filtri durante l'esportazione dei metadati, consulta. Esporta esempi di metadati

Esporta metadati ()AWS CLI

La procedura seguente spiega l'azione di AWS CLI esportazione:

Esportazione di dati AWS IoT SiteWise da Amazon S3

1. Crea un file JSON con il corpo della richiesta. Il corpo della richiesta specifica l'origine e la destinazione del processo di trasferimento. L'esempio seguente mostra un esempio di corpo della richiesta:

```
{
    "metadataTransferJobId": "your-transfer-job-Id",
    "sources": [{
        "type": "iotsitewise"
    }],
    "destination": {
        "type": "s3",
        "s3Configuration": {
            "location": "arn:aws:s3:::your-S3-bucket-location"
        }
    }
}
```

   Assicurati di specificare il tuo bucket Amazon S3 come destinazione del processo di trasferimento dei metadati.

   > **Note**
   >
   > Questo esempio esporterà tutti i tuoi modelli e asset di asset. Per limitare l'esportazione a modelli o asset specifici, potete includere filtri nel corpo della richiesta. Per ulteriori informazioni sull'applicazione dei filtri di esportazione, consultaEsporta esempi di metadati.

2. Salva il file del corpo della richiesta da utilizzare nel passaggio successivo. In questo esempio, il file è denominato `createMetadataTransferJobExport.json`.
3. Invoca il `CreateMetadataTransferJob` eseguendo il seguente AWS CLI comando:

```
aws iottwinmaker create-metadata-transfer-job --region us-east-1 \
```

```
        --cli-input-json file://createMetadataTransferJobExport.json
```

Sostituisci il file JSON di input `createMetadataTransferJobExport.json` con il tuo nome del file di trasferimento.

Monitoraggio dell'avanzamento dei lavori e gestione degli errori

L'elaborazione di un processo di massa richiede tempo. Ogni processo viene elaborato nell'ordine di AWS IoT SiteWise ricezione della richiesta. Viene elaborato one-at-a-time per ogni account. Quando un lavoro viene completato, il successivo in coda avvia automaticamente l'elaborazione. AWS IoT SiteWise risolve i job in modo asincrono e aggiorna lo stato di ciascuno man mano che procede. Ogni processo ha un campo di stato che contiene lo stato della risorsa e un messaggio di errore, se applicabile.

Lo stato può avere uno dei seguenti valori:

- `VALIDATING`— Convalida del lavoro, incluso il formato del file inviato e il relativo contenuto.
- `PENDING`— Il lavoro è in coda. È possibile annullare i lavori in questo stato dalla AWS IoT SiteWise console, ma tutti gli altri stati continueranno fino alla fine.
- `RUNNING`— Elaborazione del lavoro. Sta creando e aggiornando risorse come definito dal file di importazione o esportando risorse in base ai filtri del processo di esportazione scelti. Se viene annullata, qualsiasi risorsa importata da questo lavoro non viene eliminata. Per ulteriori informazioni, consulta Verifica lo stato di avanzamento e i dettagli del lavoro (console).
- `CANCELLING`— Il lavoro viene annullato attivamente.
- `ERROR`— Una o più risorse non sono state elaborate. Consulta il rapporto dettagliato sul lavoro per ulteriori informazioni. Per ulteriori informazioni, consulta Controlla i dettagli dell'errore (console).
- `COMPLETED`— Job completato senza errori.
- `CANCELLED`— Il lavoro viene annullato e non è in coda. Se hai annullato un `RUNNING` lavoro, le risorse già importate da questo lavoro al momento dell'annullamento non vengono eliminate da. AWS IoT SiteWise

Argomenti

- Monitoraggio dei progressi dei lavori
- Ispeziona gli errori

Monitoraggio dei progressi dei lavori

Verifica lo stato di avanzamento e i dettagli del lavoro (console)

Visualizza Importa metadati (console) o Esporta metadati (console) avvia un lavoro collettivo.

Panoramica dello stato di avanzamento del lavoro nella AWS IoT SiteWise console:

1. Passare alla console AWS IoT SiteWise.
2. Scegli Operazioni in blocco Nuove dal pannello di navigazione.
3. La tabella di avanzamento dei lavori nella AWS IoT SiteWise console mostra l'elenco dei lavori eseguiti in blocco.
4. La colonna Job type descrive se si tratta di un processo di esportazione o importazione. Le colonne Data di importazione mostrano la data di inizio del processo.
5. La colonna Stato mostra lo stato del lavoro. È possibile selezionare un lavoro per visualizzarne i dettagli.
6. Il lavoro selezionato mostra Successo in caso di esito positivo o un elenco di errori se il lavoro non è riuscito. Per ogni tipo di risorsa viene inoltre visualizzata una descrizione dell'errore.

Panoramica dei dettagli del lavoro nella AWS IoT SiteWise console:

La tabella di avanzamento dei lavori nella AWS IoT SiteWise console mostra l'elenco dei lavori eseguiti in blocco.

1. Scegli un lavoro per visualizzare maggiori dettagli.
2. Per un processo di importazione, `Data source ARN` rappresenta la posizione Amazon S3 del file di importazione.
3. Per un processo di esportazione, `Data destination ARN` rappresenta la posizione Amazon S3 del file dopo l'esportazione.
4. Inoltre `StatusStatus reason`, fornisci ulteriori dettagli sul lavoro corrente. Per ulteriori dettagli, consulta Monitoraggio dell'avanzamento dei lavori e gestione degli errori.
5. `Queued position`Rappresenta la posizione del lavoro nella coda del processo. I lavori vengono elaborati uno alla volta. Una posizione in coda pari a 1 indica che il lavoro verrà elaborato successivamente.
6. La pagina dei dettagli dei lavori mostra anche i conteggi relativi allo stato di avanzamento dei lavori.

- I tipi di conteggio dell'avanzamento dei lavori sono:

  i. `Total resources`— Indica il numero totale di asset nel processo di trasferimento.

  ii. `Succeeded`— Indica il numero di asset trasferiti con successo durante il processo.

  iii. `Failed`— Indica il numero di asset che hanno avuto esito negativo durante il processo.

  iv. `Skipped`— Indica il numero di risorse che sono state ignorate durante il processo.

7. Uno stato del lavoro pari a `PENDING` o`VALIDATING`, visualizza tutti i conteggi relativi all'avanzamento dei lavori. – Ciò indica che i conteggi relativi allo stato di avanzamento dei lavori sono in fase di valutazione.
8. Uno stato del lavoro pari a `RUNNING` mostra il `Total resources` conteggio, il lavoro inviato per l'elaborazione. I conteggi dettagliati (`Succeeded`, `Failed`, e`Skipped`) si applicano alle risorse elaborate. La somma dei conteggi dettagliati è inferiore al `Total resources` conteggio, finché lo stato del lavoro non è `COMPLETED` o`ERROR`.
9. Se lo stato di un lavoro è `COMPLETED` o`ERROR`, il `Total resources` conteggio è uguale alla somma dei conteggi dettagliati (`Succeeded`, `Failed`, e). `Skipped`
10. Se lo stato di un lavoro è`ERROR`, consulta la tabella Job failures per i dettagli sugli errori e gli errori specifici. Per ulteriori dettagli, consulta Controlla i dettagli dell'errore (console).

Rivedi lo stato di avanzamento e i dettagli del lavoro ()AWS CLI

Dopo aver avviato un'operazione in blocco, puoi verificarne o aggiornarne lo stato utilizzando le seguenti azioni API:

- Per recuperare informazioni su un lavoro specifico, utilizza l'azione GetMetadataTransferJobAPI.

  Recupera informazioni con l'**`GetMetadataTransferJob`**API:

  1. Crea ed esegui un processo di trasferimento. Chiamata dell'API `GetMetadataTransferJob`.

     Example AWS CLI comando:

```
aws iottwinmaker get-metadata-transfer-job \
        --metadata-transfer-job-id your_metadata_transfer_job_id \
        --region your_region
```

2. L'`GetMetadataTransferJob`API restituisce un `MetadataTransferJobProgress` oggetto con i seguenti parametri:
   - successeededCount: indica il numero di risorse trasferite correttamente durante il processo.
   - FailedCount: indica il numero di asset che hanno avuto esito negativo durante il processo.
   - SkippedCount: indica il conteggio degli asset che sono stati ignorati durante il processo.
   - totalCount: indica il conteggio totale degli asset nel processo di trasferimento.

   Questi parametri indicano lo stato di avanzamento del lavoro. Se lo stato è`RUNNING`, aiutano a tenere traccia del numero di risorse ancora da elaborare.

   Se si verificano errori di convalida dello schema o se failedCount è maggiore o uguale a 1, lo stato di avanzamento del lavoro diventa. `ERROR` Un report di errore completo per il processo viene inserito nel tuo bucket Amazon S3. Per ulteriori dettagli, consulta Ispeziona gli errori.

- Per elencare i lavori correnti, utilizza l'azione ListMetadataTransferJobsAPI.

  Utilizza un file JSON per filtrare i lavori restituiti in base al loro stato corrente. Consultate la procedura seguente:

  1. Per specificare i filtri che desideri utilizzare, crea un file JSON AWS CLI di input. Vuoi usare:

     ```
     {
         "sourceType": "s3",
         "destinationType": "iottwinmaker",
         "filters": [{
             "state": "COMPLETED"
         }]
     }
     ```

     Per un elenco di `state` valori validi, consulta la Guida ListMetadataTransferJobsFilterdi riferimento dell'AWS IoT TwinMaker API.

  2. Utilizzate il file JSON come argomento nel seguente comando di AWS CLI esempio:

     ```
     aws iottwinmaker list-metadata-transfer-job --region your_region \
             --cli-input-json file://ListMetadataTransferJobsExample.json
     ```

- Per annullare un lavoro, utilizza l'azione CancelMetadataTransferJobAPI. Questa API annulla lo specifico processo di trasferimento dei metadati, senza influire sulle risorse già esportate o importate:

```
aws iottwinmaker cancel-metadata-transfer-job \
        --region your_region \
        --metadata-transfer-job-id job-to-cancel-id
```

Ispeziona gli errori

Controlla i dettagli dell'errore (console)

I dettagli dell'errore nella AWS IoT SiteWise console:

1. Passare alla console AWS IoT SiteWise.
2. Consulta la tabella di avanzamento dei lavori in blocco Console AWS IoT SiteWise per un elenco dei lavori eseguiti in blocco.
3. Seleziona un lavoro per visualizzarne i dettagli.
4. Se lo stato di un lavoro è `COMPLETED` o`ERROR`, il `Total resources` conteggio è uguale alla somma dei conteggi dettagliati (`Succeeded`+`Failed`, e`Skipped`).
5. Se lo stato di un lavoro è`ERROR`, consulta la tabella Job failures per i dettagli sugli errori e gli errori specifici.
6. La tabella Job failures mostra il contenuto del rapporto Job. Il `Resource type` campo indica la posizione dell'errore o degli errori, ad esempio:
   - Ad esempio, un errore di convalida nel `Resource type` campo indica che il modello di importazione e il formato del file dello schema dei metadati non corrispondono. `Bulk operations template` Per ulteriori informazioni, consulta AWS IoT SiteWise schema del processo di trasferimento dei metadati.
   - Un errore `Asset` nel `Resource type` campo indica che la risorsa non è stata creata a causa di un conflitto con un'altra risorsa. Per informazioni sugli errori e i conflitti relativi alle AWS IoT SiteWise risorse, consultate Errori comuni.

Controlla i dettagli dell'errore ()AWS CLI

Per gestire e diagnosticare gli errori prodotti durante un processo di trasferimento, vedete la seguente procedura sull'utilizzo dell'azione `GetMetadataTransferJob` API:

1. Dopo aver creato ed eseguito un processo di trasferimento, chiama GetMetadataTransferJob:

   ```
   aws iottwinmaker get-metadata-transfer-job \
           --metadata-transfer-job-id your_metadata_transfer_job_id \
           --region us-east-1
   ```

2. Una volta visualizzato lo stato del lavoro a cui rivolgitiCOMPLETED, puoi iniziare a verificare i risultati del lavoro.
3. Quando si chiamaGetMetadataTransferJob, restituisce un oggetto chiamato MetadataTransferJobProgress.

   L' MetadataTransferJobProgress oggetto contiene i seguenti parametri:

   - FailedCount: indica il numero di asset che hanno avuto esito negativo durante il processo di trasferimento.
   - SkippedCount: indica il numero di asset che sono stati ignorati durante il processo di trasferimento.
   - successeededCount: indica il numero di asset che hanno avuto successo durante il processo di trasferimento.
   - totalCount: indica il numero totale di asset coinvolti nel processo di trasferimento.
4. Inoltre, la chiamata API restituisce un elemento `reportUrl` che contiene un URL predefinito. Se la tua operazione di trasferimento presenta problemi che devi approfondire, visita questo URL.

Importa esempi di metadati

Questa sezione mostra come creare file di metadati per importare modelli di asset e risorse con un'unica operazione di importazione in blocco.

Esempio di importazione in blocco

È possibile importare molti modelli di asset e asset con un'unica operazione di importazione in blocco. L'esempio seguente mostra come creare un file di metadati a tale scopo.

In questo scenario di esempio, sono presenti diversi siti di lavoro che contengono robot industriali nelle celle di lavoro.

L'esempio definisce due modelli di asset:

- `RobotModel1`: Questo modello di asset rappresenta un particolare tipo di robot che avete nei vostri cantieri. Il robot ha una proprietà di misurazione,`Temperature`.
- `WorkCell`: Questo modello di asset rappresenta una raccolta di robot all'interno di uno dei vostri siti di lavoro. Il modello di asset definisce una gerarchia`robotHierarchyOEM1`, per rappresentare la relazione tra robot e celle di lavoro.

L'esempio definisce anche alcune risorse:

- `WorkCell1`: una cella di lavoro all'interno del sito di Boston
- `RobotArm123456`: un robot all'interno di quella cella di lavoro
- `RobotArm987654`: un altro robot all'interno di quella cella di lavoro

Il seguente file di metadati JSON definisce questi modelli e asset. L'esecuzione di un'importazione in blocco con questi metadati crea i modelli di asset e le risorse al loro interno AWS IoT SiteWise, comprese le relative relazioni gerarchiche.

File di metadati per l'importazione

```
{
    "assetModels": [
        {
            "assetModelExternalId": "Robot.OEM1.3536",
            "assetModelName": "RobotModel1",
            "assetModelProperties": [
                {
                    "dataType": "DOUBLE",
                    "externalId": "Temperature",
                    "name": "Temperature",
                    "type": {
                        "measurement": {
                            "processingConfig": {
                                "forwardingConfig": {
                                    "state": "ENABLED"
                                }
                            }
```

```
                    }
                },
                "unit": "fahrenheit"
            }
        ]
    },
    {
        "assetModelExternalId": "ISA95.WorkCell",
        "assetModelName": "WorkCell",
        "assetModelProperties": [],
        "assetModelHierarchies": [
            {
                "externalId": "workCellHierarchyWithOEM1Robot",
                "name": "robotHierarchyOEM1",
                "childAssetModelExternalId": "Robot.OEM1.3536"
            }
        ]
    }
],
"assets": [
    {
        "assetExternalId": "Robot.OEM1.3536.123456",
        "assetName": "RobotArm123456",
        "assetModelExternalId": "Robot.OEM1.3536"
    },
    {
        "assetExternalId": "Robot.OEM1.3536.987654",
        "assetName": "RobotArm987654",
        "assetModelExternalId": "Robot.OEM1.3536"
    },
    {
        "assetExternalId": "BostonSite.Area1.Line1.WorkCell1",
        "assetName": "WorkCell1",
        "assetModelExternalId": "ISA95.WorkCell",
        "assetHierarchies": [
            {
                "externalId": "workCellHierarchyWithOEM1Robot",
                "childAssetExternalId": "Robot.OEM1.3536.123456"
            },
            {
                "externalId": "workCellHierarchyWithOEM1Robot",
                "childAssetExternalId": "Robot.OEM1.3536.987654"
            }
        ]
```

```
        }
    ]
}
```

Esempio di onboarding iniziale di modelli e asset

In questo scenario di esempio, in un'azienda sono presenti diversi siti di lavoro che contengono robot industriali.

L'esempio definisce più modelli di asset:

- `Sample_Enterprise`— Questo modello di asset rappresenta la società di cui fanno parte i siti. Il modello di asset definisce una gerarchia per rappresentare la relazione tra i siti e l'azienda. `Enterprise to Site`
- `Sample_Site`— Questo modello di asset rappresenta i siti di produzione all'interno dell'azienda. Il modello di asset definisce una gerarchia`Site to Line`, per rappresentare la relazione tra le linee e il sito.
- `Sample_Welding Line`— Questo modello di asset rappresenta una linea di assemblaggio all'interno dei siti di lavoro. Il modello di asset definisce una gerarchia`Line to Robot`, per rappresentare la relazione tra i robot e la linea.
- `Sample_Welding Robot`— Questo modello di asset rappresenta un particolare tipo di robot nei vostri cantieri.

L'esempio definisce anche gli asset in base ai modelli di asset.

- `Sample_AnyCompany Motor`— Questa risorsa viene creata a partire da un modello di `Sample_Enterprise` asset.
- `Sample_Chicago`— Questa risorsa viene creata a partire da un modello di `Sample_Site` asset.
- `Sample_Welding Line 1`— Questa risorsa viene creata a partire da un modello di `Sample_Welding Line` asset.
- `Sample_Welding Robot 1`— Questa risorsa viene creata a partire da un modello di `Sample_Welding Robot` asset.
- `Sample_Welding Robot 2`— Questa risorsa viene creata a partire da un modello di `Sample_Welding Robot` asset.

Il seguente file di metadati JSON definisce questi modelli e risorse di asset. L'esecuzione di un'importazione in blocco con questi metadati crea i modelli di asset e le risorse al loro interno AWS IoT SiteWise, comprese le relative relazioni gerarchiche.

File JSON per integrare risorse e modelli da importare

```
{
    "assetModels": [
        {
            "assetModelExternalId": "External_Id_Welding_Robot",
            "assetModelName": "Sample_Welding Robot",
            "assetModelProperties": [
                {
                    "dataType": "STRING",
                    "externalId": "External_Id_Welding_Robot_Serial_Number",
                    "name": "Serial Number",
                    "type": {
                        "attribute": {
                            "defaultValue": "-"
                        }
                    },
                    "unit": "-"
                },
                {
                    "dataType": "DOUBLE",
                    "externalId": "External_Id_Welding_Robot_Cycle_Count",
                    "name": "CycleCount",
                    "type": {
                        "measurement": {}
                    },
                    "unit": "EA"
                },
                {
                    "dataType": "DOUBLE",
                    "externalId": "External_Id_Welding_Robot_Joint_1_Current",
                    "name": "Joint 1 Current",
                    "type": {
                        "measurement": {}
                    },
                    "unit": "Amps"
                },
                {
```

```
                    "dataType": "DOUBLE",
                    "externalId": "External_Id_Welding_Robot_Joint_1_Max_Current",
                    "name": "Max Joint 1 Current",
                    "type": {
                        "metric": {
                            "expression": "max(joint1current)",
                            "variables": [
                                {
                                    "name": "joint1current",
                                    "value": {
                                        "propertyExternalId":
"External_Id_Welding_Robot_Joint_1_Current"
                                    }
                                }
                            ],
                            "window": {
                                "tumbling": {
                                    "interval": "5m"
                                }
                            }
                        }
                    },
                    "unit": "Amps"
                }
            ]
        },
        {
            "assetModelExternalId": "External_Id_Welding_Line",
            "assetModelName": "Sample_Welding Line",
            "assetModelProperties": [
                {
                    "dataType": "DOUBLE",
                    "externalId": "External_Id_Welding_Line_Availability",
                    "name": "Availability",
                    "type": {
                        "measurement": {}
                    },
                    "unit": "%"
                }
            ],
            "assetModelHierarchies": [
                {
                    "externalId": "External_Id_Welding_Line_TO_Robot",
                    "name": "Line to Robot",
```

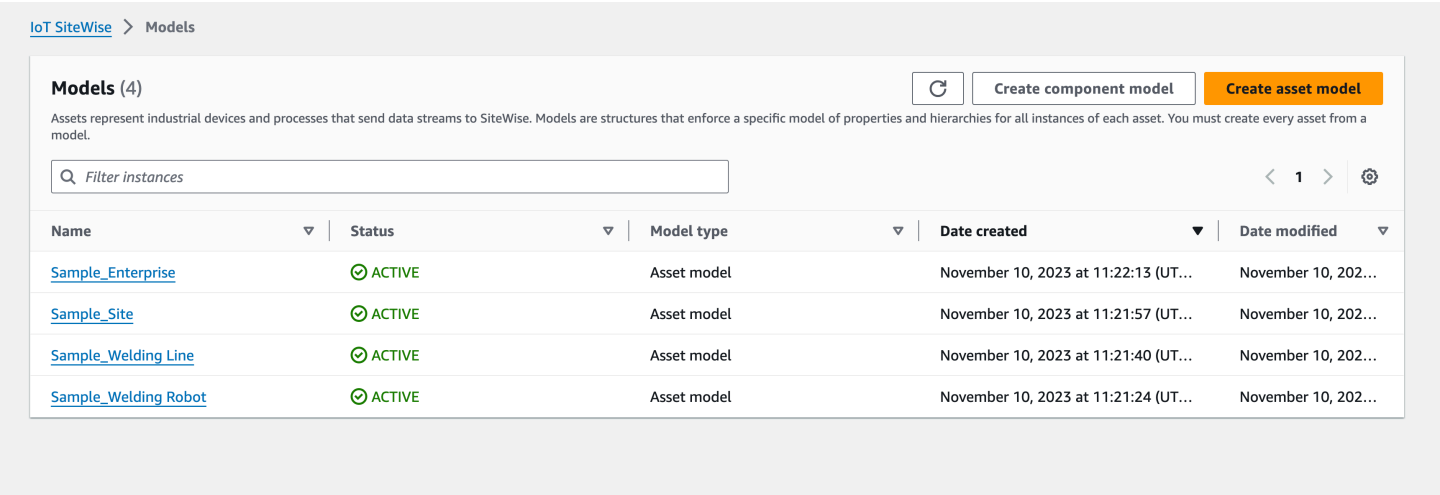
```
                "childAssetModelExternalId": "External_Id_Welding_Robot"
            }
        ]
    },
    {
        "assetModelExternalId": "External_Id_Site",
        "assetModelName": "Sample_Site",
        "assetModelProperties": [
            {
                "dataType": "STRING",
                "externalId": "External_Id_Site_Street_Address",
                "name": "Street Address",
                "type": {
                    "attribute": {
                        "defaultValue": "-"
                    }
                },
                "unit": "-"
            }
        ],
        "assetModelHierarchies": [
            {
                "externalId": "External_Id_Site_TO_Line",
                "name": "Site to Line",
                "childAssetModelExternalId": "External_Id_Welding_Line"
            }
        ]
    },
    {
        "assetModelExternalId": "External_Id_Enterprise",
        "assetModelName": "Sample_Enterprise",
        "assetModelProperties": [
            {
                "dataType": "STRING",
                "name": "Company Name",
                "externalId": "External_Id_Enterprise_Company_Name",
                "type": {
                    "attribute": {
                        "defaultValue": "-"
                    }
                },
                "unit": "-"
            }
        ],
```

```
            "assetModelHierarchies": [
                {
                    "externalId": "External_Id_Enterprise_TO_Site",
                    "name": "Enterprise to Site",
                    "childAssetModelExternalId": "External_Id_Site"
                }
            ]
        }
    ],
    "assets": [
        {
            "assetExternalId": "External_Id_Welding_Robot_1",
            "assetName": "Sample_Welding Robot 1",
            "assetModelExternalId": "External_Id_Welding_Robot",
            "assetProperties": [
                {
                    "externalId": "External_Id_Welding_Robot_Serial_Number",
                    "attributeValue": "S1000"
                },
                {
                    "externalId": "External_Id_Welding_Robot_Cycle_Count",
                    "alias": "AnyCompany/Chicago/Welding Line/S1000/Count"
                },
                {
                    "externalId": "External_Id_Welding_Robot_Joint_1_Current",
                    "alias": "AnyCompany/Chicago/Welding Line/S1000/1/Current"
                }
            ]
        },
        {
            "assetExternalId": "External_Id_Welding_Robot_2",
            "assetName": "Sample_Welding Robot 2",
            "assetModelExternalId": "External_Id_Welding_Robot",
            "assetProperties": [
                {
                    "externalId": "External_Id_Welding_Robot_Serial_Number",
                    "attributeValue": "S2000"
                },
                {
                    "externalId": "External_Id_Welding_Robot_Cycle_Count",
                    "alias": "AnyCompany/Chicago/Welding Line/S2000/Count"
                },
                {
                    "externalId": "External_Id_Welding_Robot_Joint_1_Current",
```

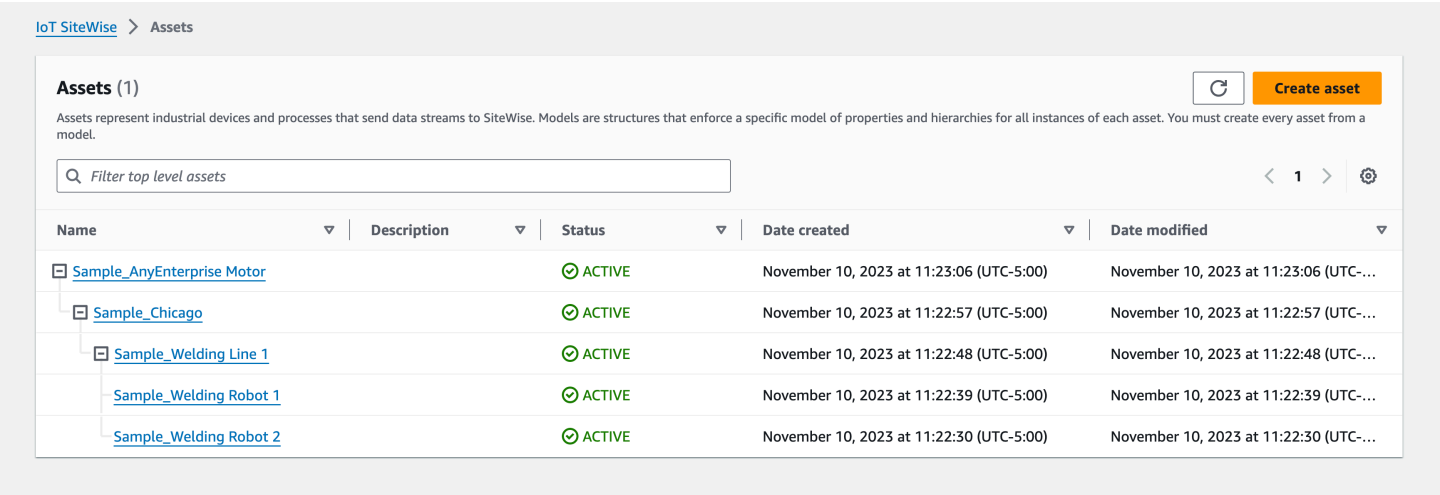
```
                    "alias": "AnyCompany/Chicago/Welding Line/S2000/1/Current"
                }
            ]
        },
        {
            "assetExternalId": "External_Id_Welding_Line_1",
            "assetName": "Sample_Welding Line 1",
            "assetModelExternalId": "External_Id_Welding_Line",
            "assetProperties": [
                {
                    "externalId": "External_Id_Welding_Line_Availability",
                    "alias": "AnyCompany/Chicago/Welding Line/Availability"
                }
            ],
            "assetHierarchies": [
                {
                    "externalId": "External_Id_Welding_Line_TO_Robot",
                    "childAssetExternalId": "External_Id_Welding_Robot_1"
                },
                {
                    "externalId": "External_Id_Welding_Line_TO_Robot",
                    "childAssetExternalId": "External_Id_Welding_Robot_2"
                }
            ]
        },
        {
            "assetExternalId": "External_Id_Site_Chicago",
            "assetName": "Sample_Chicago",
            "assetModelExternalId": "External_Id_Site",
            "assetHierarchies": [
                {
                    "externalId": "External_Id_Site_TO_Line",
                    "childAssetExternalId": "External_Id_Welding_Line_1"
                }
            ]
        },
        {
            "assetExternalId": "External_Id_Enterprise_AnyCompany",
            "assetName": "Sample_AnyEnterprise Motor",
            "assetModelExternalId": "External_Id_Enterprise",
            "assetHierarchies": [
                {
                    "externalId": "External_Id_Enterprise_TO_Site",
                    "childAssetExternalId": "External_Id_Site_Chicago"
```

```
                }
            ]
        }
    ]
}
```

La schermata seguente mostra i modelli visualizzati nell'esempio di codice precedente Console AWS IoT SiteWise dopo l'esecuzione del precedente esempio di codice.



La schermata seguente mostra i modelli, gli asset e le gerarchie visualizzati Console AWS IoT SiteWise dopo l'esecuzione del precedente esempio di codice.



Esempio di onboarding di risorse aggiuntive

Questo esempio definisce risorse aggiuntive da importare in un modello di asset esistente nel tuo account:

- `Sample_Welding Line 2`— Questa risorsa viene creata a partire da un modello di `Sample_Welding Line` asset.
- `Sample_Welding Robot 3`— Questa risorsa viene creata a partire da un modello di `Sample_Welding Robot` asset.
- `Sample_Welding Robot 4`— Questa risorsa viene creata a partire da un modello di `Sample_Welding Robot` asset.

Per creare le risorse iniziali per questo esempio, vedereEsempio di onboarding iniziale di modelli e asset.

Il seguente file di metadati JSON definisce questi modelli e asset di asset. L'esecuzione di un'importazione in blocco con questi metadati crea i modelli di asset e le risorse al loro interno AWS IoT SiteWise, comprese le relative relazioni gerarchiche.

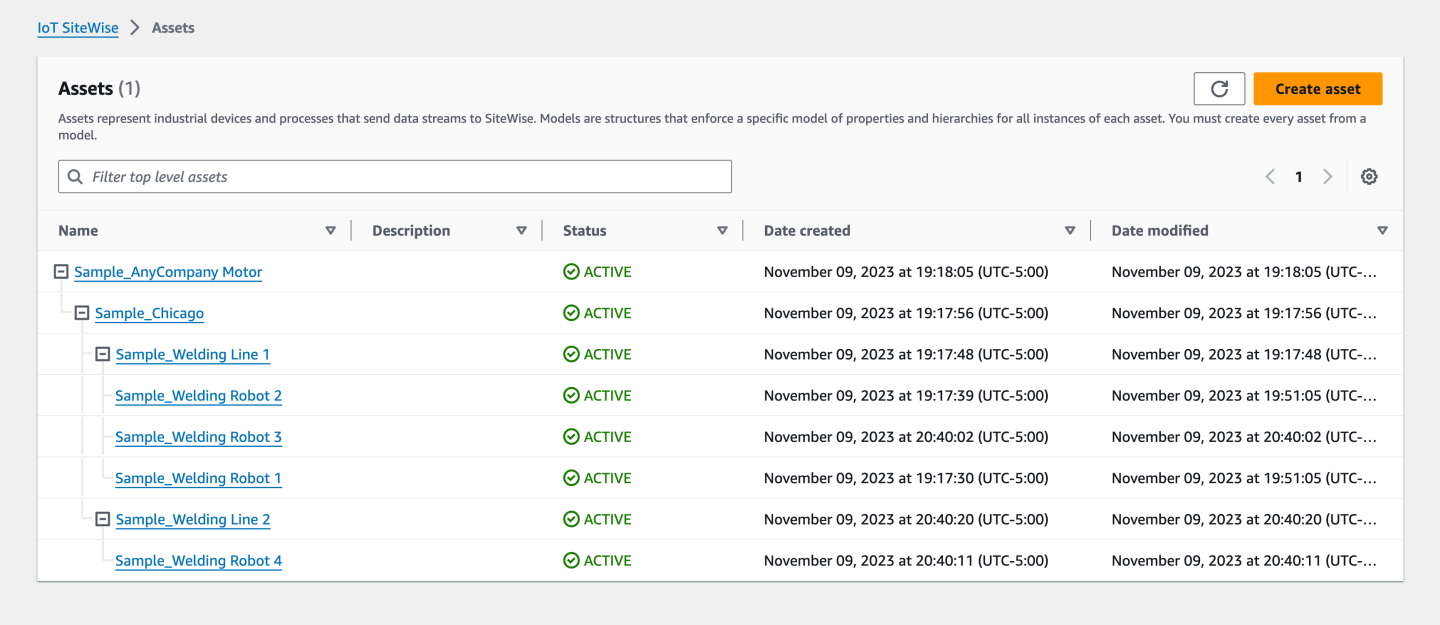
File JSON per l'onboarding di risorse aggiuntive

```
{
    "assets": [
        {
            "assetExternalId": "External_Id_Welding_Robot_3",
            "assetName": "Sample_Welding Robot 3",
            "assetModelExternalId": "External_Id_Welding_Robot",
            "assetProperties": [
                {
                    "externalId": "External_Id_Welding_Robot_Serial_Number",
                    "attributeValue": "S3000"
                },
                {
                    "externalId": "External_Id_Welding_Robot_Cycle_Count",
                    "alias": "AnyCompany/Chicago/Welding Line/S3000/Count"
                },
                {
                    "externalId": "External_Id_Welding_Robot_Joint_1_Current",
                    "alias": "AnyCompany/Chicago/Welding Line/S3000/1/Current"
                }
            ]
        },
        {
            "assetExternalId": "External_Id_Welding_Robot_4",
            "assetName": "Sample_Welding Robot 4",
```

```
            "assetModelExternalId": "External_Id_Welding_Robot",
            "assetProperties": [
                {
                    "externalId": "External_Id_Welding_Robot_Serial_Number",
                    "attributeValue": "S4000"
                },
                {
                    "externalId": "External_Id_Welding_Robot_Cycle_Count",
                    "alias": "AnyCompany/Chicago/Welding Line/S4000/Count"
                },
                {
                    "externalId": "External_Id_Welding_Robot_Joint_1_Current",
                    "alias": "AnyCompany/Chicago/Welding Line/S4000/1/Current"
                }
            ]
        },
        {
            "assetExternalId": "External_Id_Welding_Line_1",
            "assetName": "Sample_Welding Line 1",
            "assetModelExternalId": "External_Id_Welding_Line",
            "assetHierarchies": [
                {
                    "externalId": "External_Id_Welding_Line_TO_Robot",
                    "childAssetExternalId": "External_Id_Welding_Robot_1"
                },
                {
                    "externalId": "External_Id_Welding_Line_TO_Robot",
                    "childAssetExternalId": "External_Id_Welding_Robot_2"
                },
                {
                    "externalId": "External_Id_Welding_Line_TO_Robot",
                    "childAssetExternalId": "External_Id_Welding_Robot_3"
                }
            ]
        },
        {
            "assetExternalId": "External_Id_Welding_Line_2",
            "assetName": "Sample_Welding Line 2",
            "assetModelExternalId": "External_Id_Welding_Line",
            "assetHierarchies": [
                {
                    "externalId": "External_Id_Welding_Line_TO_Robot",
                    "childAssetExternalId": "External_Id_Welding_Robot_4"
                }
```

```
            ]
        },
        {
            "assetExternalId": "External_Id_Site_Chicago",
            "assetName": "Sample_Chicago",
            "assetModelExternalId": "External_Id_Site",
            "assetHierarchies": [
                {
                    "externalId": "External_Id_Site_TO_Line",
                    "childAssetExternalId": "External_Id_Welding_Line_1"
                },
                {
                    "externalId": "External_Id_Site_TO_Line",
                    "childAssetExternalId": "External_Id_Welding_Line_2"
                }
            ]
        }
    ]
}
```

La schermata seguente mostra modelli, risorse e gerarchie visualizzati Console AWS IoT SiteWise dopo l'esecuzione del precedente esempio di codice.



Esempio di onboarding di nuove proprietà

Questo esempio definisce nuove proprietà sui modelli di asset esistenti. Guarda Esempio di onboarding di risorse aggiuntive come integrare risorse e modelli aggiuntivi.

- `Joint 1 Temperature`— Questa proprietà viene aggiunta al modello di `Sample_Welding Robot` asset. Questa nuova proprietà si propagherà anche a ogni risorsa creata dal modello di `Sample_Welding Robot` asset.

Per aggiungere una nuova proprietà a un modello di asset esistente, vedete il seguente esempio di file di metadati JSON. Come mostrato in JSON, l'intera definizione del modello di `Sample_Welding Robot` asset esistente deve essere fornita insieme alla nuova proprietà. Se non viene fornito l'intero elenco di proprietà della definizione esistente, AWS IoT SiteWise elimina le proprietà omesse.

File JSON per incorporare nuove proprietà

Questo esempio aggiunge una nuova proprietà `Joint 1 Temperature` al modello di asset.

```
{
    "assetModels": [
        {
            "assetModelExternalId": "External_Id_Welding_Robot",
            "assetModelName": "Sample_Welding Robot",
            "assetModelProperties": [
                {
                    "dataType": "STRING",
                    "externalId": "External_Id_Welding_Robot_Serial_Number",
                    "name": "Serial Number",
                    "type": {
                        "attribute": {
                            "defaultValue": "-"
                        }
                    },
                    "unit": "-"
                },
                {
                    "dataType": "DOUBLE",
                    "externalId": "External_Id_Welding_Robot_Cycle_Count",
                    "name": "CycleCount",
                    "type": {
                        "measurement": {}
                    },
                    "unit": "EA"
                },
                {
                    "dataType": "DOUBLE",
```

```
                    "externalId": "External_Id_Welding_Robot_Joint_1_Current",
                    "name": "Joint 1 Current",
                    "type": {
                        "measurement": {}
                    },
                    "unit": "Amps"
                },
                {
                    "dataType": "DOUBLE",
                    "externalId": "External_Id_Welding_Robot_Joint_1_Max_Current",
                    "name": "Max Joint 1 Current",
                    "type": {
                        "metric": {
                            "expression": "max(joint1current)",
                            "variables": [
                                {
                                    "name": "joint1current",
                                    "value": {
                                        "propertyExternalId":
"External_Id_Welding_Robot_Joint_1_Current"
                                    }
                                }
                            ],
                            "window": {
                                "tumbling": {
                                    "interval": "5m"
                                }
                            }
                        }
                    },
                    "unit": "Amps"
                },
                {
                    "dataType": "DOUBLE",
                    "externalId": "External_Id_Welding_Robot_Joint_1_Temperature",
                    "name": "Joint 1 Temperature",
                    "type": {
                        "measurement": {}
                    },
                    "unit": "degC"
                }
            ]
        }
    ]
```

```
}
```

Esporta esempi di metadati

Quando esegui un'esportazione in blocco dei tuoi AWS IoT SiteWise contenuti su Amazon S3, puoi specificare filtri per limitare i modelli e gli asset specifici che desideri esportare.

Specificate i filtri in una `iotSiteWiseConfiguration` sezione all'interno della `sources` sezione del corpo della richiesta.

> **Note**
>
> Puoi includere più filtri. L'operazione in blocco esporterà qualsiasi modello di asset o risorsa che corrisponde a uno qualsiasi dei filtri.
> Se non fornite alcun filtro, l'operazione esporterà tutti i modelli e gli asset degli asset.

```
{
    "metadataTransferJobId": "your-transfer-job-id",
    "sources": [{
        "type": "iotsitewise",
        "iotSiteWiseConfiguration": {
            "filters": [{
                list of filters
            }]
        }
    }],
    "destination": {
        "type": "s3",
        "s3Configuration": {
            "location": "arn:aws:s3:::your-S3-bucket-location"
        }
    }
}
```

Filtraggio per modello di asset

Puoi filtrare un modello di asset specifico. Puoi anche includere tutti gli asset che utilizzano quel modello o tutti i modelli di asset all'interno della sua gerarchia. Non puoi includere sia gli asset che la gerarchia.

Per ulteriori informazioni sulle gerarchie, consultare Definizione delle gerarchie dei modelli di asset.

Asset model

Questo filtro include il modello di asset specificato:

```
"filterByAssetModel": {
    "assetModelId": "asset model ID"
}
```

Asset model and its assets

Questo filtro include il modello di asset specificato, insieme a tutti gli asset che utilizzano quel modello di asset:

```
"filterByAssetModel": {
    "assetModelId": "asset model ID",
    "includeAssets": true
}
```

Asset model and its hierarchy

Questo filtro include il modello di asset specificato, insieme a tutti i modelli di asset associati nella sua gerarchia:

```
"filterByAssetModel": {
    "assetModelId": "asset model ID",
    "includeOffspring": true
}
```

Filtraggio per risorsa

Puoi filtrare una risorsa specifica. Puoi anche includere il suo modello di asset o tutte le risorse associate all'interno della sua gerarchia. Non è possibile includere sia il modello di asset che la gerarchia.

Per ulteriori informazioni sulle gerarchie, consultare Definizione delle gerarchie dei modelli di asset.

Asset

Questo filtro include la risorsa specificata:

```
"filterByAsset": {
    "assetId": "asset ID"
}
```

Asset and its asset model

Questo filtro include l'asset specificato, insieme al modello di asset che utilizza:

```
"filterByAsset": {
    "assetId": "asset ID",
    "includeAssetModel": true
}
```

Asset and its hierarchy

Questo filtro include la risorsa specificata, insieme a tutte le risorse associate nella sua gerarchia:

```
"filterByAsset": {
    "assetId": "asset ID",
    "includeOffspring": true
}
```

AWS IoT SiteWise schema del processo di trasferimento dei metadati

Utilizza lo schema del processo di trasferimento AWS IoT SiteWise dei metadati come riferimento quando esegui le tue operazioni di importazione ed esportazione in blocco:

```
{
  "$schema": "https://json-schema.org/draft/2020-12/schema",
  "title": "IoTSiteWise",
  "description": "Metadata transfer job resource schema for IoTSiteWise",
  "definitions": {
    "Name": {
      "type": "string",
      "minLength": 1,
      "maxLength": 256,
      "pattern": "[^\\u0000-\\u001F\\u007F]+"
    },
    "Description": {
      "type": "string",
      "minLength": 1,
```

```
      "maxLength": 2048,
      "pattern": "[^\\u0000-\\u001F\\u007F]+"
    },
    "ID": {
      "type": "string",
      "minLength": 36,
      "maxLength": 36,
      "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}$"
    },
    "ExternalId": {
      "type": "string",
      "minLength": 2,
      "maxLength": 128,
      "pattern": "[a-zA-Z0-9_][a-zA-Z_\\-0-9.:]*[a-zA-Z0-9_]+"
    },
    "AttributeValue": {
      "description": "The value of the property attribute.",
      "type": "string",
      "minLength": 1,
      "maxLength": 1024,
      "pattern": "[^\\u0000-\\u001F\\u007F]+"
    },
    "PropertyUnit": {
      "description": "The unit of measure (such as Newtons or RPM) of the asset
property.",
      "type": "string",
      "minLength": 1,
      "maxLength": 256,
      "pattern": "[^\\u0000-\\u001F\\u007F]+"
    },
    "PropertyAlias": {
      "description": "The property alias that identifies the property.",
      "type": "string",
      "minLength": 1,
      "maxLength": 1000,
      "pattern": "[^\\u0000-\\u001F\\u007F]+"
    },
    "AssetProperty": {
      "description": "The asset property's definition, alias, unit, and notification
state.",
      "type": "object",
      "additionalProperties": false,
      "anyOf": [
        {
```

```
          "required": [
            "id"
          ]
        },
        {
          "required": [
            "externalId"
          ]
        }
      ],
      "properties": {
        "id": {
          "description": "The ID of the asset property.",
          "$ref": "#/definitions/ID"
        },
        "externalId": {
          "description": "The ExternalID of the asset property.",
          "$ref": "#/definitions/ExternalId"
        },
        "alias": {
          "$ref": "#/definitions/PropertyAlias"
        },
        "unit": {
          "$ref": "#/definitions/PropertyUnit"
        },
        "attributeValue": {
          "$ref": "#/definitions/AttributeValue"
        },
        "retainDataOnAliasChange": {
          "type": "string",
          "default": "TRUE",
          "enum": [
            "TRUE",
            "FALSE"
          ]
        },
        "propertyNotificationState": {
          "description": "The MQTT notification state (ENABLED or DISABLED) for this
 asset property.",
          "type": "string",
          "enum": [
            "ENABLED",
            "DISABLED"
          ]
```

```
        }
      }
    },
    "AssetHierarchy": {
      "description": "A hierarchy specifies allowed parent/child asset relationships.",
      "type": "object",
      "additionalProperties": false,
      "anyOf": [
        {
          "required": [
            "id",
            "childAssetId"
          ]
        },
        {
          "required": [
            "externalId",
            "childAssetId"
          ]
        },
        {
          "required": [
            "id",
            "childAssetExternalId"
          ]
        },
        {
          "required": [
            "externalId",
            "childAssetExternalId"
          ]
        }
      ],
      "properties": {
        "id": {
          "description": "The ID of a hierarchy in the parent asset's model.",
          "$ref": "#/definitions/ID"
        },
        "externalId": {
          "description": "The ExternalID of a hierarchy in the parent asset's model.",
          "$ref": "#/definitions/ExternalId"
        },
        "childAssetId": {
          "description": "The ID of the child asset to be associated.",
```

```
          "$ref": "#/definitions/ID"
        },
        "childAssetExternalId": {
          "description": "The ExternalID of the child asset to be associated.",
          "$ref": "#/definitions/ExternalId"
        }
      }
    },
    "Tag": {
      "type": "object",
      "additionalProperties": false,
      "required": [
        "key",
        "value"
      ],
      "properties": {
        "key": {
          "type": "string"
        },
        "value": {
          "type": "string"
        }
      }
    },
    "AssetModelType": {
      "type": "string",
      "default": null,
      "enum": [
        "ASSET_MODEL",
        "COMPONENT_MODEL"
      ]
    },
    "AssetModelCompositeModel": {
      "description": "Contains a composite model definition in an asset model. This
composite model definition is applied to all assets created from the asset model.",
      "type": "object",
      "additionalProperties": false,
      "anyOf": [
        {
          "required": [
            "id"
          ]
        },
        {
```

```
          "required": [
            "externalId"
          ]
        }
      ],
      "required": [
        "name",
        "type"
      ],
      "properties": {
        "id": {
          "description": "The ID of the asset model composite model.",
          "$ref": "#/definitions/ID"
        },
        "externalId": {
          "description": "The ExternalID of the asset model composite model.",
          "$ref": "#/definitions/ExternalId"
        },
        "parentId": {
          "description": "The ID of the parent asset model composite model.",
          "$ref": "#/definitions/ID"
        },
        "parentExternalId": {
          "description": "The ExternalID of the parent asset model composite model.",
          "$ref": "#/definitions/ExternalId"
        },
        "composedAssetModelId": {
          "description": "The ID of the composed asset model.",
          "$ref": "#/definitions/ID"
        },
        "composedAssetModelExternalId": {
          "description": "The ExternalID of the composed asset model.",
          "$ref": "#/definitions/ExternalId"
        },
        "description": {
          "description": "A description for the asset composite model.",
          "$ref": "#/definitions/Description"
        },
        "name": {
          "description": "A unique, friendly name for the asset composite model.",
          "$ref": "#/definitions/Name"
        },
        "type": {
```

```
          "description": "The type of the composite model. For alarm composite models,
 this type is AWS/ALARM.",
          "$ref": "#/definitions/Name"
        },
        "properties": {
          "description": "The property definitions of the asset model.",
          "type": "array",
          "items": {
            "$ref": "#/definitions/AssetModelProperty"
          }
        }
      }
    },
    "AssetModelProperty": {
      "description": "Contains information about an asset model property.",
      "type": "object",
      "additionalProperties": false,
      "anyOf": [
        {
          "required": [
            "id"
          ]
        },
        {
          "required": [
            "externalId"
          ]
        }
      ],
      "required": [
        "name",
        "dataType",
        "type"
      ],
      "properties": {
        "id": {
          "description": "The ID of the asset model property.",
          "$ref": "#/definitions/ID"
        },
        "externalId": {
          "description": "The ExternalID of the asset model property.",
          "$ref": "#/definitions/ExternalId"
        },
        "name": {
```

```
          "description": "The name of the asset model property.",
          "$ref": "#/definitions/Name"
        },
        "dataType": {
          "description": "The data type of the asset model property.",
          "$ref": "#/definitions/DataType"
        },
        "dataTypeSpec": {
          "description": "The data type of the structure for this property.",
          "$ref": "#/definitions/Name"
        },
        "unit": {
          "description": "The unit of the asset model property, such as Newtons or
RPM.",
          "type": "string",
          "minLength": 1,
          "maxLength": 256,
          "pattern": "[^\\u0000-\\u001F\\u007F]+"
        },
        "type": {
          "description": "The property type",
          "$ref": "#/definitions/PropertyType"
        }
      }
    },
    "DataType": {
      "type": "string",
      "enum": [
        "STRING",
        "INTEGER",
        "DOUBLE",
        "BOOLEAN",
        "STRUCT"
      ]
    },
    "PropertyType": {
      "description": "Contains a property type, which can be one of attribute,
measurement, metric, or transform.",
      "type": "object",
      "additionalProperties": false,
      "properties": {
        "attribute": {
          "$ref": "#/definitions/Attribute"
        },
```

```
        "transform": {
          "$ref": "#/definitions/Transform"
        },
        "metric": {
          "$ref": "#/definitions/Metric"
        },
        "measurement": {
          "$ref": "#/definitions/Measurement"
        }
      }
    },
    "Attribute": {
      "type": "object",
      "additionalProperties": false,
      "properties": {
        "defaultValue": {
          "type": "string",
          "minLength": 1,
          "maxLength": 1024,
          "pattern": "[^\\u0000-\\u001F\\u007F]+"
        }
      }
    },
    "Transform": {
      "type": "object",
      "additionalProperties": false,
      "required": [
        "expression",
        "variables"
      ],
      "properties": {
        "expression": {
          "description": "The mathematical expression that defines the transformation
function.",
          "type": "string",
          "minLength": 1,
          "maxLength": 1024
        },
        "variables": {
          "description": "The list of variables used in the expression.",
          "type": "array",
          "items": {
            "$ref": "#/definitions/ExpressionVariable"
          }
```

```
        },
        "processingConfig": {
          "$ref": "#/definitions/TransformProcessingConfig"
        }
      }
    },
    "TransformProcessingConfig": {
      "description": "The processing configuration for the given transform property.",
      "type": "object",
      "additionalProperties": false,
      "required": [
        "computeLocation"
      ],
      "properties": {
        "computeLocation": {
          "description": "The compute location for the given transform property.",
          "$ref": "#/definitions/ComputeLocation"
        },
        "forwardingConfig": {
          "description": "The forwarding configuration for a given property.",
          "$ref": "#/definitions/ForwardingConfig"
        }
      }
    },
    "Metric": {
      "type": "object",
      "additionalProperties": false,
      "required": [
        "expression",
        "variables",
        "window"
      ],
      "properties": {
        "expression": {
          "description": "The mathematical expression that defines the metric
aggregation function.",
          "type": "string",
          "minLength": 1,
          "maxLength": 1024
        },
        "variables": {
          "description": "The list of variables used in the expression.",
          "type": "array",
          "items": {
```

```
            "$ref": "#/definitions/ExpressionVariable"
          }
        },
        "window": {
          "description": "The window (time interval) over which AWS IoT SiteWise
computes the metric's aggregation expression",
          "$ref": "#/definitions/MetricWindow"
        },
        "processingConfig": {
          "$ref": "#/definitions/MetricProcessingConfig"
        }
      }
    },
    "MetricProcessingConfig": {
      "description": "The processing configuration for the metric.",
      "type": "object",
      "additionalProperties": false,
      "required": [
        "computeLocation"
      ],
      "properties": {
        "computeLocation": {
          "description": "The compute location for the given metric property.",
          "$ref": "#/definitions/ComputeLocation"
        }
      }
    },
    "ComputeLocation": {
      "type": "string",
      "enum": [
        "EDGE",
        "CLOUD"
      ]
    },
    "ForwardingConfig": {
      "type": "object",
      "additionalProperties": false,
      "required": [
        "state"
      ],
      "properties": {
        "state": {
          "type": "string",
          "enum": [
```

```
            "ENABLED",
            "DISABLED"
          ]
        }
      }
    },
    "MetricWindow": {
      "description": "Contains a time interval window used for data aggregate
computations (for example, average, sum, count, and so on).",
      "type": "object",
      "additionalProperties": false,
      "properties": {
        "tumbling": {
          "description": "The tumbling time interval window.",
          "type": "object",
          "additionalProperties": false,
          "required": [
            "interval"
          ],
          "properties": {
            "interval": {
              "description": "The time interval for the tumbling window.",
              "type": "string",
              "minLength": 2,
              "maxLength": 23
            },
            "offset": {
              "description": "The offset for the tumbling window.",
              "type": "string",
              "minLength": 2,
              "maxLength": 25
            }
          }
        }
      }
    },
    "ExpressionVariable": {
      "type": "object",
      "additionalProperties": false,
      "required": [
        "name",
        "value"
      ],
      "properties": {
```

```
        "name": {
          "description": "The friendly name of the variable to be used in the
expression.",
          "type": "string",
          "minLength": 1,
          "maxLength": 64,
          "pattern": "^[a-z][a-z0-9_]*$"
        },
        "value": {
          "description": "The variable that identifies an asset property from which to
use values.",
          "$ref": "#/definitions/VariableValue"
        }
      }
    },
    "VariableValue": {
      "type": "object",
      "additionalProperties": false,
      "anyOf": [
        {
          "required": [
            "propertyId"
          ]
        },
        {
          "required": [
            "propertyExternalId"
          ]
        }
      ],
      "properties": {
        "propertyId": {
          "$ref": "#/definitions/ID"
        },
        "propertyExternalId": {
          "$ref": "#/definitions/ExternalId"
        },
        "hierarchyId": {
          "$ref": "#/definitions/ID"
        },
        "hierarchyExternalId": {
          "$ref": "#/definitions/ExternalId"
        }
      }
```

```
    },
    "Measurement": {
      "type": "object",
      "additionalProperties": false,
      "properties": {
        "processingConfig": {
          "$ref": "#/definitions/MeasurementProcessingConfig"
        }
      }
    },
    "MeasurementProcessingConfig": {
      "type": "object",
      "additionalProperties": false,
      "required": [
        "forwardingConfig"
      ],
      "properties": {
        "forwardingConfig": {
          "description": "The forwarding configuration for the given measurement
property.",
          "$ref": "#/definitions/ForwardingConfig"
        }
      }
    },
    "AssetModelHierarchy": {
      "description": "Contains information about an asset model hierarchy.",
      "type": "object",
      "additionalProperties": false,
      "anyOf": [
        {
          "required": [
            "id",
            "childAssetModelId"
          ]
        },
        {
          "required": [
            "id",
            "childAssetModelExternalId"
          ]
        },
        {
          "required": [
            "externalId",
```

```
            "childAssetModelId"
          ]
        },
        {
          "required": [
            "externalId",
            "childAssetModelExternalId"
          ]
        }
      ],
      "required": [
        "name"
      ],
      "properties": {
        "id": {
          "description": "The ID of the asset model hierarchy.",
          "$ref": "#/definitions/ID"
        },
        "externalId": {
          "description": "The ExternalID of the asset model hierarchy.",
          "$ref": "#/definitions/ExternalId"
        },
        "name": {
          "description": "The name of the asset model hierarchy.",
          "$ref": "#/definitions/Name"
        },
        "childAssetModelId": {
          "description": "The ID of the asset model. All assets in this hierarchy must
be instances of the child AssetModelId asset model.",
          "$ref": "#/definitions/ID"
        },
        "childAssetModelExternalId": {
          "description": "The ExternalID of the asset model. All assets in this
hierarchy must be instances of the child AssetModelId asset model.",
          "$ref": "#/definitions/ExternalId"
        }
      }
    },
    "AssetModel": {
      "type": "object",
      "additionalProperties": false,
      "anyOf": [
        {
          "required": [
```

```
            "assetModelId"
          ]
        },
        {
          "required": [
            "assetModelExternalId"
          ]
        }
      ],
      "required": [
        "assetModelName"
      ],
      "properties": {
        "assetModelId": {
          "description": "The ID of the asset model.",
          "$ref": "#/definitions/ID"
        },
        "assetModelExternalId": {
          "description": "The ID of the asset model.",
          "$ref": "#/definitions/ExternalId"
        },
        "assetModelName": {
          "description": "A unique, friendly name for the asset model.",
          "$ref": "#/definitions/Name"
        },
        "assetModelDescription": {
          "description": "A description for the asset model.",
          "$ref": "#/definitions/Description"
        },
        "assetModelType": {
          "description": "The type of the asset model.",
          "$ref": "#/definitions/AssetModelType"
        },
        "assetModelProperties": {
          "description": "The property definitions of the asset model.",
          "type": "array",
          "items": {
            "$ref": "#/definitions/AssetModelProperty"
          }
        },
        "assetModelCompositeModels": {
          "description": "The composite asset models that are part of this asset model.
 Composite asset models are asset models that contain specific properties.",
          "type": "array",
```

```
          "items": {
            "$ref": "#/definitions/AssetModelCompositeModel"
          }
        },
        "assetModelHierarchies": {
          "description": "The hierarchy definitions of the asset model. Each hierarchy
specifies an asset model whose assets can be children of any other assets created from
this asset model.",
          "type": "array",
          "items": {
            "$ref": "#/definitions/AssetModelHierarchy"
          }
        },
        "tags": {
          "description": "A list of key-value pairs that contain metadata for the asset
model.",
          "type": "array",
          "items": {
            "$ref": "#/definitions/Tag"
          }
        }
      }
    },
    "Asset": {
      "type": "object",
      "additionalProperties": false,
      "anyOf": [
        {
          "required": [
            "assetId",
            "assetModelId"
          ]
        },
        {
          "required": [
            "assetExternalId",
            "assetModelId"
          ]
        },
        {
          "required": [
            "assetId",
            "assetModelExternalId"
          ]
```

```
        },
        {
          "required": [
            "assetExternalId",
            "assetModelExternalId"
          ]
        }
      ],
      "required": [
        "assetName"
      ],
      "properties": {
        "assetId": {
          "description": "The ID of the asset",
          "$ref": "#/definitions/ID"
        },
        "assetExternalId": {
          "description": "The external ID of the asset",
          "$ref": "#/definitions/ExternalId"
        },
        "assetModelId": {
          "description": "The ID of the asset model from which to create the asset.",
          "$ref": "#/definitions/ID"
        },
        "assetModelExternalId": {
          "description": "The ExternalID of the asset model from which to create the
asset.",
          "$ref": "#/definitions/ExternalId"
        },
        "assetName": {
          "description": "A unique, friendly name for the asset.",
          "$ref": "#/definitions/Name"
        },
        "assetDescription": {
          "description": "A description for the asset",
          "$ref": "#/definitions/Description"
        },
        "assetProperties": {
          "type": "array",
          "items": {
            "$ref": "#/definitions/AssetProperty"
          }
        },
        "assetHierarchies": {
```

```
          "type": "array",
          "items": {
            "$ref": "#/definitions/AssetHierarchy"
          }
        },
        "tags": {
          "description": "A list of key-value pairs that contain metadata for the
 asset.",
          "type": "array",
          "uniqueItems": false,
          "items": {
            "$ref": "#/definitions/Tag"
          }
        }
      }
    }
  },
  "additionalProperties": false,
  "properties": {
    "assetModels": {
      "type": "array",
      "uniqueItems": false,
      "items": {
        "$ref": "#/definitions/AssetModel"
      }
    },
    "assets": {
      "type": "array",
      "uniqueItems": false,
      "items": {
        "$ref": "#/definitions/Asset"
      }
    }
  }
}
```

Monitoraggio dei dati con allarmi

Puoi configurare allarmi per i tuoi dati per avvisare il team quando le apparecchiature o i processi funzionano in modo non ottimale. Prestazioni ottimali di una macchina o di un processo significa che i valori di determinati parametri devono rientrare in un intervallo di limiti superiore e inferiore. Quando questi parametri sono esterni al loro intervallo di funzionamento, gli operatori delle apparecchiature devono ricevere una notifica per poter risolvere il problema. Utilizza gli allarmi per identificare rapidamente i problemi e avvisare gli operatori per massimizzare le prestazioni delle apparecchiature e dei processi.

Argomenti

Tipi di allarmi

È possibile definire allarmi rilevati nel AWS Cloud e allarmi rilevati con processi esterni. AWS IoT SiteWise supporta i seguenti tipi di allarmi:

- AWS IoT Events allarmi

  AWS IoT Events gli allarmi sono allarmi che rilevano AWS IoT Events AWS IoT SiteWise invia i valori delle proprietà degli asset a un modello di allarme in. AWS IoT Events Quindi, AWS IoT Events invia lo stato di allarme a AWS IoT SiteWise. È possibile configurare opzioni come quando viene rilevato l'allarme e a chi notificare quando lo stato dell'allarme cambia. È inoltre possibile definire le AWS IoT Events azioni che si verificano quando lo stato dell'allarme cambia.

  Gli allarmi in AWS IoT Events sono esempi di modelli di allarme. Il modello di allarme specifica la soglia e la gravità dell'allarme, cosa fare quando lo stato dell'allarme cambia e altro ancora. Quando si configura ogni caratteristica del modello di allarme, si specifica una proprietà di attributo

dal modello di asset monitorato dall'allarme. Tutte le risorse basate sul modello di asset utilizzano il valore dell'attributo per AWS IoT Events valutare quella caratteristica dell'allarme. Per ulteriori informazioni, consulta Uso degli allarmi nella Guida per gli AWS IoT Events sviluppatori.

È possibile rispondere a un AWS IoT Events allarme quando cambia stato. Ad esempio, puoi confermare o posticipare una sveglia quando diventa attiva. Puoi anche abilitare, disabilitare e ripristinare gli allarmi.

SiteWise Gli utenti di Monitor possono visualizzare, configurare e rispondere agli AWS IoT Events allarmi nei SiteWise portali Monitor. Per ulteriori informazioni, consulta Monitoraggio con allarmi nella Guida all'applicazione.AWS IoT SiteWise Monitor

> **Note**
>
> AWS IoT Events si applicano costi per valutare questi allarmi e trasferire dati tra AWS IoT SiteWise e. AWS IoT Events Per ulteriori informazioni, consultare Prezzi di AWS IoT Events.

- Allarmi esterni

  Gli allarmi esterni sono allarmi che vengono valutati al di fuori. AWS IoT SiteWise Usa gli allarmi esterni se disponi di una fonte di dati che riporta lo stato degli allarmi. L'allarme esterno contiene una proprietà di misurazione in cui si inseriscono i dati sullo stato dell'allarme.

  Non è possibile confermare o posticipare un allarme esterno quando cambia stato.

  SiteWise Gli utenti di Monitor possono vedere lo stato degli allarmi esterni nei portali SiteWise Monitor, ma non possono configurare o rispondere a questi allarmi.

  AWS IoT SiteWise non valuta lo stato degli allarmi esterni.

Stati di allarme

Gli allarmi industriali includono informazioni sullo stato dell'apparecchiatura o del processo che monitorano e (opzionali) informazioni sulla risposta dell'operatore allo stato di allarme.

Quando si definisce un AWS IoT Events allarme, si specifica se abilitare o meno il flusso di conferma. Il flusso di conferma è abilitato per impostazione predefinita. Quando si abilita questa opzione, gli operatori possono confermare l'allarme e lasciare una nota con i dettagli sull'allarme o sulle azioni

intraprese per risolverlo. Se un operatore non riconosce un allarme attivo prima che diventi inattivo, l'allarme si blocca. Lo stato bloccato indica che l'allarme è diventato attivo e non è stato riconosciuto, quindi l'operatore deve controllare l'apparecchiatura o il processo e confermare l'allarme interrotto.

Gli allarmi hanno i seguenti stati:

- Normale (`Normal`): l'allarme è abilitato ma inattivo. Il processo o l'attrezzatura industriale funzionano come previsto.
- Attivo (`Active`): l'allarme è attivo. Il processo o l'attrezzatura industriale non rientra nel suo intervallo operativo e richiede attenzione.
- Riconosciuto (`Acknowledged`): un operatore ha riconosciuto lo stato dell'allarme.

  Questo stato si applica solo agli allarmi in cui è abilitato il flusso di conferma.
- Latched (`Latched`): l'allarme è tornato alla normalità ma era attivo e nessun operatore lo ha riconosciuto. Il processo o l'attrezzatura industriale richiedono l'attenzione di un operatore per ripristinare l'allarme alla normalità.

  Questo stato si applica solo agli allarmi in cui è abilitato il flusso di conferma.
- Snoozed (`SnoozeDisabled`): l'allarme è disattivato perché un operatore ha posticipato l'allarme. L'operatore definisce la durata della sonorizzazione dell'allarme. Dopo tale durata, l'allarme torna allo stato normale.
- Disabilitato (`Disabled`): l'allarme è disabilitato e non viene rilevato.

Proprietà dello stato di allarme

AWS IoT SiteWise memorizza i dati sullo stato di allarme come oggetto JSON serializzato su una stringa. Questo oggetto contiene lo stato e informazioni aggiuntive sull'allarme, come le azioni di risposta dell'operatore e la regola valutata dall'allarme.

Si identifica la proprietà dello stato dell'allarme in base al nome e al tipo di struttura,`AWS/ALARM_STATE`. Per ulteriori informazioni, consulta Definizione degli allarmi sui modelli di asset.

L'oggetto dati sullo stato dell'allarme contiene le seguenti informazioni:

`stateName`

Lo stato di un allarme. Per ulteriori informazioni, consulta Stati di allarme.

Tipo di dati: `STRING`

`customerAction`

(Facoltativo) Un oggetto che contiene informazioni sulla risposta di un operatore all'allarme. Gli operatori possono abilitare, disabilitare, confermare e posticipare gli allarmi. Quando lo fanno, i dati sullo stato di allarme includono la loro risposta e la nota che possono lasciare quando rispondono. Questo oggetto contiene le seguenti informazioni:

`actionName`

Il nome dell'azione intrapresa dall'operatore per rispondere all'allarme. Questo valore contiene una delle seguenti stringhe:

- `ENABLE`
- `DISABLE`
- `SNOOZE`
- `ACKNOWLEDGE`
- `RESET`

Tipo di dati: `STRING`

`enable`

(Facoltativo) Un oggetto presente `customerAction` quando l'operatore attiva l'allarme. Quando un operatore attiva l'allarme, lo stato dell'allarme cambia in`Normal`. Questo oggetto contiene le seguenti informazioni:

`note`

(Facoltativo) La nota che il cliente lascia quando attiva l'allarme.

Tipo di dati: `STRING`

Lunghezza massima: 128 caratteri

`disable`

(Facoltativo) Un oggetto presente `customerAction` quando l'operatore disattiva l'allarme. Quando un operatore attiva l'allarme, lo stato dell'allarme cambia in`Disabled`. Questo oggetto contiene le seguenti informazioni:

`note`

(Facoltativo) La nota che il cliente lascia quando disattiva l'allarme.

Tipo di dati: `STRING`

Lunghezza massima: 128 caratteri

`acknowledge`

(Facoltativo) Un oggetto presente `customerAction` quando l'operatore riconosce l'allarme. Quando un operatore attiva l'allarme, lo stato dell'allarme cambia in`Acknowledged`. Questo oggetto contiene le seguenti informazioni:

`note`

(Facoltativo) La nota che il cliente lascia quando riconosce l'allarme.

Tipo di dati: `STRING`

Lunghezza massima: 128 caratteri

`snooze`

(Facoltativo) Un oggetto presente `customerAction` quando l'operatore inserisce l'allarme. Quando un operatore attiva l'allarme, lo stato dell'allarme cambia in. `SnoozeDisabled` Questo oggetto contiene le seguenti informazioni:

`snoozeDuration`

La durata in secondi durante la quale l'operatore posticipa l'allarme. L'allarme cambia allo `Normal` stato dopo questa durata.

Tipo di dati: `INTEGER`

`note`

(Facoltativo) La nota che il cliente lascia quando posticipa la sveglia.

Tipo di dati: `STRING`

Lunghezza massima: 128 caratteri

`ruleEvaluation`

(Facoltativo) Un oggetto che contiene informazioni sulla regola che valuta l'allarme. Questo oggetto contiene le seguenti informazioni:

`simpleRule`

Un oggetto che contiene informazioni su una regola semplice, che confronta il valore di una proprietà con un valore di soglia con un operatore di confronto. Questo oggetto contiene le seguenti informazioni:

`inputProperty`

Il valore della proprietà che questo allarme valuta.

Tipo di dati: `DOUBLE`

`operator`

L'operatore di confronto utilizzato da questo allarme per confrontare la proprietà con la soglia. Questo valore contiene una delle seguenti stringhe:

- `<` — Meno di
- `<=` — Minore o uguale
- `==` — Uguale
- `!=` — Non uguale
- `>=` — Maggiore o uguale
- `>` — Maggiore di

Tipo di dati: `STRING`

`threshold`

Il valore di soglia con cui questo allarme confronta il valore della proprietà.

Tipo di dati: `DOUBLE`

Definizione degli allarmi sui modelli di asset

I modelli di asset favoriscono la standardizzazione dei dati e degli allarmi industriali. È possibile definire le definizioni degli allarmi sui modelli di asset per standardizzare gli allarmi per tutti gli asset in base a un modello di asset.

Utilizzate modelli di asset compositi per definire allarmi sui modelli di asset. I modelli di asset compositi sono modelli di asset che standardizzano un insieme specifico di proprietà su un altro modello di asset. I modelli di asset compositi assicurano la presenza di determinate proprietà su un modello di asset. Gli allarmi hanno proprietà relative al tipo, allo stato e (facoltativo) all'origine, quindi il modello composito degli allarmi impone l'esistenza di tali proprietà.

Ogni modello di asset composito ha un tipo che definisce le proprietà di quel modello composito. I modelli compositi di allarme definiscono le proprietà per il tipo di allarme, lo stato di allarme e

(opzionale) la fonte di allarme. Quando create una risorsa da un modello di asset con modelli compositi, la risorsa include le proprietà del modello composito insieme alle proprietà specificate nel modello di asset.

Ogni proprietà in un modello composito deve avere il nome che la identifica per il tipo di modello composito. Le proprietà del modello composito supportano proprietà con tipi di dati complessi. Queste proprietà hanno il tipo di `STRUCT` dati e una `dataTypeSpec` caratteristica che specifica il tipo di dati complesso della proprietà. Le proprietà dei tipi di dati complessi contengono dati JSON serializzati come stringhe.

I modelli compositi di allarme hanno le seguenti proprietà. Ogni proprietà deve avere il nome che la identifica per questo tipo di modello composito.

Tipo di allarme

Il tipo di allarme. Specifica una delle seguenti proprietà:

- `IOT_EVENTS`— Un AWS IoT Events allarme. AWS IoT SiteWise invia dati AWS IoT Events per valutare lo stato di questo allarme. È necessario specificare la proprietà della fonte dell'allarme per definire il modello di AWS IoT Events allarme per questa definizione di allarme.
- `EXTERNAL`— Un allarme esterno. Si inserisce lo stato dell'allarme come misurazione.

Nome della proprietà: `AWS/ALARM_TYPE`

Tipo di proprietà: attributo

Tipo di dati: `STRING`

Stato di allarme

I dati delle serie temporali relativi allo stato dell'allarme. Si tratta di un oggetto serializzato come stringa che contiene lo stato e altre informazioni sull'allarme. Per ulteriori informazioni, consulta Proprietà dello stato di allarme.

Nome della proprietà: `AWS/ALARM_STATE`

Tipo di proprietà: misurazione

Tipo di dati: `STRUCT`

Tipo di struttura dati: `AWS/ALARM_STATE`

Fonte di allarme

(Facoltativo) L'Amazon Resource Name (ARN) della risorsa che valuta lo stato dell'allarme. Per gli AWS IoT Events allarmi, questo è l'ARN del modello di allarme.

Nome della proprietà: `AWS/ALARM_SOURCE`

Tipo di proprietà: attributo

Tipo di dati: `STRING`

Example Esempio di modello composito di allarme

Il seguente modello di impianto rappresenta una caldaia dotata di un allarme per monitorarne la temperatura. AWS IoT SiteWise invia i dati di temperatura AWS IoT Events a per rilevare l'allarme.

```
{
  "assetModelName": "Boiler",
  "assetModelDescription": "A boiler that alarms when its temperature exceeds its
 limit.",
  "assetModelProperties": [
    {
      "name": "Temperature",
      "dataType": "DOUBLE",
      "unit": "Celsius",
      "type": {
        "measurement": {}
      }
    },
    {
      "name": "High Temperature",
      "dataType": "DOUBLE",
      "unit": "Celsius",
      "type": {
        "attribute": {
          "defaultValue": "105.0"
        }
      }
    }
  ],
  "assetModelCompositeModels": [
    {
```

```
      "name": "BoilerTemperatureHighAlarm",
      "type": "AWS/ALARM",
      "properties": [
        {
          "name": "AWS/ALARM_TYPE",
          "dataType": "STRING",
          "type": {
            "attribute": {
              "defaultValue": "IOT_EVENTS"
            }
          }
        },
        {
          "name": "AWS/ALARM_STATE",
          "dataType": "STRUCT",
          "dataTypeSpec": "AWS/ALARM_STATE",
          "type": {
            "measurement": {}
          }
        },
        {
          "name": "AWS/ALARM_SOURCE",
          "dataType": "STRING",
          "type": {
            "attribute": {}
          }
        }
      ]
    }
  ]
}
```

Argomenti

- Definizione degli AWS IoT Events allarmi
- Definizione di allarmi esterni

Definizione degli AWS IoT Events allarmi

Quando si crea un AWS IoT Events allarme, AWS IoT SiteWise invia i valori delle proprietà dell'asset AWS IoT Events per valutare lo stato dell'allarme. AWS IoT Events le definizioni degli allarmi dipendono dal modello di allarme in cui si definisce AWS IoT Events. Per definire un AWS IoT Events

allarme su un modello di asset, si definisce un modello composito di allarme che specifica il modello di AWS IoT Events allarme come proprietà della fonte dell'allarme.

AWS IoT Events gli allarmi dipendono da input come le soglie di allarme e le impostazioni di notifica degli allarmi. Questi input vengono definiti come attributi nel modello di asset. È quindi possibile personalizzare questi input su ogni risorsa in base al modello. La AWS IoT SiteWise console può creare questi attributi per te. Se definisci gli allarmi con l'API AWS CLI o, devi definire manualmente questi attributi nel modello di asset.

Puoi anche definire altre azioni che si verificano quando viene rilevato un allarme, come azioni di notifica di allarme personalizzate. Ad esempio, puoi configurare un'azione che invia una notifica push a un argomento di Amazon SNS. Per ulteriori informazioni sulle azioni che puoi definire, consulta Lavorare con altri AWS servizi nella Guida per gli AWS IoT Events sviluppatori.

Quando aggiorni o elimini un modello di asset, AWS IoT SiteWise puoi verificare se un modello di allarme in AWS IoT Events sta monitorando una proprietà di asset associata a questo modello di asset. Ciò impedisce di eliminare una proprietà dell'asset attualmente utilizzata da un AWS IoT Events allarme. Per abilitare questa funzionalità AWS IoT SiteWise, è necessario disporre dell'`iotevents:ListInputRoutings`autorizzazione. Questa autorizzazione consente di AWS IoT SiteWise effettuare chiamate all'operazione ListInputRoutingsAPI supportata da AWS IoT Events. Per ulteriori informazioni, consulta ListInputRoutings Autorizzazione (Facoltativa).

> **Note**
>
> La funzionalità di notifica degli allarmi non è disponibile nella regione Cina (Pechino).

Argomenti

- Requisiti per le notifiche di allarme
- Definizione di un AWS IoT Events allarme (AWS IoT SiteWise console)
- Definizione di un AWS IoT Events allarme (AWS IoT Events console)
- Definizione di un AWS IoT Events allarme (AWS CLI)

Requisiti per le notifiche di allarme

AWS IoT Events utilizza una AWS Lambda funzione del tuo AWS account per inviare notifiche di allarme. È necessario creare questa funzione Lambda nella stessa AWS regione degli allarmi per abilitare le notifiche di allarme. Questa funzione Lambda utilizza Amazon Simple Notification Service

(Amazon SNS) per inviare notifiche di testo e Amazon Simple Email Service (Amazon SES) per inviare notifiche e-mail. Quando crei l' AWS IoT Events allarme, configuri i protocolli e le impostazioni che l'allarme utilizza per inviare le notifiche.

AWS IoT Events fornisce un modello di AWS CloudFormation stack che puoi usare per creare questa funzione Lambda nel tuo account. Per ulteriori informazioni, consulta la funzione Lambda di notifica degli allarmi nella Guida per gli AWS IoT Events sviluppatori.

Definizione di un AWS IoT Events allarme (AWS IoT SiteWise console)

È possibile utilizzare la AWS IoT SiteWise console per definire un AWS IoT Events allarme su un modello di asset esistente. Per definire un AWS IoT Events allarme su un nuovo modello di asset, create il modello di asset, quindi completate questi passaggi. Per ulteriori informazioni, consulta Creazione dei modelli di asset.

> **Important**
>
> Ogni allarme richiede un attributo che specifica il valore di soglia con cui confrontare l'allarme. È necessario definire l'attributo del valore di soglia nel modello di asset prima di poter definire un allarme.
> Si consideri un esempio in cui si desidera definire un allarme che rilevi quando una turbina eolica supera la velocità massima del vento di 50 mph. Prima di definire l'allarme, è necessario definire un attributo (Velocità massima del vento) con un valore predefinito di. `50`

Per definire un AWS IoT Events allarme su un modello di asset

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione selezionare Models (Modelli).
3. Scegliete il modello di asset per il quale definire un allarme.
4. Scegliete la scheda Allarme.
5. Scegli Aggiungi allarme.
6. Nella sezione Opzioni del tipo di allarme, scegli AWS IoT Events Allarme.
7. Nella sezione Dettagli dell'allarme, procedi come segue:
    a. Immetti un nome per l’allarme.
    b. (Facoltativo) Inserisci una descrizione per l'allarme.

8. Nella sezione Definizioni delle soglie, definisci quando viene rilevato l'allarme e la gravità dell'allarme. Esegui questa operazione:

   a. Seleziona la proprietà in base alla quale viene rilevato l'allarme. Ogni volta che questa proprietà riceve un nuovo valore, AWS IoT SiteWise invia il valore AWS IoT Events a per valutare lo stato dell'allarme.

   b. Seleziona l'operatore da utilizzare per confrontare la proprietà con il valore di soglia. Seleziona una delle opzioni seguenti:

      - < meno di
      - <= minore o uguale
      - == uguale
      - ! = non uguale
      - >= maggiore o uguale
      - > maggiore di

   c. Per Valore, selezionate la proprietà dell'attributo da utilizzare come valore di soglia. AWS IoT Events confronta il valore della proprietà con il valore di questo attributo.

   d. Inserisci la gravità dell'allarme. Usa un numero comprensibile al tuo team per indicare la gravità dell'allarme.

9. (Facoltativo) Nella sezione Impostazioni di notifica - opzionale, procedi come segue:

   a. Scegli Attivo.

   > **Note**
   >
   > Se scegli Inattivo, tu e il tuo team non riceverete alcuna notifica di allarme.

   b. Per Destinatario, scegli il destinatario.

   > **Important**
   >
   > È possibile inviare notifiche di allarme agli AWS IAM Identity Center utenti. Per utilizzare questa funzionalità, è necessario abilitare IAM Identity Center. Puoi abilitare IAM Identity Center solo in una AWS regione alla volta. Ciò significa che puoi definire le notifiche di allarme solo nella regione in cui abiliti IAM Identity Center.

Per ulteriori informazioni, consulta Nozioni di base nella Guida per l'utente di AWS IAM Identity Center .

c. Per Protocollo, scegli tra le seguenti opzioni:

- Email e testo: l'allarme avvisa gli utenti di IAM Identity Center con un messaggio SMS e un messaggio e-mail.
- E-mail: l'allarme avvisa gli utenti di IAM Identity Center con un messaggio e-mail.
- Testo: l'allarme avvisa gli utenti di IAM Identity Center con un messaggio SMS.

d. Per Mittente, scegli il mittente.

Important

È necessario verificare l'indirizzo e-mail del mittente in Amazon Simple Email Service (Amazon SES). Per ulteriori informazioni, consulta la sezione Verifica degli indirizzi e-mail in Amazon SES, nella Amazon Simple Email Service Developer Guide.

10. Nella sezione Stato predefinito degli asset, puoi impostare lo stato predefinito per gli allarmi creati da questo modello di asset.

Note

Attivate o disattivate questo allarme per gli asset che create da questo modello di asset in una fase successiva.

11. Nella sezione Impostazioni avanzate, puoi configurare le autorizzazioni, le impostazioni di notifica aggiuntive, le azioni relative allo stato degli allarmi, il modello di allarme in SiteWise Monitor e il flusso di conferma.

Note

AWS IoT Events gli allarmi richiedono i seguenti ruoli di servizio:

- Un ruolo che AWS IoT Events presuppone di inviare i valori dello stato di allarme a. AWS IoT SiteWise

- Un ruolo che AWS IoT Events presuppone l'invio di dati a Lambda. Questo ruolo è necessario solo se l'allarme invia notifiche.

Nella sezione Autorizzazioni, procedi come segue:

a. Per AWS IoT Events il ruolo, utilizza un ruolo esistente o crea un ruolo con le autorizzazioni richieste. Questo ruolo richiede l'`iotsitewise:BatchPutAssetPropertyValue`autorizzazione e una relazione di fiducia che consenta a iotevents.amazonaws.com di assumere il ruolo.

b. Per il ruolo AWS IoT Events Lambda, usa un ruolo esistente o crea un ruolo con le autorizzazioni richieste. Questo ruolo richiede le `sso-directory:DescribeUser` autorizzazioni `lambda:InvokeFunction` e e una relazione di fiducia che `iotevents.amazonaws.com` consenta di assumere il ruolo.

12. (Facoltativo) Nella sezione Impostazioni di notifica aggiuntive, procedi come segue:

a. Per l'attributo Destinatario, si definisce un attributo il cui valore specifica il destinatario della notifica. Puoi scegliere gli utenti di IAM Identity Center come destinatari.

Puoi creare un attributo o utilizzare un attributo esistente sul modello di asset.

- Se scegli Crea un nuovo attributo destinatario, specifica il nome dell'attributo Destinatario e il valore predefinito del destinatario, facoltativo per l'attributo.
- Se scegli Usa un attributo destinatario esistente, scegli l'attributo in Nome attributo destinatario. L'avviso utilizza il valore predefinito dell'attributo scelto.

È possibile sovrascrivere il valore predefinito di ogni risorsa creata da questo modello di asset.

b. Per l'attributo messaggio personalizzato, si definisce un attributo il cui valore specifica il messaggio personalizzato da inviare oltre al messaggio di modifica dello stato predefinito. Ad esempio, puoi specificare un messaggio che aiuti il tuo team a capire come rispondere a questo allarme.

È possibile scegliere di creare un attributo o utilizzare un attributo esistente nel modello di asset.

- Se scegli di creare un nuovo attributo personalizzato del messaggio, specifica il nome dell'attributo del messaggio personalizzato e il valore predefinito del messaggio personalizzato, facoltativo per l'attributo.
- Se scegli Usa un attributo di messaggio personalizzato esistente, scegli l'attributo in Nome attributo messaggio personalizzato. L'avviso utilizza il valore predefinito dell'attributo scelto.

È possibile sovrascrivere il valore predefinito di ogni risorsa creata da questo modello di asset.

c. Per Gestire la funzione Lambda, effettuate una delle seguenti operazioni:

- Per AWS IoT SiteWise creare una nuova funzione Lambda, scegli Crea una nuova lambda da un modello gestito da AWS.
- Per utilizzare una funzione Lambda esistente, scegli Usa una funzione Lambda esistente e scegli il nome della funzione.

Per ulteriori informazioni, consulta Gestione delle notifiche di allarme nella Guida per gli AWS IoT Events sviluppatori.

13. (Facoltativo) Nella sezione Imposta l'azione dello stato, procedi come segue:

a. Scegliete Modifica azione.

b. In Aggiungi azioni relative allo stato di allarme, aggiungi azioni, quindi scegli Salva.

Puoi aggiungere fino a 10 azioni.

AWS IoT Events può eseguire azioni quando l'allarme è attivo. È possibile definire azioni integrate per utilizzare un timer o impostare una variabile o inviare dati ad altre AWS risorse. Per ulteriori informazioni, consulta Azioni supportate nella Guida per AWS IoT Events gli sviluppatori.

14. (Facoltativo) In Gestisci il modello di allarme in SiteWise Monitor: facoltativo, scegli Attivo o Inattivo.

Usa questa opzione per aggiornare il modello di allarme in SiteWise Monitorss. Per impostazione predefinita, questa opzione è abilitata.

15. In Conferma flusso, scegli Attivo o Inattivo. Per ulteriori informazioni sul flusso di conferma, consultaStati di allarme.

16. Scegli Aggiungi allarme.

> **Note**
>
> La AWS IoT SiteWise console effettua più richieste API per aggiungere l'allarme al modello di asset. Quando scegli Aggiungi allarme, la console apre una finestra di dialogo che mostra lo stato di avanzamento di queste richieste API. Rimani su questa pagina fino a quando ogni richiesta API non ha esito positivo o finché una richiesta API non riesce. Se una richiesta fallisce, chiudi la finestra di dialogo, risolvi il problema e scegli Aggiungi allarme per riprovare.

Definizione di un AWS IoT Events allarme (AWS IoT Events console)

È possibile utilizzare la AWS IoT Events console per definire un AWS IoT Events allarme su un modello di asset esistente. Per definire un AWS IoT Events allarme su un nuovo modello di asset, create il modello di asset, quindi completate questi passaggi. Per ulteriori informazioni, consulta Creazione dei modelli di asset.

> **Important**
>
> Ogni allarme richiede un attributo che specifica il valore di soglia con cui confrontare l'allarme. È necessario definire l'attributo del valore di soglia nel modello di asset prima di poter definire un allarme.
> Si consideri un esempio in cui si desidera definire un allarme che rilevi quando una turbina eolica supera la velocità massima del vento di 50 mph. Prima di definire l'allarme, è necessario definire un attributo (Velocità massima del vento) con un valore predefinito di. `50`

Per definire un AWS IoT Events allarme su un modello di asset

1. Passare alla console AWS IoT Events.
2. Nel pannello di navigazione, scegli Modelli di allarme.
3. Scegli Crea modello di allarme.
4. Immetti un nome per l'allarme.
5. (Facoltativo) Inserisci una descrizione per il tuo allarme.
6. Nella sezione Obiettivo dell'allarme, procedi come segue:

a. Per le opzioni di Target, scegli la proprietàAWS IoT SiteWise dell'asset.

b. Scegli il modello di asset per il quale desideri aggiungere l'allarme.

7. Nella sezione Definizioni delle soglie, definisci quando viene rilevato l'allarme e la gravità dell'allarme. Esegui questa operazione:

a. Seleziona la proprietà in base alla quale viene rilevato l'allarme. Ogni volta che questa proprietà riceve un nuovo valore, AWS IoT SiteWise invia il valore AWS IoT Events a per valutare lo stato dell'allarme.

b. Seleziona l'operatore da utilizzare per confrontare la proprietà con il valore di soglia. Seleziona una delle opzioni seguenti:

- < meno di
- <= minore o uguale
- == uguale
- ! = non uguale
- >= maggiore o uguale
- > maggiore di

c. Per Valore, selezionate la proprietà dell'attributo da utilizzare come valore di soglia. AWS IoT Events confronta il valore della proprietà con il valore di questo attributo.

d. Inserisci la gravità dell'allarme. Usa un numero comprensibile al tuo team per indicare la gravità dell'allarme.

8. (Facoltativo) Nella sezione Impostazioni di notifica - opzionale, procedi come segue:

a. Per Protocollo, scegli tra le seguenti opzioni:

- Email e testo: l'allarme avvisa gli utenti di IAM Identity Center con un messaggio SMS e un messaggio e-mail.
- E-mail: l'allarme avvisa gli utenti di IAM Identity Center con un messaggio e-mail.
- Testo: l'allarme avvisa gli utenti di IAM Identity Center con un messaggio SMS.

b. Per Mittente, scegli il mittente.

> **Important**
>
> È necessario verificare l'indirizzo e-mail del mittente in Amazon Simple Email Service (Amazon SES). Per ulteriori informazioni, consulta la sezione Verifica degli

indirizzi e-mail in Amazon SES, nella Amazon Simple Email Service Developer Guide.

c. Scegli l'attributo nell'attributo Recipient (facoltativo). L'allarme utilizza il valore predefinito dell'attributo scelto.

d. Scegli l'attributo in Attributo messaggio personalizzato - opzionale. L'avviso utilizza il valore predefinito dell'attributo scelto.

9. Nella sezione Istanza, specifica lo stato predefinito per questo avviso. È possibile attivare o disattivare questo allarme per tutte le risorse create da questo modello di asset in un passaggio successivo.

10. Nelle impostazioni avanzate, è possibile configurare le autorizzazioni, le impostazioni di notifica aggiuntive, le azioni relative allo stato di allarme, il modello di allarme in SiteWise Monitor e il flusso di conferma.

> **Note**
>
> AWS IoT Events gli allarmi richiedono i seguenti ruoli di servizio:
>
> - Un ruolo che AWS IoT Events presuppone di inviare i valori dello stato di allarme a. AWS IoT SiteWise
> - Un ruolo che AWS IoT Events presuppone l'invio di dati a Lambda. Questo ruolo è necessario solo se l'allarme invia notifiche.

a. Nella sezione Conferma flusso, scegli Abilitato o Disabilitato. Per ulteriori informazioni sul flusso di conferma, consultaStati di allarme.

b. Nella sezione Autorizzazioni, procedi come segue:

i. Per AWS IoT Events il ruolo, utilizza un ruolo esistente o crea un ruolo con le autorizzazioni richieste. Questo ruolo richiede l'`iotsitewise:BatchPutAssetPropertyValue`autorizzazione e una relazione di fiducia che consenta a iotevents.amazonaws.com di assumere il ruolo.

ii. Per il ruolo Lambda, usa un ruolo esistente o crea un ruolo con le autorizzazioni richieste. Questo ruolo richiede le `sso-directory:DescribeUser` autorizzazioni `lambda:InvokeFunction` e e una relazione di fiducia che `iotevents.amazonaws.com` consenta di assumere il ruolo.

c. (Facoltativo) Nel riquadro Impostazioni di notifica aggiuntive, procedi come segue:

   - Per Gestire la funzione Lambda, effettuate una delle seguenti operazioni:
     - Per AWS IoT Events creare una nuova funzione Lambda, scegli Crea una nuova funzione Lambda.
     - Per utilizzare una funzione Lambda esistente, scegli Usa una funzione Lambda esistente e scegli il nome della funzione.

   Per ulteriori informazioni, consulta Gestione delle notifiche di allarme nella Guida per gli AWS IoT Events sviluppatori.

d. (Facoltativo) Nella sezione Imposta l'azione dello stato - opzionale, procedi come segue:

   - In Azioni relative allo stato di allarme, aggiungi azioni, quindi scegli Salva.

     Puoi aggiungere fino a 10 azioni.

   AWS IoT Events può eseguire azioni quando l'allarme è attivo. È possibile definire azioni integrate per utilizzare un timer o impostare una variabile o inviare dati ad altre AWS risorse. Per ulteriori informazioni, consulta Azioni supportate nella Guida per AWS IoT Events gli sviluppatori.

11. Scegli Crea.

> **Note**
>
> La AWS IoT Events console effettua più richieste API per aggiungere l'allarme al modello di asset. Quando scegli Aggiungi allarme, la console apre una finestra di dialogo che mostra lo stato di avanzamento di queste richieste API. Rimani su questa pagina fino a quando ogni richiesta API non ha esito positivo o finché una richiesta API non riesce. Se una richiesta fallisce, chiudi la finestra di dialogo, risolvi il problema e scegli Aggiungi allarme per riprovare.

Definizione di un AWS IoT Events allarme (AWS CLI)

È possibile utilizzare il AWS Command Line Interface (AWS CLI) per definire un AWS IoT Events allarme che monitora la proprietà di un asset. È possibile definire l'allarme su un modello di asset

nuovo o esistente. Dopo aver definito l'allarme sul modello di asset, create un allarme AWS IoT Events e lo collegate al modello di asset. In questo processo, effettuate le seguenti operazioni:

Fasi

- Fase 1: Definizione di un allarme su un modello di asset
- Fase 2: Definizione di un modello di allarme AWS IoT Events
- Fase 3: Attivazione del flusso di dati tra e AWS IoT SiteWiseAWS IoT Events

Fase 1: Definizione di un allarme su un modello di asset

Aggiungere una definizione di allarme e le proprietà associate a un modello di asset nuovo o esistente.

Per definire un allarme su un modello di asset (CLI)

1. Crea un file denominato `asset-model-payload.json`. Segui i passaggi in queste altre sezioni per aggiungere i dettagli del tuo modello di asset al file, ma non inviare la richiesta per creare o aggiornare il modello di asset. In questa sezione, aggiungi una definizione di allarme ai dettagli del modello di asset contenuti nel `asset-model-payload.json` file.
   - Per ulteriori informazioni su come creare un modello di asset, consultaCreazione di un modello di asset (AWS CLI).
   - Per ulteriori informazioni su come aggiornare un modello di asset esistente, consultaAggiornamento di un modello di asset o componente ()AWS CLI.

   > **Note**
   >
   > Il modello di asset deve definire almeno una proprietà dell'asset, inclusa la proprietà dell'asset da monitorare con l'allarme.

2. Aggiungi un modello composito di allarme (`assetModelCompositeModels`) al modello di asset. Un modello composito di AWS IoT Events allarme specifica il `IOT_EVENTS` tipo e specifica una proprietà della fonte di allarme. Si aggiunge la proprietà della fonte di allarme dopo aver creato il modello di allarme in. AWS IoT Events

> **Important**
>
> Il modello composito di allarme deve avere lo stesso nome del modello di AWS IoT Events allarme creato in seguito. I nomi dei modelli di allarme possono contenere solo caratteri alfanumerici. Specificate un nome alfanumerico univoco in modo da poter utilizzare lo stesso nome per il modello di allarme.

```
{
  ...
  "assetModelCompositeModels": [
    {
      "name": "BoilerTemperatureHighAlarm",
      "type": "AWS/ALARM",
      "properties": [
        {
          "name": "AWS/ALARM_TYPE",
          "dataType": "STRING",
          "type": {
            "attribute": {
              "defaultValue": "IOT_EVENTS"
            }
          }
        },
        {
          "name": "AWS/ALARM_STATE",
          "dataType": "STRUCT",
          "dataTypeSpec": "AWS/ALARM_STATE",
          "type": {
            "measurement": {}
          }
        }
      ]
    }
  ]
}
```

3. Aggiungi un attributo di soglia di allarme al modello di asset. Specificate il valore predefinito da utilizzare per questa soglia. È possibile sovrascrivere questo valore predefinito su ogni risorsa basata su questo modello.

> **Note**
>
> L'attributo della soglia di allarme deve essere un `INTEGER` o un`DOUBLE`.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "Temperature Max Threshold",
      "dataType": "DOUBLE",
      "type": {
        "attribute": {
          "defaultValue": "105.0"
        }
      }
    }
  ]
}
```

4. (Facoltativo) Aggiungi gli attributi di notifica degli allarmi al modello di asset. Questi attributi specificano il destinatario di IAM Identity Center e altri input AWS IoT Events utilizzati per inviare notifiche quando l'allarme cambia stato. Puoi sovrascrivere queste impostazioni predefinite su ogni risorsa basata su questo modello.

   > **Important**
   >
   > È possibile inviare notifiche di allarme agli utenti. AWS IAM Identity Center Per utilizzare questa funzionalità, è necessario abilitare IAM Identity Center. Puoi abilitare IAM Identity Center solo in una AWS regione alla volta. Ciò significa che puoi definire le notifiche di allarme solo nella regione in cui abiliti IAM Identity Center. Per ulteriori informazioni, consulta Nozioni di base nella Guida per l'utente di AWS IAM Identity Center .

   Esegui questa operazione:

a. Aggiungi un attributo che specifica l'ID del tuo archivio di identità IAM Identity Center. Puoi utilizzare l'operazione ListInstancesAPI IAM Identity Center per elencare i tuoi archivi di identità. Questa operazione funziona solo nella regione in cui è abilitato IAM Identity Center.

```
aws sso-admin list-instances
```

Quindi, specifica l'Identity Store ID (ad esempio,`d-123EXAMPLE`) come valore predefinito per l'attributo.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "identityStoreId",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "d-123EXAMPLE"
        }
      }
    }
  ]
}
```

b. Aggiungi un attributo che specifica l'ID dell'utente IAM Identity Center che riceve le notifiche. Per definire un destinatario di notifica predefinito, aggiungi un ID utente IAM Identity Center come valore predefinito. Effettua una delle seguenti operazioni per ottenere un ID utente IAM Identity Center:

i. Puoi utilizzare l'ListUsersAPI IAM Identity Center per ottenere l'ID di un utente di cui conosci il nome utente. Sostituisci *D-123Example* con l'ID del tuo archivio di identità e sostituisci *Name con il nome* utente dell'utente.

```
aws identitystore list-users \
  --identity-store-id d-123EXAMPLE \
  --filters AttributePath=UserName,AttributeValue=Name
```

ii. Utilizza la console IAM Identity Center per sfogliare gli utenti e trovare un ID utente.

Quindi, specifica l'ID utente (ad esempio`123EXAMPLE-a1b2c3d4-5678-90ab-cdef-33333EXAMPLE`) come valore predefinito per l'attributo o definisci l'attributo senza un valore predefinito.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "userId",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "123EXAMPLE-a1b2c3d4-5678-90ab-cdef-33333EXAMPLE"
        }
      }
    }
  ]
}
```

c. (Facoltativo) Aggiungi un attributo che specifica l'ID mittente predefinito per le notifiche tramite SMS (testo). L'ID mittente viene visualizzato come mittente dei messaggi inviati da Amazon Simple Notification Service (Amazon SNS). Per ulteriori informazioni, consulta Richiesta degli ID mittente per la messaggistica SMS con Amazon SNS nella Amazon Simple Notification Service Developer Guide.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "senderId",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "MyFactory"
        }
      }
    }
  ]
```

```
}
```

d. (Facoltativo) Aggiungi un attributo che specifica l'indirizzo e-mail predefinito da utilizzare come indirizzo del mittente nelle notifiche e-mail.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "fromAddress",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "my.factory@example.com"
        }
      }
    }
  ]
}
```

e. (Facoltativo) Aggiungi un attributo che specifica l'oggetto predefinito da utilizzare nelle notifiche e-mail.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "emailSubject",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "[ALERT] High boiler temperature"
        }
      }
    }
  ]
}
```

f. (Facoltativo) Aggiungi un attributo che specifica un messaggio aggiuntivo da includere nelle notifiche. Per impostazione predefinita, i messaggi di notifica includono informazioni

sull'allarme. È inoltre possibile includere un messaggio aggiuntivo che fornisca all'utente ulteriori informazioni.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "additionalMessage",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "Turn off the power before you check the alarm."
        }
      }
    }
  ]
}
```

5. Crea il modello di asset o aggiorna il modello di asset esistente. Esegui una di queste operazioni:
   - Per creare il modello di asset, esegui il comando seguente.

     ```
     aws iotsitewise create-asset-model --cli-input-json file://asset-model-payload.json
     ```

   - Per aggiornare il modello di asset esistente, esegui il comando seguente. Sostituisci *asset-model-id* con l'ID del modello di asset.

     ```
     aws iotsitewise update-asset-model \
       --asset-model-id asset-model-id \
       --cli-input-json file://asset-model-payload.json
     ```

   Dopo aver eseguito il comando, `assetModelId` annotatelo nella risposta.

Esempio: modello di asset per caldaie

Il seguente modello di asset rappresenta una caldaia che riporta i dati sulla temperatura. Questo modello di asset definisce un allarme che rileva il surriscaldamento della caldaia.

```
{
  "assetModelName": "Boiler Model",
```

```
  "assetModelDescription": "Represents a boiler.",
  "assetModelProperties": [
    {
      "name": "Temperature",
      "dataType": "DOUBLE",
      "unit": "C",
      "type": {
        "measurement": {}
      }
    },
    {
      "name": "Temperature Max Threshold",
      "dataType": "DOUBLE",
      "type": {
        "attribute": {
          "defaultValue": "105.0"
        }
      }
    },
    {
      "name": "identityStoreId",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "d-123EXAMPLE"
        }
      }
    },
    {
      "name": "userId",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "123EXAMPLE-a1b2c3d4-5678-90ab-cdef-33333EXAMPLE"
        }
      }
    },
    {
      "name": "senderId",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "MyFactory"
        }
```

```
      }
    },
    {
      "name": "fromAddress",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "my.factory@example.com"
        }
      }
    },
    {
      "name": "emailSubject",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "[ALERT] High boiler temperature"
        }
      }
    },
    {
      "name": "additionalMessage",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "Turn off the power before you check the alarm."
        }
      }
    }
  ],
  "assetModelHierarchies": [

  ],
  "assetModelCompositeModels": [
    {
      "name": "BoilerTemperatureHighAlarm",
      "type": "AWS/ALARM",
      "properties": [
        {
          "name": "AWS/ALARM_TYPE",
          "dataType": "STRING",
          "type": {
            "attribute": {
              "defaultValue": "IOT_EVENTS"
```

```
            }
          }
        },
        {
          "name": "AWS/ALARM_STATE",
          "dataType": "STRUCT",
          "dataTypeSpec": "AWS/ALARM_STATE",
          "type": {
            "measurement": {}
          }
        }
      ]
    }
  ]
}
```

Fase 2: Definizione di un modello di allarme AWS IoT Events

Crea il modello di allarme in AWS IoT Events. In AWS IoT Events, si utilizzano le espressioni per specificare i valori nei modelli di allarme. È possibile utilizzare espressioni per specificare valori AWS IoT SiteWise da valutare e utilizzare come input per l'allarme. Quando AWS IoT SiteWise invia i valori delle proprietà dell'asset al modello di allarme, AWS IoT Events valuta l'espressione per ottenere il valore della proprietà o l'ID della risorsa. È possibile utilizzare le seguenti espressioni nel modello di allarme:

- Valori delle proprietà degli asset

  Per ottenere il valore di una proprietà dell'asset, utilizzate la seguente espressione. Sostituisci *`assetModelId`*con l'ID del modello di asset e sostituisci *`PropertyID`* con l'ID della proprietà.

  ```
  $sitewise.assetModel.`assetModelId`.`propertyId`.propertyValue.value
  ```

- ID delle risorse

  Per ottenere l'ID della risorsa, utilizzate la seguente espressione. Sostituisci *`assetModelId`*con l'ID del modello di asset e sostituisci *`PropertyID`* con l'ID della proprietà.

  ```
  $sitewise.assetModel.`assetModelId`.`propertyId`.assetId
  ```

> **Note**
>
> Quando si crea il modello di allarme, è possibile definire valori letterali anziché espressioni che restituiscono valori. AWS IoT SiteWise In questo modo è possibile ridurre il numero di attributi definiti nel modello di asset. Tuttavia, se definisci un valore come valore letterale, non puoi personalizzare quel valore sugli asset in base al modello di asset. Inoltre, gli AWS IoT SiteWise Monitor utenti non possono personalizzare l'allarme, poiché possono configurare le impostazioni di allarme solo sugli asset.

Per creare un modello di AWS IoT Events allarme (CLI)

1. Quando si crea il modello di allarme in AWS IoT Events, è necessario specificare l'ID di ogni proprietà utilizzata dall'allarme, che include quanto segue:

   - La proprietà dello stato di allarme nel modello di asset composito
   - La proprietà monitorata dall'allarme
   - L'attributo threshold
   - (Facoltativo) L'attributo ID del negozio di identità di IAM Identity Center
   - (Facoltativo) L'attributo ID utente di IAM Identity Center
   - (Facoltativo) L'attributo ID mittente SMS
   - (Facoltativo) L'attributo email proveniente dall'indirizzo
   - (Facoltativo) L'attributo oggetto dell'email
   - (Facoltativo) L'attributo aggiuntivo del messaggio

   Eseguite il comando seguente per recuperare gli ID di queste proprietà sul modello di asset. *`asset-model-id`*Sostituitelo con l'ID del modello di asset del passaggio precedente.

   ```
   aws iotsitewise describe-asset-model --asset-model-id asset-model-id
   ```

   L'operazione restituisce una risposta contenente i dettagli del modello di asset. Annota l'ID di ogni proprietà utilizzata dall'allarme. Questi ID vengono utilizzati quando si crea il modello di AWS IoT Events allarme nel passaggio successivo.

2. Crea il modello di allarme in AWS IoT Events. Esegui questa operazione:

a. Crea un file denominato `alarm-model-payload.json`.

b. Copia il seguente oggetto JSON nel file.

c. Inserisci un nome (`alarmModelName`), una descrizione (`alarmModelDescription`) e una gravità (`severity`) per l'allarme. Per quanto riguarda la gravità, specificate un numero intero che rifletta i livelli di gravità della vostra azienda.

> **Important**
>
> Il modello di allarme deve avere lo stesso nome del modello composito di allarmi definito in precedenza nel modello di asset.
> I nomi dei modelli di allarme possono contenere solo caratteri alfanumerici.

```
{
  "alarmModelName": "BoilerTemperatureHighAlarm",
  "alarmModelDescription": "Detects when the boiler temperature is high.",
  "severity": 3
}
```

d. Aggiungi la regola di confronto (`alarmRule`) all'allarme. Questa regola definisce la proprietà da monitorare (`inputProperty`), il valore di soglia da confrontare (`threshold`) e l'operatore di confronto da utilizzare (`comparisonOperator`).

- Sostituisci *`assetModelId`*con l'ID del modello di asset.
- Sostituisci *`alarmPropertyId`*con l'ID della proprietà monitorata dall'allarme.
- Sostituisci *`thresholdAttributeId`*con l'ID della proprietà dell'attributo di soglia.
- Sostituire *`GREATER`* con l'operatore da utilizzare per confrontare i valori delle proprietà con la soglia. Seleziona una delle opzioni seguenti:
  - `LESS`
  - `LESS_OR_EQUAL`
  - `EQUAL`
  - `NOT_EQUAL`
  - `GREATER_OR_EQUAL`
  - `GREATER`

```
{
  "alarmModelName": "BoilerTemperatureHighAlarm",
  "alarmModelDescription": "Detects when the boiler temperature is high.",
  "severity": 3,
  "alarmRule": {
    "simpleRule": {
      "inputProperty":
 "$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.propertyValue.value",
      "comparisonOperator": "GREATER",
      "threshold":
 "$sitewise.assetModel.`assetModelId`.`thresholdAttributeId`.propertyValue.value"
    }
  }
}
```

e. Aggiungi un'azione (`alarmEventActions`) per inviare lo stato di allarme al AWS IoT SiteWise momento in cui l'allarme cambia stato.

> **Note**
>
> Per la configurazione avanzata, è possibile definire azioni aggiuntive da eseguire quando l'allarme cambia stato. Ad esempio, è possibile richiamare una AWS Lambda funzione o pubblicare su un argomento MQTT. Per ulteriori informazioni, consulta Lavorare con altri AWS servizi nella Guida per gli AWS IoT Events sviluppatori.

- Sostituisci *`assetModelId`*con l'ID del modello di asset.
- Sostituisci *`alarmPropertyId`*con l'ID della proprietà monitorata dall'allarme.
- Sostituisci *`alarmStatePropertyId`* con l'ID della proprietà dello stato di allarme nel modello composito di allarme.

```
{
  "alarmModelName": "BoilerTemperatureHighAlarm",
  "alarmModelDescription": "Detects when the boiler temperature is high.",
  "severity": 3,
  "alarmRule": {
```

```
    "simpleRule": {
      "inputProperty":
 "$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.propertyValue.value",
      "comparisonOperator": "GREATER",
      "threshold":
 "$sitewise.assetModel.`assetModelId`.`thresholdAttributeId`.propertyValue.value"
    }
  },
  "alarmEventActions": {
    "alarmActions": [
      {
        "iotSiteWise": {
          "assetId":
 "$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.assetId",
          "propertyId": "'alarmStatePropertyId'"
        }
      }
    ]
  }
}
```

f. (Facoltativo) Configura le impostazioni di notifica degli allarmi. L'azione di notifica degli allarmi utilizza una funzione Lambda nel tuo account per inviare notifiche di allarme. Per ulteriori informazioni, consulta Requisiti per le notifiche di allarme. Nelle impostazioni di notifica degli allarmi, puoi configurare le notifiche SMS ed e-mail da inviare agli utenti di IAM Identity Center. Esegui questa operazione:

   i. Aggiungi la configurazione della notifica di allarme (`alarmNotification`) al payload in`alarm-model-payload.json`.

      - Sostituisci *`alarmNotificationFunctionArn`* con l'ARN della funzione Lambda che gestisce le notifiche di allarme.

```
{
  "alarmModelName": "BoilerTemperatureHighAlarm",
  "alarmModelDescription": "Detects when the boiler temperature is high.",
  "severity": 3,
  "alarmRule": {
    "simpleRule": {
      "inputProperty":
 "$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.propertyValue.value",
```

```
      "comparisonOperator": "GREATER",
      "threshold":
"$sitewise.assetModel.`assetModelId`.`thresholdAttributeId`.propertyValue.value"
    }
  },
  "alarmEventActions": {
    "alarmActions": [
      {
        "iotSiteWise": {
          "assetId":
"$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.assetId",
          "propertyId": "'alarmStatePropertyId'"
        }
      }
    ]
  },
  "alarmNotification": {
    "notificationActions": [
      {
        "action": {
          "lambdaAction": {
            "functionArn": "alarmNotificationFunctionArn"
          }
        }
      }
    ]
  }
}
```

ii. (Facoltativo) Configura le notifiche SMS (`smsConfigurations`) da inviare a un utente di IAM Identity Center quando l'allarme cambia stato.

- Sostituisci *identityStoreIdAttributeId*con l'ID dell'attributo che contiene l'ID dell'archivio di identità di IAM Identity Center.
- Sostituisci *userIdAttributeId* con l'ID dell'attributo che contiene l'ID dell'utente IAM Identity Center.
- Sostituisci *senderIdAttributeId* con l'ID dell'attributo che contiene l'ID mittente di Amazon SNS o rimuovilo `senderId` dal payload.
- Sostituisci *additionalMessageAttributeId* con l'ID dell'attributo che contiene il messaggio aggiuntivo o rimuovilo `additionalMessage` dal payload.

```
{
  "alarmModelName": "BoilerTemperatureHighAlarm",
  "alarmModelDescription": "Detects when the boiler temperature is high.",
  "severity": 3,
  "alarmRule": {
    "simpleRule": {
      "inputProperty":
 "$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.propertyValue.value",
      "comparisonOperator": "GREATER",
      "threshold":
 "$sitewise.assetModel.`assetModelId`.`thresholdAttributeId`.propertyValue.value"
    }
  },
  "alarmEventActions": {
    "alarmActions": [
      {
        "iotSiteWise": {
          "assetId":
 "$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.assetId",
          "propertyId": "'alarmStatePropertyId'"
        }
      }
    ]
  },
  "alarmNotification": {
    "notificationActions": [
      {
        "action": {
          "lambdaAction": {
            "functionArn": "alarmNotificationFunctionArn"
          }
        },
        "smsConfigurations": [
          {
            "recipients": [
              {
                "ssoIdentity": {
                  "identityStoreId":
 "$sitewise.assetModel.`assetModelId`.`identityStoreIdAttributeId`.propertyValue.va
                  "userId":
 "$sitewise.assetModel.`assetModelId`.`userIdAttributeId`.propertyValue.value"
                }
```

```
            }
          ],
          "senderId":
"$sitewise.assetModel.`assetModelId`.`senderIdAttributeId`.propertyValue.value",
          "additionalMessage":
"$sitewise.assetModel.`assetModelId`.`additionalMessageAttributeId`.propertyValue.
        }
      ]
    }
  ]
 }
}
```

iii. (Facoltativo) Configura le notifiche e-mail (`emailConfigurations`) da inviare a un utente di IAM Identity Center quando l'allarme cambia stato.

- Sostituisci *`identityStoreIdAttributeId`*con l'ID della proprietà dell'attributo Identity Store ID di IAM Identity Center.
- Sostituisci *`userIdAttributeId`* con l'ID della proprietà dell'attributo ID utente di IAM Identity Center.
- Sostituisci *`fromAddressAttributeId`* con l'ID della proprietà dell'attributo dell'indirizzo «from» o rimuovi `from` dal payload.
- Sostituisci *`emailSubjectAttributeId`* con l'ID della proprietà dell'attributo email subject o rimuovi `subject` dal payload.
- Sostituisci *`additionalMessageAttributeId`* con l'ID della proprietà aggiuntiva dell'attributo del messaggio o rimuovi `additionalMessage` dal payload.

```
{
  "alarmModelName": "BoilerTemperatureHighAlarm",
  "alarmModelDescription": "Detects when the boiler temperature is high.",
  "severity": 3,
  "alarmRule": {
    "simpleRule": {
      "inputProperty":
"$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.propertyValue.value",
      "comparisonOperator": "GREATER",
      "threshold":
"$sitewise.assetModel.`assetModelId`.`thresholdAttributeId`.propertyValue.value"
    }
  },
```

```
 "alarmEventActions": {
   "alarmActions": [
     {
       "iotSiteWise": {
         "assetId":
"$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.assetId",
         "propertyId": "'alarmStatePropertyId'"
       }
     }
   ]
 },
 "alarmNotification": {
   "notificationActions": [
     {
       "action": {
         "lambdaAction": {
           "functionArn": "alarmNotificationFunctionArn"
         }
       },
       "smsConfigurations": [
         {
           "recipients": [
             {
               "ssoIdentity": {
                 "identityStoreId":
"$sitewise.assetModel.`assetModelId`.`identityStoreIdAttributeId`.propertyValue.va
                 "userId":
"$sitewise.assetModel.`assetModelId`.`userIdAttributeId`.propertyValue.value"
               }
             }
           ],
           "senderId":
"$sitewise.assetModel.`assetModelId`.`senderIdAttributeId`.propertyValue.value",
           "additionalMessage":
"$sitewise.assetModel.`assetModelId`.`additionalMessageAttributeId`.propertyValue.
         }
       ],
       "emailConfigurations": [
         {
           "from":
"$sitewise.assetModel.`assetModelId`.`fromAddressAttributeId`.propertyValue.value"
           "recipients": {
             "to": [
               {
```

```
                  "ssoIdentity": {
                    "identityStoreId":
  "$sitewise.assetModel.`assetModelId`.`identityStoreIdAttributeId`.propertyValue.va
                    "userId":
  "$sitewise.assetModel.`assetModelId`.`userIdAttributeId`.propertyValue.value"
                  }
                }
              ]
            },
            "content": {
              "subject":
  "$sitewise.assetModel.`assetModelId`.`emailSubjectAttributeId`.propertyValue.value
              "additionalMessage":
  "$sitewise.assetModel.`assetModelId`.`additionalMessageAttributeId`.propertyValue.
            }
          }
        ]
      }
    ]
  }
}
```

g. (Facoltativo) Aggiungi le funzionalità di allarme (`alarmCapabilities`) al payload in. `alarm-model-payload.json` In questo oggetto, è possibile specificare se il flusso di conferma è abilitato e lo stato di abilitazione predefinito per gli asset in base al modello di asset. Per ulteriori informazioni sul flusso di conferma, consultaStati di allarme.

```
{
  "alarmModelName": "BoilerTemperatureHighAlarm",
  "alarmModelDescription": "Detects when the boiler temperature is high.",
  "severity": 3,
  "alarmRule": {
    "simpleRule": {
      "inputProperty":
 "$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.propertyValue.value",
      "comparisonOperator": "GREATER",
      "threshold":
 "$sitewise.assetModel.`assetModelId`.`thresholdAttributeId`.propertyValue.value"
    }
  },
  "alarmEventActions": {
    "alarmActions": [
      {
```

```
        "iotSiteWise": {
          "assetId":
"$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.assetId",
          "propertyId": "'alarmStatePropertyId'"
        }
      }
    ]
  },
  "alarmNotification": {
    "notificationActions": [
      {
        "action": {
          "lambdaAction": {
            "functionArn": "alarmNotificationFunctionArn"
          }
        },
        "smsConfigurations": [
          {
            "recipients": [
              {
                "ssoIdentity": {
                  "identityStoreId":
"$sitewise.assetModel.`assetModelId`.`identityStoreIdAttributeId`.propertyValue.value"
                  "userId":
"$sitewise.assetModel.`assetModelId`.`userIdAttributeId`.propertyValue.value"
                }
              }
            ],
            "senderId":
"$sitewise.assetModel.`assetModelId`.`senderIdAttributeId`.propertyValue.value",
            "additionalMessage":
"$sitewise.assetModel.`assetModelId`.`additionalMessageAttributeId`.propertyValue.valu
          }
        ],
        "emailConfigurations": [
          {
            "from":
"$sitewise.assetModel.`assetModelId`.`fromAddressAttributeId`.propertyValue.value",
            "recipients": {
              "to": [
                {
                  "ssoIdentity": {
                    "identityStoreId":
"$sitewise.assetModel.`assetModelId`.`identityStoreIdAttributeId`.propertyValue.value"
```

```
                    "userId":
 "$sitewise.assetModel.`assetModelId`.`userIdAttributeId`.propertyValue.value"
                  }
                }
              ]
            },
            "content": {
              "subject":
 "$sitewise.assetModel.`assetModelId`.`emailSubjectAttributeId`.propertyValue.value",
              "additionalMessage":
 "$sitewise.assetModel.`assetModelId`.`additionalMessageAttributeId`.propertyValue.valu
            }
          }
        ]
      }
    ]
  },
  "alarmCapabilities": {
    "initializationConfiguration": {
      "disabledOnInitialization": false
    },
    "acknowledgeFlow": {
      "enabled": true
    }
  }
}
```

h. Aggiungi il ruolo del servizio IAM (`roleArn`) a cui AWS IoT Events puoi presumere di inviare dati AWS IoT SiteWise. Questo ruolo richiede l'`iotsitewise:BatchPutAssetPropertyValue`autorizzazione e una relazione di fiducia che `iotevents.amazonaws.com` consenta di assumere il ruolo. Per inviare notifiche, questo ruolo richiede anche le `sso-directory:DescribeUser` autorizzazioni `lambda:InvokeFunction` e. Per ulteriori informazioni, consulta i ruoli del servizio di allarme nella Guida per gli AWS IoT Events sviluppatori.

   - Sostituisci `roleArn` con l'ARN del ruolo che AWS IoT Events può assumere per eseguire queste azioni.

```
{
  "alarmModelName": "BoilerTemperatureHighAlarm",
  "alarmModelDescription": "Detects when the boiler temperature is high.",
```

```
 "severity": 3,
 "alarmRule": {
   "simpleRule": {
     "inputProperty":
"$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.propertyValue.value",
     "comparisonOperator": "GREATER",
     "threshold":
"$sitewise.assetModel.`assetModelId`.`thresholdAttributeId`.propertyValue.value"
   }
 },
 "alarmEventActions": {
   "alarmActions": [
     {
       "iotSiteWise": {
         "assetId":
"$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.assetId",
         "propertyId": "'alarmStatePropertyId'"
       }
     }
   ]
 },
 "alarmNotification": {
   "notificationActions": [
     {
       "action": {
         "lambdaAction": {
           "functionArn": "alarmNotificationFunctionArn"
         }
       },
       "smsConfigurations": [
         {
           "recipients": [
             {
               "ssoIdentity": {
                 "identityStoreId":
"$sitewise.assetModel.`assetModelId`.`identityStoreIdAttributeId`.propertyValue.value"
                 "userId":
"$sitewise.assetModel.`assetModelId`.`userIdAttributeId`.propertyValue.value"
               }
             }
           ],
           "senderId":
"$sitewise.assetModel.`assetModelId`.`senderIdAttributeId`.propertyValue.value",
```

```
            "additionalMessage":
 "$sitewise.assetModel.`assetModelId`.`additionalMessageAttributeId`.propertyValue.valu
          }
        ],
        "emailConfigurations": [
          {
            "from":
 "$sitewise.assetModel.`assetModelId`.`fromAddressAttributeId`.propertyValue.value",
            "recipients": {
              "to": [
                {
                  "ssoIdentity": {
                    "identityStoreId":
 "$sitewise.assetModel.`assetModelId`.`identityStoreIdAttributeId`.propertyValue.value"
                    "userId":
 "$sitewise.assetModel.`assetModelId`.`userIdAttributeId`.propertyValue.value"
                  }
                }
              ]
            },
            "content": {
              "subject":
 "$sitewise.assetModel.`assetModelId`.`emailSubjectAttributeId`.propertyValue.value",
              "additionalMessage":
 "$sitewise.assetModel.`assetModelId`.`additionalMessageAttributeId`.propertyValue.valu
            }
          }
        ]
      }
    ]
  },
  "alarmCapabilities": {
    "initializationConfiguration": {
      "disabledOnInitialization": false
    },
    "acknowledgeFlow": {
      "enabled": false
    }
  },
  "roleArn": "arn:aws:iam::123456789012:role/MyIoTEventsAlarmRole"
}
```

i. Esegui il comando seguente per creare il modello di AWS IoT Events allarme dal payload in. `alarm-model-payload.json`

```
aws iotevents create-alarm-model --cli-input-json file://alarm-model-
payload.json
```

j. L'operazione restituisce una risposta che include l'ARN del modello di allarme,. `alarmModelArn` Copia questo ARN per impostare la definizione di allarme sul tuo modello di asset nel passaggio successivo.

Fase 3: Attivazione del flusso di dati tra e AWS IoT SiteWiseAWS IoT Events

Dopo aver creato le risorse richieste in AWS IoT SiteWise e AWS IoT Events, puoi abilitare il flusso di dati tra le risorse per attivare l'allarme. In questa sezione, aggiorni la definizione di allarme nel modello di asset per utilizzare il modello di allarme creato nel passaggio precedente.

Per abilitare il flusso di dati tra AWS IoT SiteWise e AWS IoT Events (CLI)

- Imposta il modello di allarme come fonte dell'allarme nel modello di asset. Esegui questa operazione:

  a. Esegui il comando seguente per recuperare la definizione del modello di asset esistente. Sostituisci *`asset-model-id`*con l'ID del modello di asset.

  ```
  aws iotsitewise describe-asset-model --asset-model-id asset-model-id
  ```

  L'operazione restituisce una risposta contenente i dettagli del modello di asset.

  b. Crea un file denominato `update-asset-model-payload.json` e copia la risposta del comando precedente nel file.

  c. Rimuovete le seguenti coppie chiave-valore dal `update-asset-model-payload.json` file:

  - `assetModelId`
  - `assetModelArn`
  - `assetModelCreationDate`
  - `assetModelLastUpdateDate`
  - `assetModelStatus`

d. Aggiungi la proprietà della fonte dell'allarme (`AWS/ALARM_SOURCE`) al modello composito di allarme che hai definito in precedenza. Sostituisci *`alarmModelArn`* con l'ARN del modello di allarme, che imposta il valore della proprietà della fonte di allarme.

```
{
  ...
  "assetModelCompositeModels": [
    ...
    {
      "name": "BoilerTemperatureHighAlarm",
      "type": "AWS/ALARM",
      "properties": [
        {
          "id": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
          "name": "AWS/ALARM_TYPE",
          "dataType": "STRING",
          "type": {
            "attribute": {
              "defaultValue": "IOT_EVENTS"
            }
          }
        },
        {
          "id": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
          "name": "AWS/ALARM_STATE",
          "dataType": "STRUCT",
          "dataTypeSpec": "AWS/ALARM_STATE",
          "type": {
            "measurement": {}
          }
        },
        {
          "name": "AWS/ALARM_SOURCE",
          "dataType": "STRING",
          "type": {
            "attribute": {
              "defaultValue": "alarmModelArn"
            }
          }
        }
      ]
    }
  ]
```

```
}
```

e. Eseguite il comando seguente per aggiornare il modello di asset con la definizione memorizzata nel `update-asset-model-payload.json` file. Sostituisci *`asset-model-id`*con l'ID del modello di asset.

```
aws iotsitewise update-asset-model \
  --asset-model-id asset-model-id \
  --cli-input-json file://update-asset-model-payload.json
```

Il tuo modello di asset ora definisce un allarme che viene rilevato. AWS IoT Events L'allarme monitora la proprietà di destinazione in tutti gli asset in base a questo modello di asset. Puoi configurare l'allarme su ogni asset per personalizzare proprietà come la soglia o il destinatario IAM Identity Center per ogni asset. Per ulteriori informazioni, consulta Configurazione degli allarmi sugli asset.

Definizione di allarmi esterni

Gli allarmi esterni contengono lo stato di un allarme rilevato all'esterno. AWS IoT SiteWise

Definizione di un allarme esterno (console)

È possibile utilizzare la AWS IoT SiteWise console per definire un allarme esterno su un modello di asset esistente. Per definire un allarme esterno su un nuovo modello di asset, create il modello di asset, quindi completate questi passaggi. Per ulteriori informazioni, consulta Creazione dei modelli di asset.

Per definire un allarme su un modello di asset

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione selezionare Models (Modelli).
3. Scegliete il modello di asset per il quale definire un allarme.
4. Scegliete la scheda Definizioni degli allarmi.
5. Scegli Aggiungi allarme.
6. Nelle opzioni del tipo di allarme, scegli Allarme esterno.
7. Immetti un nome per l’allarme.
8. (Facoltativo) Inserisci una descrizione per l'allarme.
9. Scegli Aggiungi allarme.

Definizione di un allarme esterno (CLI)

È possibile utilizzare il AWS CLI per definire un allarme esterno su un modello di asset nuovo o esistente.

Per aggiungere un allarme esterno a un modello di asset, è necessario aggiungere un modello composito di allarmi al modello di asset. Un modello composito di allarme esterno specifica il `EXTERNAL` tipo e non specifica una proprietà della fonte di allarme. L'esempio seguente di allarme composito definisce un allarme di temperatura esterna.

```
{
  ...
  "assetModelCompositeModels": [
    {
      "name": "BoilerTemperatureHighAlarm",
      "type": "AWS/ALARM",
      "properties": [
        {
          "name": "AWS/ALARM_TYPE",
          "dataType": "STRING",
          "type": {
            "attribute": {
              "defaultValue": "EXTERNAL"
            }
          }
        },
        {
          "name": "AWS/ALARM_STATE",
          "dataType": "STRUCT",
          "dataTypeSpec": "AWS/ALARM_STATE",
          "type": {
            "measurement": {}
          }
        }
      ]
    }
  ]
}
```

Per ulteriori informazioni su come aggiungere un modello composito a un modello di asset nuovo o esistente, consultate quanto segue:

- Creazione di un modello di asset (AWS CLI)
- Aggiornamento di un modello di asset o componente ()AWS CLI

Dopo aver definito l'allarme esterno, potete importare lo stato di allarme agli asset in base al modello di asset. Per ulteriori informazioni, consulta Acquisizione dello stato di allarme esterno.

Configurazione degli allarmi sugli asset

Dopo aver definito un AWS IoT Events allarme su un modello di asset, è possibile configurare l'allarme su ogni asset in base al modello di asset. È possibile modificare il valore di soglia e le impostazioni di notifica per l'allarme. Ciascuno di questi valori è un attributo della risorsa, quindi puoi aggiornare il valore predefinito dell'attributo per configurare questi valori.

> **Note**
>
> Puoi configurare questi valori per gli AWS IoT Events allarmi, ma non per gli allarmi esterni.

Argomenti

- Configurazione di un valore di soglia (console)
- Configurazione di un valore di soglia ()AWS CLI
- Configurazione delle impostazioni di notifica (console)
- Configurazione delle impostazioni di notifica (CLI)

Configurazione di un valore di soglia (console)

È possibile utilizzare la AWS IoT SiteWise console per aggiornare il valore dell'attributo che specifica il valore di soglia di un allarme.

Per aggiornare il valore di soglia di un allarme (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Asset.
3. Scegliete la risorsa per la quale desiderate aggiornare un valore di soglia di allarme.

> **Tip**
>
> Puoi scegliere l'icona a forma di freccia per espandere una gerarchia di asset e trovare il tuo asset.

4. Scegli Modifica.
5. Trova l'attributo che l'allarme utilizza per il suo valore di soglia, quindi inserisci il nuovo valore.
6. Selezionare Salva.

Configurazione di un valore di soglia ()AWS CLI

È possibile utilizzare AWS Command Line Interface (AWS CLI) per aggiornare il valore dell'attributo che specifica il valore di soglia di un allarme.

Per completare questa procedura, è necessario conoscere l'elemento `assetId` dell'asset e l'elemento `propertyId` della proprietà. Puoi anche usare l'ID esterno. Se hai creato una risorsa e non la conosci`assetId`, utilizza l'ListAssetsAPI per elencare tutte le risorse per un modello specifico. Utilizzate l'DescribeAssetoperazione per visualizzare le proprietà della risorsa, compresi gli ID delle proprietà.

Utilizzate l'BatchPutAssetPropertyValueoperazione per assegnare i valori degli attributi alla risorsa. È possibile utilizzare questa operazione per impostare più attributi contemporaneamente. Il payload di questa operazione include un elenco di voci, ciascuna delle quali contenente l'ID asset, l'ID proprietà e il valore dell'attributo.

Per aggiornare il valore di un attributo ()AWS CLI

1. Crea un file denominato `batch-put-payload.json` e copia il seguente oggetto JSON nel file. Questo esempio di payload mostra come impostare la latitudine e la longitudine di una turbina eolica. Aggiorna gli ID, i valori e i timestamp per modificare il payload per il tuo caso d'uso.

```
{
  "entries": [
    {
      "entryId": "windfarm3-turbine7-latitude",
      "assetId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
      "propertyId": "a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
      "propertyValues": [
```

```
        {
          "value": {
            "doubleValue": 47.6204
          },
          "timestamp": {
            "timeInSeconds": 1575691200
          }
        }
      ]
    },
    {
      "entryId": "windfarm3-turbine7-longitude",
      "assetId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
      "propertyId": "a1b2c3d4-5678-90ab-cdef-55555EXAMPLE",
      "propertyValues": [
        {
          "value": {
            "doubleValue": 122.3491
          },
          "timestamp": {
            "timeInSeconds": 1575691200
          }
        }
      ]
    }
  ]
}
```

- Ogni voce nel payload contiene un `entryId` che è possibile definire come una qualsiasi stringa univoca. Se una richiesta non riesce, ciascun errore conterrà l'`entryId` della richiesta corrispondente in modo che sia possibile sapere quale richiesta riprovare.
- Per impostare il valore di un attributo, è possibile includere una struttura timestamp-quality-value (TQV) nell'elenco di ogni proprietà dell'`propertyValues`attributo. Questa struttura deve contenere il nuovo `value` e il `timestamp` corrente.
  - `value`— Una struttura che contiene uno dei seguenti campi, a seconda del tipo di proprietà impostata:
    - `booleanValue`
    - `doubleValue`
    - `integerValue`
    - `stringValue`

- `timestamp`— Una struttura che contiene l'ora attuale dell'epoca Unix in secondi,. `timeInSeconds` AWS IoT SiteWise rifiuta tutti i punti dati con timestamp che esistevano da più di 7 giorni nel passato o più recenti di 5 minuti nelle future.

Per ulteriori informazioni su come preparare un payload per, consulta. BatchPutAssetPropertyValueAcquisizione di dati tramite l'API AWS IoT SiteWise

2. Eseguite il comando seguente per inviare i valori degli attributi a AWS IoT SiteWise:

```
aws iotsitewise batch-put-asset-property-value -\-cli-input-json file://batch-put-payload.json
```

Configurazione delle impostazioni di notifica (console)

È possibile utilizzare la AWS IoT SiteWise console per aggiornare il valore degli attributi che specificano le impostazioni di notifica per un allarme.

Per aggiornare le impostazioni di notifica di un avviso (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Asset.
3. Scegli la risorsa per la quale desideri aggiornare le impostazioni della sveglia.
4. Scegli Modifica.
5. Trova l'attributo utilizzato dall'allarme per l'impostazione di notifica che desideri modificare, quindi inserisci il nuovo valore.
6. Selezionare Salva.

Configurazione delle impostazioni di notifica (CLI)

È possibile utilizzare AWS Command Line Interface (AWS CLI) per aggiornare il valore dell'attributo che specifica le impostazioni di notifica per un avviso.

Per completare questa procedura, è necessario conoscere l'elemento `assetId` dell'asset e l'elemento `propertyId` della proprietà. Puoi anche usare l'ID esterno. Se hai creato una risorsa e non la conosci`assetId`, utilizza l'ListAssetsAPI per elencare tutte le risorse per un modello specifico.

Utilizzate l'DescribeAssetoperazione per visualizzare le proprietà della risorsa, compresi gli ID delle proprietà.

Utilizzate l'BatchPutAssetPropertyValueoperazione per assegnare i valori degli attributi alla risorsa. È possibile utilizzare questa operazione per impostare più attributi contemporaneamente. Il payload di questa operazione include un elenco di voci, ciascuna delle quali contenente l'ID asset, l'ID proprietà e il valore dell'attributo.

Per aggiornare il valore di un attributo ()AWS CLI

1. Crea un file denominato `batch-put-payload.json` e copia il seguente oggetto JSON nel file. Questo esempio di payload mostra come impostare la latitudine e la longitudine di una turbina eolica. Aggiorna gli ID, i valori e i timestamp per modificare il payload per il tuo caso d'uso.

```
{
  "entries": [
    {
      "entryId": "windfarm3-turbine7-latitude",
      "assetId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
      "propertyId": "a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
      "propertyValues": [
        {
          "value": {
            "doubleValue": 47.6204
          },
          "timestamp": {
            "timeInSeconds": 1575691200
          }
        }
      ]
    },
    {
      "entryId": "windfarm3-turbine7-longitude",
      "assetId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
      "propertyId": "a1b2c3d4-5678-90ab-cdef-55555EXAMPLE",
      "propertyValues": [
        {
          "value": {
            "doubleValue": 122.3491
          },
          "timestamp": {
            "timeInSeconds": 1575691200
```

```
          }
        }
      ]
    }
  ]
}
```

- Ogni voce nel payload contiene un `entryId` che è possibile definire come una qualsiasi stringa univoca. Se una richiesta non riesce, ciascun errore conterrà l'`entryId` della richiesta corrispondente in modo che sia possibile sapere quale richiesta riprovare.
- Per impostare il valore di un attributo, è possibile includere una struttura timestamp-quality-value (TQV) nell'elenco di ogni proprietà dell'`propertyValues`attributo. Questa struttura deve contenere il nuovo `value` e il `timestamp` corrente.
  - `value`— Una struttura che contiene uno dei seguenti campi, a seconda del tipo di proprietà impostata:
    - `booleanValue`
    - `doubleValue`
    - `integerValue`
    - `stringValue`
  - `timestamp`— Una struttura che contiene l'ora attuale dell'epoca Unix in secondi,. `timeInSeconds` AWS IoT SiteWise rifiuta tutti i punti dati con timestamp che esistevano da più di 7 giorni nel passato o più recenti di 5 minuti nelle future.

Per ulteriori informazioni su come preparare un payload per, consulta. BatchPutAssetPropertyValueAcquisizione di dati tramite l'API AWS IoT SiteWise

2. Eseguite il comando seguente per inviare i valori degli attributi a AWS IoT SiteWise:

```
aws iotsitewise batch-put-asset-property-value -\-cli-input-json file://batch-put-payload.json
```

Risposta agli allarmi

Quando un AWS IoT Events allarme cambia stato, puoi fare quanto segue per rispondere all'allarme:

- Conferma un allarme per indicare che stai gestendo il problema.

- Posticipa una sveglia per disattivarla temporaneamente.
- Disattiva un allarme per disattivarlo in modo permanente fino a quando non lo riabiliti.
- Abilita un allarme disabilitato per rilevare lo stato dell'allarme.
- Reimposta un allarme per cancellarne lo stato e l'ultimo valore.

Puoi utilizzare la AWS IoT SiteWise console o l' AWS IoT Events API per rispondere a un allarme.

> **Note**
>
> È possibile rispondere agli AWS IoT Events allarmi, ma non agli allarmi esterni.

Argomenti

Risposta a un allarme (console)

Puoi utilizzare la AWS IoT SiteWise console per confermare, posticipare, disabilitare o attivare un allarme.

Argomenti

Riconoscere un allarme (console)

Puoi confermare un allarme per indicare che stai gestendo il problema.

> **Note**
>
> È necessario abilitare il flusso di conferma sull'allarme in modo da poter confermare l'allarme. Questa opzione è abilitata di default se si definisce l'allarme dalla AWS IoT SiteWise console.

Per confermare un allarme (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Asset.
3. Scegliete la risorsa per la quale desiderate confermare un allarme.

   > **Tip**
   >
   > Puoi scegliere l'icona a forma di freccia per espandere una gerarchia di asset e trovare il tuo asset.

4. Scegli la scheda Allarmi.
5. Seleziona l'allarme da confermare, quindi scegli Azioni per aprire il menu delle azioni di risposta.
6. Scegli Riconosci. Lo stato dell'allarme cambia in Riconosciuto.

Posticipa una sveglia (console)

È possibile posticipare una sveglia per disattivarla temporaneamente. Specificate la durata per cui posticipare la sveglia.

Per posticipare una sveglia (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Asset.
3. Scegliete la risorsa per la quale desiderate posticipare una sveglia.

   > **Tip**
   >
   > Puoi scegliere l'icona a forma di freccia per espandere una gerarchia di asset e trovare il tuo asset.

4. Scegli la scheda Allarmi.
5. Seleziona la sveglia da posticipare, quindi scegli Azioni per aprire il menu delle azioni di risposta.
6. Scegli Snooze. Si apre un modello in cui si specifica la durata dello snooze.
7. Scegliete la lunghezza dello snooze o inserite una lunghezza dello snooze personalizzata.
8. Selezionare Salva. Lo stato della sveglia cambia in Snoozed.

Disattiva un allarme (console)

Puoi disabilitare un allarme in modo che non venga più rilevato. Dopo aver disattivato l'allarme, è necessario riattivarlo se si desidera che l'allarme venga rilevato.

Per disattivare un allarme (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Asset.
3. Scegliete la risorsa per cui desiderate disattivare un allarme.

> **Tip**
>
> Puoi scegliere l'icona a forma di freccia per espandere una gerarchia di asset e trovare il tuo asset.

4. Scegli la scheda Allarmi.
5. Seleziona l'allarme da disabilitare, quindi scegli Azioni per aprire il menu delle azioni di risposta.
6. Scegliere Disabilita. Lo stato dell'allarme diventa Disabilitato.

Abilita un allarme (console)

È possibile abilitare nuovamente il rilevamento di un allarme dopo averlo disattivato o posticipato.

Per abilitare un allarme (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Asset.
3. Scegliete la risorsa per la quale desiderate attivare un allarme.

> **Tip**
>
> Puoi scegliere l'icona a forma di freccia per espandere una gerarchia di asset e trovare il tuo asset.

4. Scegli la scheda Allarmi.
5. Seleziona l'allarme da abilitare, quindi scegli Azioni per aprire il menu delle azioni di risposta.
6. Scegli Abilita . Lo stato dell'allarme passa a Normale.

Reimpostazione di un allarme (console)

È possibile reimpostare un allarme per cancellarne lo stato e l'ultimo valore.

Per resettare un allarme (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Asset.
3. Scegliete la risorsa per la quale desiderate reimpostare un allarme.

> **Tip**
>
> Puoi scegliere l'icona a forma di freccia per espandere una gerarchia di asset e trovare il tuo asset.

4. Scegli la scheda Allarmi.
5. Seleziona l'allarme da abilitare, quindi scegli Azioni per aprire il menu delle azioni di risposta.
6. Scegliere Reimposta. Lo stato dell'allarme passa a Normale.

Risposta a un allarme (API)

Puoi utilizzare l' AWS IoT Events API per confermare, posticipare, disabilitare, abilitare o reimpostare un allarme. Per ulteriori informazioni, consulta le seguenti operazioni nell'AWS IoT Events API Reference:

- BatchAcknowledgeAlarm

- BatchSnoozeAlarm
- BatchDisableAlarm
- BatchEnableAlarm
- BatchResetAlarm

Per ulteriori informazioni, consulta Rispondere agli allarmi nella Guida per gli AWS IoT Events sviluppatori.

Acquisizione dello stato di allarme esterno

Gli allarmi esterni sono allarmi che vengono valutati all'esterno. AWS IoT SiteWise Puoi utilizzare allarmi esterni quando disponi di una fonte di dati che riporta lo stato dell'allarme che desideri importare. AWS IoT SiteWise

Le proprietà dello stato di allarme richiedono un formato specifico per i valori dei dati dello stato di allarme. Ogni valore di dati deve essere un oggetto JSON serializzato su una stringa. Quindi, si inserisce la stringa serializzata come valore di stringa. Per ulteriori informazioni, consulta Proprietà dello stato di allarme.

Example Esempio di valore dei dati sullo stato di allarme (non serializzato)

```
{
  "stateName": "Active"
}
```

Example Esempio di valore dei dati sullo stato di allarme (serializzato)

```
{\"stateName\":\"Active\"}
```

> **Note**
>
> Se la tua fonte di dati non può riportare dati in questo formato o non puoi convertire i dati in questo formato prima di inserirli, puoi scegliere di non utilizzare una proprietà di allarme. Puoi invece importare i dati come proprietà di misurazione con il tipo di dati stringa, ad esempio. Per ulteriori informazioni, consulta Definizione dei flussi di dati provenienti dalle apparecchiature (misurazioni) e Inserimento di dati in AWS IoT SiteWise.

Mappatura dei flussi di stato di allarme esterni

È possibile definire alias di proprietà per mappare i flussi di dati alle proprietà dello stato di allarme. Ciò consente di identificare facilmente una proprietà dello stato di allarme quando si inseriscono o recuperano dati. Per ulteriori informazioni sugli alias di proprietà, vedere. Mappatura dei flussi di dati industriali alle proprietà degli asset

Argomenti

Mappatura dei flussi di stato di allarme esterni (console)

È possibile definire alias di proprietà per mappare i flussi di dati alle proprietà dello stato di allarme. Ciò consente di identificare facilmente una proprietà dello stato di allarme quando si inseriscono o recuperano dati. Per ulteriori informazioni sugli alias di proprietà, vedere. Mappatura dei flussi di dati industriali alle proprietà degli asset

È possibile utilizzare la AWS IoT SiteWise console per impostare un alias per una proprietà dello stato di allarme.

Per impostare un alias di proprietà per una proprietà dello stato di allarme (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Asset.
3. Scegli l'asset per cui vuoi impostare un alias di proprietà.

   > **Tip**
   >
   > Puoi scegliere l'icona a forma di freccia per espandere una gerarchia di asset e trovare il tuo asset.

4. Scegliere Alarms (Allarmi).
5. Seleziona l'allarme esterno per il quale desideri impostare un alias di proprietà.
6. Scegliere Visualizza.
7. Nel riquadro dei dettagli dello stato dell'allarme, scegli Modifica.
8. Inserisci l'alias della proprietà.

9. Scegli Aggiorna.

Mappatura dei flussi di stato di allarme esterni ()AWS CLI

È possibile definire alias di proprietà per mappare i flussi di dati alle proprietà dello stato di allarme. Ciò consente di identificare facilmente una proprietà dello stato di allarme quando si inseriscono o recuperano dati. Per ulteriori informazioni sugli alias di proprietà, vedere. Mappatura dei flussi di dati industriali alle proprietà degli asset

È possibile utilizzare AWS Command Line Interface (AWS CLI) per impostare un alias per una proprietà dello stato di allarme.

Per completare questa procedura, è necessario conoscere l'elemento `assetId` dell'asset e l'elemento `propertyId` della proprietà. È inoltre possibile utilizzare l'ID esterno. Se hai creato una risorsa e non la conosci`assetId`, utilizza l'ListAssetsAPI per elencare tutte le risorse per un modello specifico. Utilizzate l'DescribeAssetoperazione per visualizzare le proprietà della risorsa, compresi gli ID delle proprietà.

> **Note**
>
> La DescribeAssetrisposta include l'elenco di modelli di asset compositi per l'asset. Ogni allarme è un modello composito. Per trovare il`propertyId`, trova il modello composito per l'allarme, quindi trova la `AWS/ALARM_STATE` proprietà in quel modello composito.

Per ulteriori informazioni su come impostare l'alias della proprietà, vedereImpostazione di un alias di proprietà ()AWS CLI.

Acquisizione dei dati sullo stato dell'allarme

Le proprietà dello stato di allarme prevedono che lo stato di allarme sia una stringa JSON serializzata. Per importare lo stato di allarme in un allarme esterno in AWS IoT SiteWise, si inserisce questa stringa serializzata come valore di stringa con data e ora. L'esempio seguente mostra un valore di dati di stato per un allarme attivo.

```
{\"stateName\":\"Active\"}
```

Per identificare una proprietà dello stato di allarme, puoi specificare una delle seguenti opzioni:

- La `assetId` fine `propertyId` della proprietà di allarme a cui stai inviando i dati.
- Il`propertyAlias`, che è un alias di flusso di dati (ad esempio,`/company/windfarm/3/turbine/7/temperature/high`). Per utilizzare questa opzione, devi prima impostare l'alias della proprietà di allarme. Per informazioni su come impostare gli alias di proprietà per le proprietà dello stato di allarme, vedi. Mappatura dei flussi di stato di allarme esterni

Il seguente esempio di BatchPutAssetPropertyValueAPI payload mostra come formattare lo stato di un allarme esterno. Questo allarme esterno segnala quando la lettura dei giri al minuto (RPM) di una turbina eolica è troppo alta.

Example Esempio di BatchPutAssetPropertyValue payload per i dati sullo stato di allarme

```
{
    "entries": [
      {
        "entryId": "unique entry ID",
        "propertyAlias": "/company/windfarm/3/turbine/7/temperature/high",
        "propertyValues": [
          {
            "value": {
              "stringValue": "{\"stateName\":\"Active\"}"
            },
            "timestamp": {
              "timeInSeconds": 1607550262
            }
          }
        ]
      }
    ]
  }
```

Per ulteriori informazioni su come utilizzare l'`BatchPutAssetPropertyValue`API per importare dati, consulta. Acquisizione di dati tramite l'API AWS IoT SiteWise

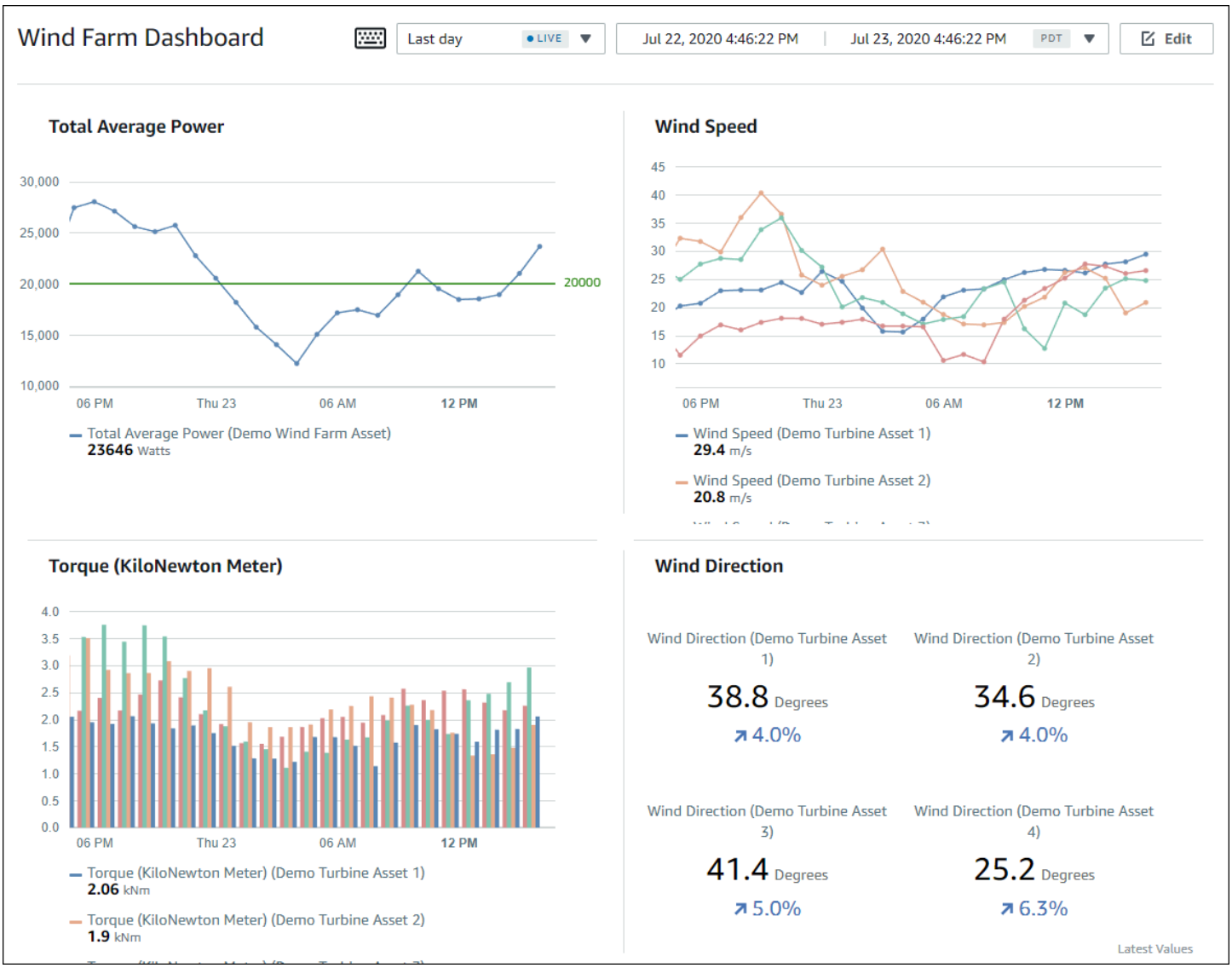
Per ulteriori informazioni su altri modi di importare dati, consulta. Inserimento di dati in AWS IoT SiteWise

Monitoraggio dei dati con AWS IoT SiteWise Monitor

Puoi utilizzarli AWS IoT SiteWise per monitorare i dati provenienti da processi, dispositivi e apparecchiature creando portali web SiteWise Monitor. SiteWise Monitor è una funzionalità AWS IoT SiteWise che puoi utilizzare per creare portali sotto forma di un'applicazione web gestita. utili a visualizzare e condividere i propri dati operativi. Puoi creare dei progetti con i pannelli di controllo per visualizzare i dati di processi, dispositivi e apparecchiature connessi a AWS IoT.

I portali consentono agli esperti dei domini, quali gli ingegneri di processo, di reperire immediatamente informazioni sui dati operativi e comprendere il comportamento dei dispositivi e delle apparecchiature.

Di seguito è riportato un pannello di controllo esemplificativo che mostra i dati relativi a un parco eolico.



Poiché AWS IoT SiteWise acquisisce i dati nel tempo, puoi utilizzare SiteWise Monitor per visualizzare i dati operativi nel tempo o gli ultimi valori riportati in momenti specifici. e, di conseguenza, notare o reperire andamenti o informazioni altrimenti difficili da rilevare.

SiteWise Monitora i ruoli

Quattro ruoli interagiscono con SiteWise Monitor:

AWS amministratore

L' AWS amministratore utilizza la AWS IoT SiteWise console per creare portali. L'amministratore AWS può anche assegnare gli amministratori per il portale e aggiungere gli utenti del portale.

Gli amministratori del portale assegnano successivamente gli utenti del portale ai progetti come proprietari o visualizzatori. L' AWS amministratore lavora esclusivamente nella AWS console.

Amministratore del portale

Ogni portale SiteWise Monitor ha uno o più amministratori del portale. Gli amministratori del portale utilizzano il portale per creare progetti che contengono raccolte di asset e pannelli di controllo. L'amministratore del portale assegna quindi asset e proprietari a ciascun progetto. Controllando l'accesso al progetto, gli amministratori del portale specificano quali asset possono vedere i proprietari e i visualizzatori del progetto.

Proprietario del progetto

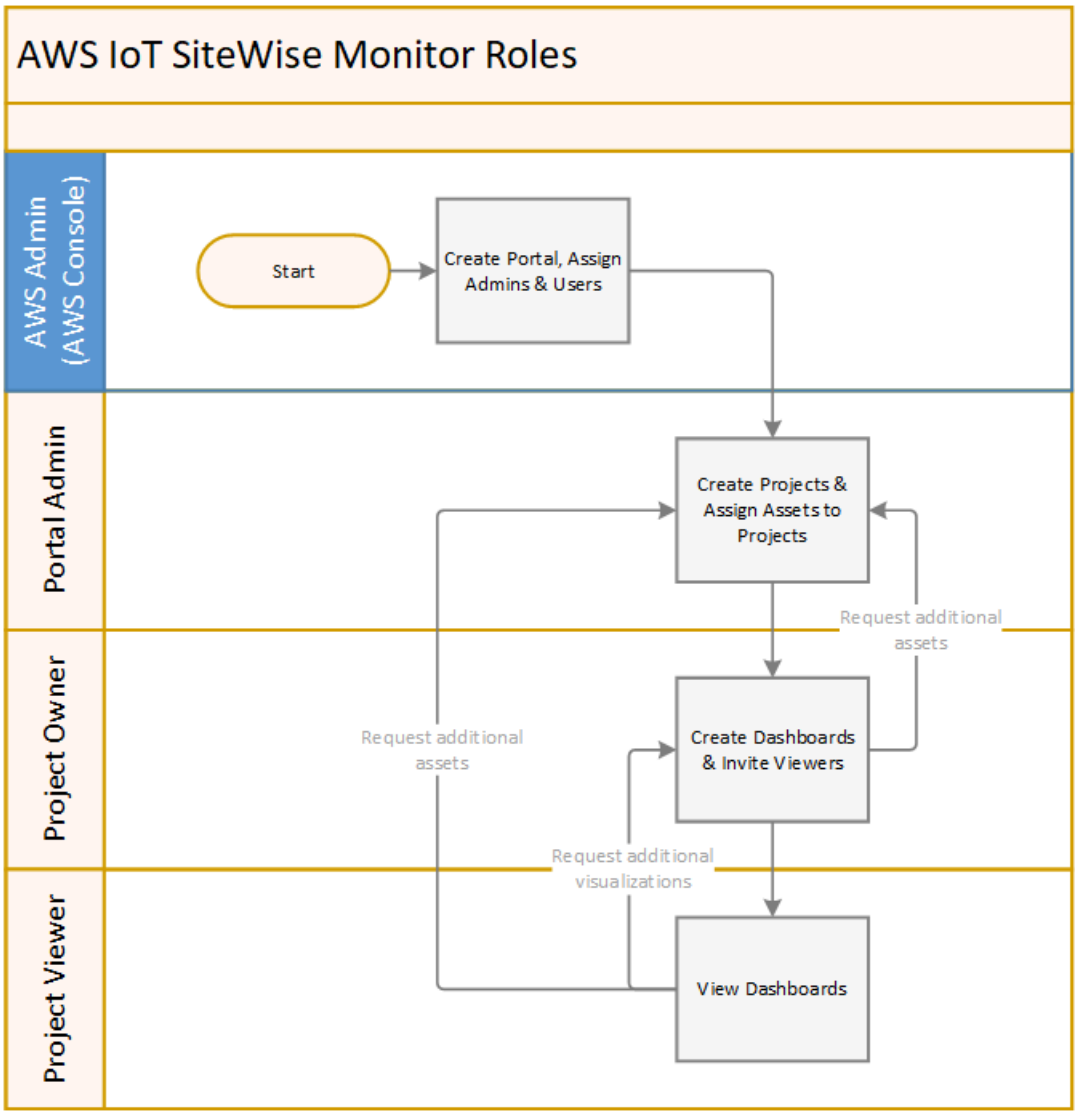
Ogni progetto SiteWise Monitor ha dei proprietari. I proprietari dei progetti creano visualizzazioni sotto forma di pannelli di controllo al fine di rappresentare i dati operativi in modo coerente. Una volta che i pannelli di controllo sono pronti per la condivisione, il proprietario del progetto può invitare i visualizzatori al progetto. I proprietari del progetto possono anche assegnare altri proprietari al progetto. I proprietari dei progetti possono configurare le soglie e le impostazioni di notifica per gli allarmi.

Visualizzatore del progetto

Ogni progetto SiteWise Monitor ha dei visualizzatori. I visualizzatori del progetto possono connettersi al portale per visualizzare i pannelli di controllo creati dai proprietari del progetto. In ogni dashboard, i visualizzatori dei progetti possono regolare l'intervallo di tempo per comprendere meglio i dati operativi. I visualizzatori del progetto possono visualizzare solo i pannelli di controllo nei progetti a cui hanno accesso. I visualizzatori del progetto possono confermare e posticipare gli allarmi.

A seconda dell'organizzazione, la stessa persona potrebbe svolgere più ruoli.

L'immagine seguente illustra come questi quattro ruoli interagiscono nel portale Monitor. SiteWise



Puoi gestire chi ha accesso ai tuoi dati utilizzando AWS IAM Identity Center o IAM. Gli utenti dei tuoi dati possono accedere a SiteWise Monitor da un browser desktop o mobile utilizzando le proprie credenziali IAM Identity Center o IAM.

Federazione SAML

IAM Identity Center e IAM supportano la federazione delle identità con SAML (Security Assertion Markup Language) 2.0. SAML 2.0 è uno standard aperto utilizzato da molti provider di identità esterni (IdPs) per autenticare gli utenti e trasmettere le informazioni relative all'identità e alla sicurezza ai provider di servizi (SP). Gli SP sono in genere applicazioni o servizi. La federazione SAML consente agli amministratori e agli utenti del portale SiteWise Monitor di accedere ai portali assegnati con credenziali esterne, come nomi utente e password aziendali.

Puoi configurare IAM Identity Center e IAM per utilizzare la federazione basata su SAML per l'accesso ai portali Monitor. SiteWise

IAM Identity Center

Gli amministratori e gli utenti del portale possono accedere al portale di AWS accesso con i loro nomi utente e password aziendali. Possono quindi accedere ai portali Monitor assegnati SiteWise . IAM Identity Center utilizza i certificati per impostare una relazione di fiducia SAML tra il tuo provider di identità e. AWSPer ulteriori informazioni, consulta il profilo SCIM e l'implementazione SAML 2.0 nella Guida per l'AWS IAM Identity Center utente.

IAM

Gli amministratori e gli utenti del portale possono richiedere credenziali di sicurezza temporanee per accedere ai portali Monitor loro assegnati. SiteWise Crei un'identità di provider di identità SAML in IAM per impostare una relazione di fiducia tra il tuo provider di identità e. AWS Per ulteriori informazioni, consulta Utilizzo della federazione basata su SAML per l'accesso alle API AWS, nella Guida per l'utente IAM.

Gli amministratori e gli utenti del portale possono accedere al portale aziendale e selezionare l'opzione per accedere alla AWS console di gestione. Possono quindi accedere ai portali SiteWise Monitor assegnati. Il portale della tua azienda gestisce lo scambio di fiducia tra il tuo provider di identità e AWS. Per ulteriori informazioni, consulta Abilitare gli utenti federati SAML 2.0 ad accedere alla Console di AWS gestione nella Guida per l'utente IAM.

> **Note**
>
> Quando aggiungi utenti o amministratori al portale, evita di creare policy IAM che limitino le autorizzazioni degli utenti, come un IP limitato. Qualsiasi policy allegata con autorizzazioni limitate non sarà in grado di connettersi al portale. AWS IoT SiteWise

SiteWise Monitora i concetti

Per utilizzare SiteWise Monitor, è necessario conoscere i seguenti concetti:

Portal

Un AWS IoT SiteWise Monitor portale è un'applicazione web che è possibile utilizzare per visualizzare e condividere AWS IoT SiteWise i dati. Un portale ha uno o più amministratori e contiene zero o più progetti.

Progetto

Ogni portale SiteWise Monitor contiene una serie di progetti. Ogni progetto ha un sottoinsieme di asset AWS IoT SiteWise associati. I proprietari del progetto creano uno o più pannelli di controllo per fornire un modo coerente per visualizzare i dati associati agli asset. I proprietari del progetto possono invitare i visualizzatori al progetto per consentire loro di visualizzare gli asset e i pannelli di controllo del progetto. Il progetto è l'unità di condivisione di base all'interno di SiteWise Monitor. I proprietari del progetto possono invitare gli utenti a cui l' AWS amministratore ha concesso l'accesso al portale. Un utente deve avere accesso a un portale prima che un progetto del portale possa essere condiviso con l'utente.

Asset

Quando i dati vengono importati AWS IoT SiteWise dalle apparecchiature industriali, i dispositivi, le apparecchiature e i processi vengono rappresentati ciascuno come risorse. A ogni risorsa sono associati proprietà e allarmi. L'amministratore del portale assegna i set di asset a ciascun progetto.

Proprietà

Le proprietà sono dati di serie temporali associati agli asset. Ad esempio, un pezzo di apparecchiatura può avere un numero di serie, una posizione, una marca e un modello e una data di installazione. Può anche avere valori di serie temporali per disponibilità, prestazioni, qualità, temperatura, pressione e così via.

Allarme

Gli allarmi monitorano le proprietà per identificare quando l'apparecchiatura si trova al di fuori del suo intervallo operativo. Ogni allarme definisce una soglia e una proprietà da monitorare. Quando la proprietà supera la soglia, l'allarme diventa attivo e indica che tu o qualcuno del tuo team dovete risolvere il problema. I proprietari del progetto possono personalizzare le soglie e le impostazioni di notifica per gli allarmi. I visualizzatori del progetto possono confermare e posticipare gli allarmi e possono lasciare un messaggio con i dettagli sull'allarme o sull'azione che hanno intrapreso per risolverlo.

Dashboard

Ogni progetto contiene un set di pannelli di controllo. I pannelli di controllo forniscono un set di visualizzazioni per i valori di un set di asset. I proprietari del progetto creano i pannelli di controllo e le visualizzazioni contenute. Quando il proprietario di un progetto è pronto a condividere il set di pannelli di controllo, il proprietario può invitare i visualizzatori al progetto, consentendo loro di accedere a tutti i pannelli di controllo del progetto. Se si desidera un set diverso di visualizzatori per pannelli di controllo diversi, è necessario dividere i pannelli di controllo tra i progetti. Quando gli spettatori guardano le dashboard, possono personalizzare l'intervallo di tempo per esaminare dati specifici.

Visualizzazione

In ogni dashboard, i proprietari del progetto decidono come visualizzare le proprietà e gli allarmi delle risorse associate al progetto. La disponibilità potrebbe essere rappresentata come un grafico a linee, mentre altri valori potrebbero essere visualizzati come grafici a barre o indicatori chiave di prestazione (KPI). Gli allarmi vengono visualizzati al meglio come griglie di stato e linee temporali di stato. I proprietari del progetto personalizzano ogni visualizzazione per fornire la migliore comprensione dei dati per l'asset.

Guida introduttiva con AWS IoT SiteWise Monitor

Se sei l' AWS amministratore della tua organizzazione, crei portali dalla AWS IoT SiteWise console. Completa i seguenti passaggi per creare un portale in modo che i membri della tua organizzazione possano visualizzare AWS IoT SiteWise i tuoi dati:

1. Configurare e creare un portale
2. Aggiungere amministratori del portale e inviare e-mail di invito
3. Aggiungere utenti del portale

Dopo aver creato un portale, l'amministratore del portale può visualizzare le AWS IoT SiteWise risorse e assegnarle ai progetti del portale. A questo punto, i proprietari di progetto possono creare pannelli di controllo per la visualizzazione delle proprietà degli asset che consentano ai visualizzatori di progetto di appurare le prestazioni di dispositivi, processi e apparecchiature.

> **Note**
>
> Quando aggiungete utenti o amministratori al portale, evitate di creare policy AWS Identity and Access Management (IAM) che limitino le autorizzazioni degli utenti, come l'IP limitato. Qualsiasi policy allegata con autorizzazioni limitate non sarà in grado di connettersi al portale. AWS IoT SiteWise

Puoi seguire un tutorial che illustra i passaggi necessari per configurare un portale con un progetto, pannelli di controllo e diversi utenti per uno scenario specifico utilizzando i dati della centrale eolica. Per ulteriori informazioni, consulta Visualizzazione e condivisione dei dati dei parchi eolici in Monitor SiteWise .

Argomenti

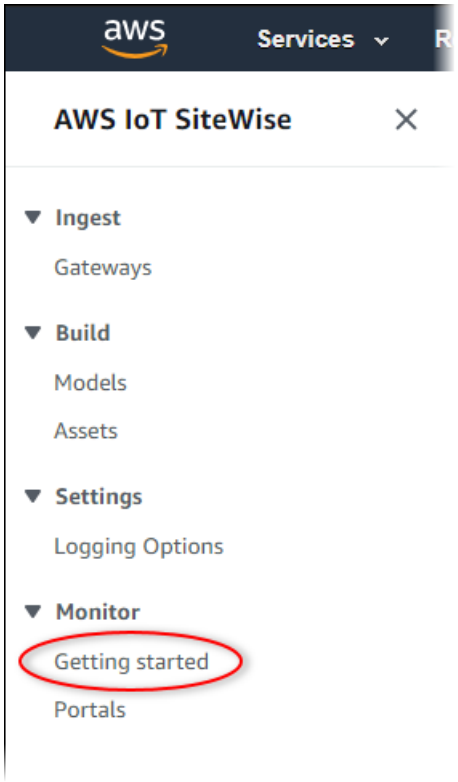
- Creazione di un portale
- Configurazione del portale
- Invito degli amministratori
- Aggiunta di utenti del portale

Creazione di un portale

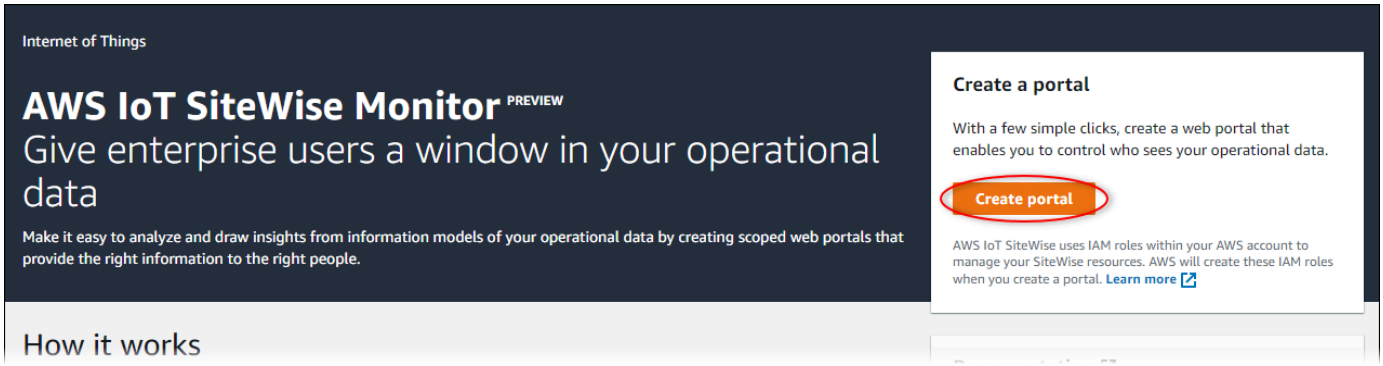
Crei un portale SiteWise Monitor nella AWS IoT SiteWise console.

Per creare un portale

1. Accedi alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, selezionare Monitor (Monitoraggio), Getting started (Operazioni di base).



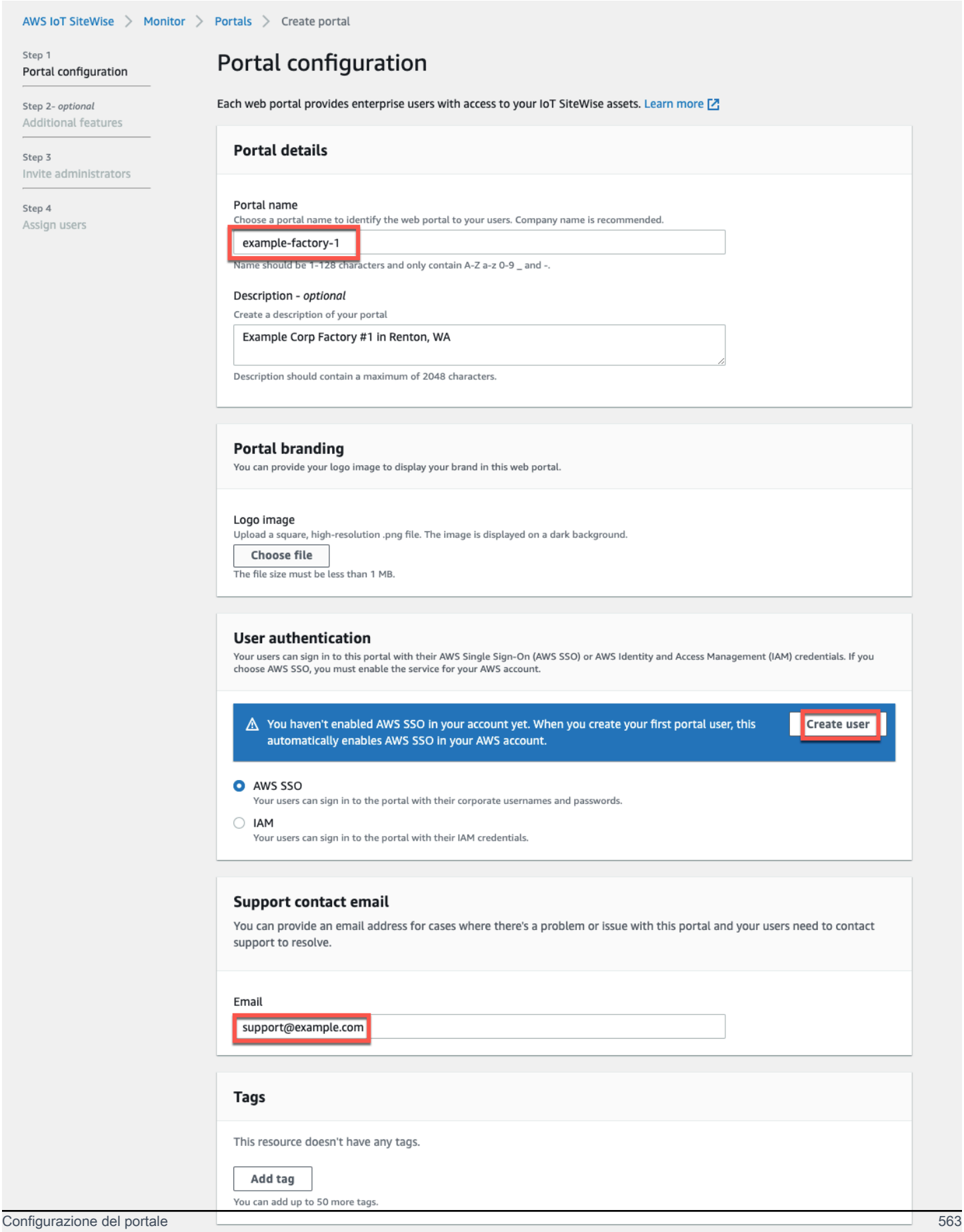
3. Selezionare Create Portal (Crea portale).



Successivamente, bisogna fornire alcune informazioni di base per la configurazione del portale.

Configurazione del portale

Gli utenti utilizzano i portali per visualizzare i tuoi dati. Puoi personalizzare il nome, la descrizione, il marchio, l'autenticazione dell'utente, l'email di contatto dell'assistenza e le autorizzazioni di un portale.


AWS IoT SiteWise > Monitor > Portals > Create portal
Step 1
Portal configuration
Step 2- optional
Additional features
Step 3
Invite administrators
Step 4
Assign users
Portal configuration
Each web portal provides enterprise users with access to your IoT SiteWise assets. Learn more
Portal details
Portal name
Choose a portal name to identify the web portal to your users. Company name is recommended.
example-factory-1
Name should be 1-128 characters and only contain A-Z a-z 0-9 _ and -.
Description - optional
Create a description of your portal
Example Corp Factory #1 in Renton, WA
Description should contain a maximum of 2048 characters.
Portal branding
You can provide your logo image to display your brand in this web portal.
Logo image
Upload a square, high-resolution .png file. The image is displayed on a dark background.
Choose file
The file size must be less than 1 MB.
User authentication
Your users can sign in to this portal with their AWS Single Sign-On (AWS SSO) or AWS Identity and Access Management (IAM) credentials. If you choose AWS SSO, you must enable the service for your AWS account.
You haven't enabled AWS SSO in your account yet. When you create your first portal user, this automatically enables AWS SSO in your AWS account.
Create user
AWS SSO
Your users can sign in to the portal with their corporate usernames and passwords.
IAM
Your users can sign in to the portal with their IAM credentials.
Support contact email
You can provide an email address for cases where there's a problem or issue with this portal and your users need to contact support to resolve.
Email
support@example.com
Tags
This resource doesn't have any tags.
Add tag
You can add up to 50 more tags.
Permissions
SiteWise Monitor assumes this role to give permissions to your federated users to access AWS IoT SiteWise resources. Learn

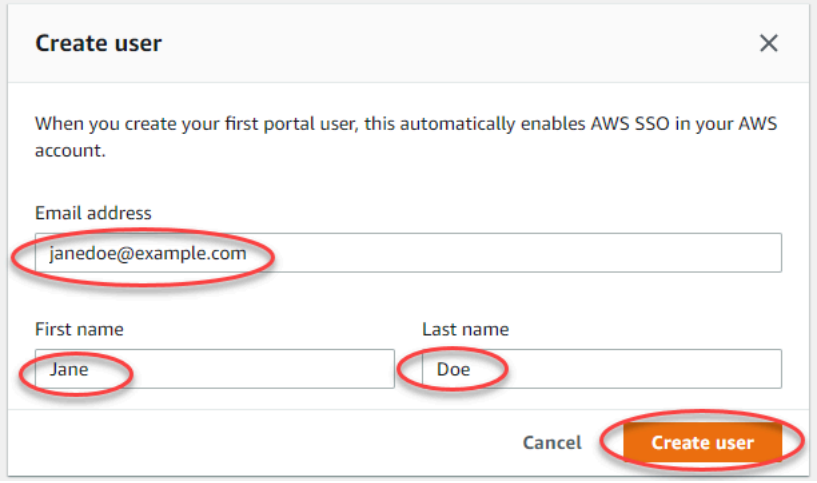
Per configurare un portale

1. Immettere un nome da assegnare al portale.
2. (Facoltativo) Inserire una descrizione del portale. Se si dispone di più portali, occorre utilizzare descrizioni significative per tenere traccia dei contenuti di ciascuno.
3. (Facoltativo) Caricare un'immagine per visualizzare il marchio nel portale. Scegliere un'immagine PNG quadrata. Se si carica un'immagine non quadrata, il portale ridimensiona l'immagine in un quadrato.
4. Selezionare una delle seguenti opzioni:
   - Scegli IAM Identity Center se gli utenti del tuo portale accedono a questo portale con i loro nomi utente e password aziendali.

     Se non hai abilitato IAM Identity Center nel tuo account, procedi come segue:

     a. Selezionare Create user (Crea utente).

     b. Nella pagina Crea utente, per creare il primo portale, inserisci l'indirizzo e-mail, il nome e il cognome dell'utente, quindi scegli Crea utente.



> **Note**
>
> - AWS abilita automaticamente IAM Identity Center nel tuo account quando crei il primo utente del portale.
> - Puoi configurare IAM Identity Center in una sola regione alla volta. SiteWise Monitor si connette alla regione che hai configurato per IAM Identity Center.

Ciò significa che utilizzi una regione per l'accesso a IAM Identity Center, ma puoi creare portali in qualsiasi regione.

- Scegli IAM se gli utenti del portale accedono a questo portale con le proprie credenziali IAM.

> **Important**
>
> Gli utenti o i ruoli devono disporre dell'`iotsitewise:DescribePortal`autorizzazione per accedere al portale.

5. Immettere un indirizzo e-mail che gli utenti del portale possano contattare, in caso di dubbi o problemi, per trovare una soluzione.
6. (Facoltativo) Aggiungere tag per il portale. Per ulteriori informazioni, consulta Taggare le tue risorse AWS IoT SiteWise.
7. Selezionare una delle seguenti opzioni:
   - Scegli Crea e usa un nuovo ruolo di servizio. Per impostazione predefinita, SiteWise Monitor crea automaticamente un ruolo di servizio per ogni portale. Questo ruolo consente agli utenti del portale di accedere alle AWS IoT SiteWise risorse dell'utente. Per ulteriori informazioni, consulta Utilizzo dei ruoli di servizio per AWS IoT SiteWise Monitor.
   - Scegli Usa un ruolo di servizio esistente, quindi scegli il ruolo di destinazione.
8. Seleziona Next (Successivo).
9. (Facoltativo) Abilita gli allarmi per il tuo portale. Per ulteriori informazioni, consulta Attivazione degli allarmi per i tuoi portali.
10. Scegli Crea. AWS IoT SiteWise creerà il tuo portale.

> **Note**
>
> Se si chiude la console, è possibile completare la procedura di configurazione aggiungendo amministratori e utenti. Per ulteriori informazioni, consulta Aggiunta o rimozione di amministratori del portale. Se non desideri conservare questo portale, eliminalo in modo che non utilizzi risorse. Per ulteriori informazioni, consulta Eliminazione di un portale.

La colonna Status può avere uno dei seguenti valori.

- CREATING - AWS IoT SiteWise sta elaborando la richiesta di creazione del portale. Il completamento di questo processo può richiedere diversi minuti.
- AGGIORNAMENTO - AWS IoT SiteWise sta elaborando la richiesta di aggiornamento del portale. Il completamento di questo processo può richiedere alcuni minuti.
- PENDING - AWS IoT SiteWise è in attesa del termine della propagazione dei record DNS. Il completamento di questo processo può richiedere diversi minuti. È possibile eliminare il portale mentre lo stato è IN SOSPESO.
- ELIMINAZIONE - AWS IoT SiteWise sta elaborando la richiesta di eliminazione del portale. Il completamento di questo processo può richiedere diversi minuti.
- ATTIVO - Quando il portale diventa attivo, gli utenti del portale possono accedervi.
- FALLITO - AWS IoT SiteWise impossibile elaborare la richiesta di creazione, aggiornamento o eliminazione del portale. Se hai abilitato AWS IoT SiteWise l'invio di log ad Amazon CloudWatch Logs, puoi utilizzare questi log per risolvere i problemi. Per ulteriori informazioni, consulta Monitoring with Logs. AWS IoT SiteWise CloudWatch

Una volta creato il portale, viene visualizzato un messaggio.

Successivamente, bisogna invitare al portale uno o più utenti che fungano da amministratori. A questo punto, è stato creato un portale al quale nessuno, però, può accedere.

Invito degli amministratori

Per iniziare a usare il nuovo portale, è necessario assegnare un amministratore del portale. L'amministratore del portale crea i progetti, ne sceglie i proprietari e vi assegna gli asset necessari. Gli amministratori del portale possono vedere tutte le tue AWS IoT SiteWise risorse.

In base al servizio di autenticazione utente, scegli una delle seguenti opzioni:

IAM Identity Center

Se utilizzi SiteWise Monitor per la prima volta, puoi scegliere l'utente che hai creato in precedenza come amministratore del portale. Se desideri aggiungere un altro utente come amministratore del portale, puoi creare un utente IAM Identity Center da questa pagina. In alternativa, puoi

connettere un provider di identità esterno a IAM Identity Center. Per ulteriori informazioni, consulta la AWS IAM Identity Center Guida per l'utente.

Come invitare gli amministratori

1. Selezionare le caselle di controllo riferite agli utenti da nominare amministratori del portale. Questo aggiunge gli utenti all'elenco degli amministratori del portale.

   > **Note**
   >
   > Se utilizzi IAM Identity Center come archivio di identità e hai effettuato l'accesso al tuo account di AWS Organizations gestione, puoi scegliere Crea utente per creare un utente IAM Identity Center. IAM Identity Center invia al nuovo utente un'e-mail per consentirgli di impostare la password. È quindi possibile assegnare l'utente al portale come amministratore. Per ulteriori informazioni, consulta la sezione Gestione delle identità in IAM Identity Center.

2. Facoltativamente, è possibile avvalersi del comando Send invite to selected users (Manda un invito agli utenti selezionati). Viene visualizzato il client di posta elettronica e nel corpo del messaggio viene popolato un invito.

   È possibile personalizzare il messaggio e-mail prima di inviarlo agli amministratori del portale. È inoltre possibile inviare l'e-mail agli amministratori del portale in un secondo momento. Se stai provando SiteWise Monitor per la prima volta e aggiungi il tuo nuovo utente o ruolo IAM Identity Center o IAM come amministratore del portale, non devi inviarti un'e-mail.

3. Se si aggiunge un utente indesiderato come amministratore, per risolvere basta deselezionarne la casella di controllo.

4. Una volta invitati gli amministratori del portale, bisogna selezionare Next (Avanti).

IAM

Puoi scegliere un utente o un ruolo come amministratore del portale. Se desideri aggiungere un altro utente o ruolo come amministratore del portale, puoi creare un utente o un ruolo nella console IAM. Per ulteriori informazioni, consulta Creazione di un utente IAM nel tuo AWS account e Creazione di ruoli IAM nella Guida per l'utente IAM.

Come invitare gli amministratori

1. Esegui questa operazione:
   - Scegli gli utenti IAM per aggiungere un utente IAM come amministratore del portale.
   - Scegli i ruoli IAM per aggiungere un ruolo IAM come amministratore del portale.
2. Seleziona le caselle di controllo per gli utenti o i ruoli che desideri come amministratori del portale. Ciò aggiunge gli utenti o i ruoli all'elenco degli amministratori del portale.
3. Se aggiungi un utente o un ruolo che non desideri utilizzare come amministratore, deseleziona la casella di controllo relativa a quell'utente o ruolo.
4. Una volta invitati gli amministratori del portale, bisogna selezionare Next (Avanti).

> **Important**
>
> Gli utenti o i ruoli devono disporre dell'`iotsitewise:DescribePortal`autorizzazione per accedere al portale.

> **Note**
>
> Se utilizzi IAM Identity Center come archivio di identità e hai effettuato l'accesso al tuo account di AWS Organizations gestione, puoi scegliere Crea utente per creare un utente IAM Identity Center. IAM Identity Center invia al nuovo utente un'e-mail per consentirgli di impostare la password. È quindi possibile assegnare l'utente al portale come amministratore. Per ulteriori informazioni, consulta la sezione Gestione delle identità in IAM Identity Center.

Sarà possibile modificare l'elenco degli amministratori del portale, in un secondo momento. Per ulteriori informazioni, consulta Aggiunta o rimozione di amministratori del portale.

> **Note**
>
> Poiché solo un amministratore del portale può creare progetti e assegnare loro risorse, è necessario specificare almeno un amministratore del portale.

Come ultimo passaggio, è possibile aggiungere utenti in grado di accedere al nuovo portale.

Aggiunta di utenti del portale

È possibile controllare quali utenti hanno accesso ai portali. In ogni portale, gli amministratori del portale creano uno o più progetti e assegnano gli utenti del portale come proprietari o visualizzatori per ciascun progetto. Ogni proprietario del progetto può invitare altri utenti del portale a diventare proprietari o visualizzatori del progetto.

In base al servizio di autenticazione utente, scegli una delle seguenti opzioni:

IAM Identity Center

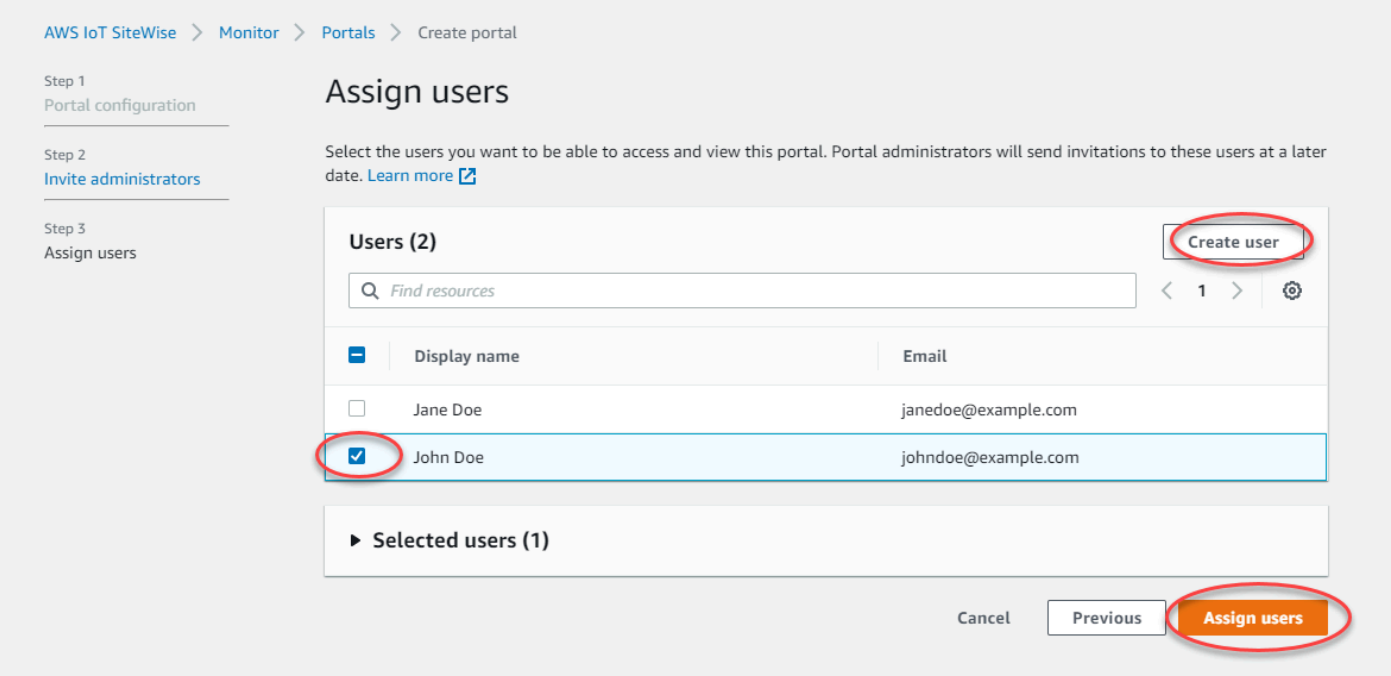
Se desideri aggiungere un utente all'elenco Utenti, completa i seguenti passaggi.

Come aggiungere utenti del portale

1. Scegli gli utenti dall'elenco Utenti da aggiungere al portale. In questo modo gli utenti vengono aggiunti all'elenco degli utenti del portale. Se utilizzi SiteWise Monitor per la prima volta, non è necessario aggiungere l'amministratore del portale come utente del portale.

   > **Note**
   >
   > Se utilizzi IAM Identity Center come archivio di identità e hai effettuato l'accesso al tuo account di AWS Organizations gestione, puoi scegliere Crea utente per creare un utente IAM Identity Center. IAM Identity Center invia al nuovo utente un'e-mail per consentirgli di impostare la password. È quindi possibile assegnare l'utente al portale come utente. Per ulteriori informazioni, consulta la sezione Gestione delle identità in IAM Identity Center.

2. Se si aggiunge e concede l'accesso a un utente indesiderato, per risolvere basta deselezionarne la casella di controllo.
3. Quando hai finito di selezionare gli utenti, scegli Assegna utenti.



IAM

Se vedi l'utente o il ruolo che desideri aggiungere nell'elenco degli utenti o dei ruoli IAM, completa i seguenti passaggi.

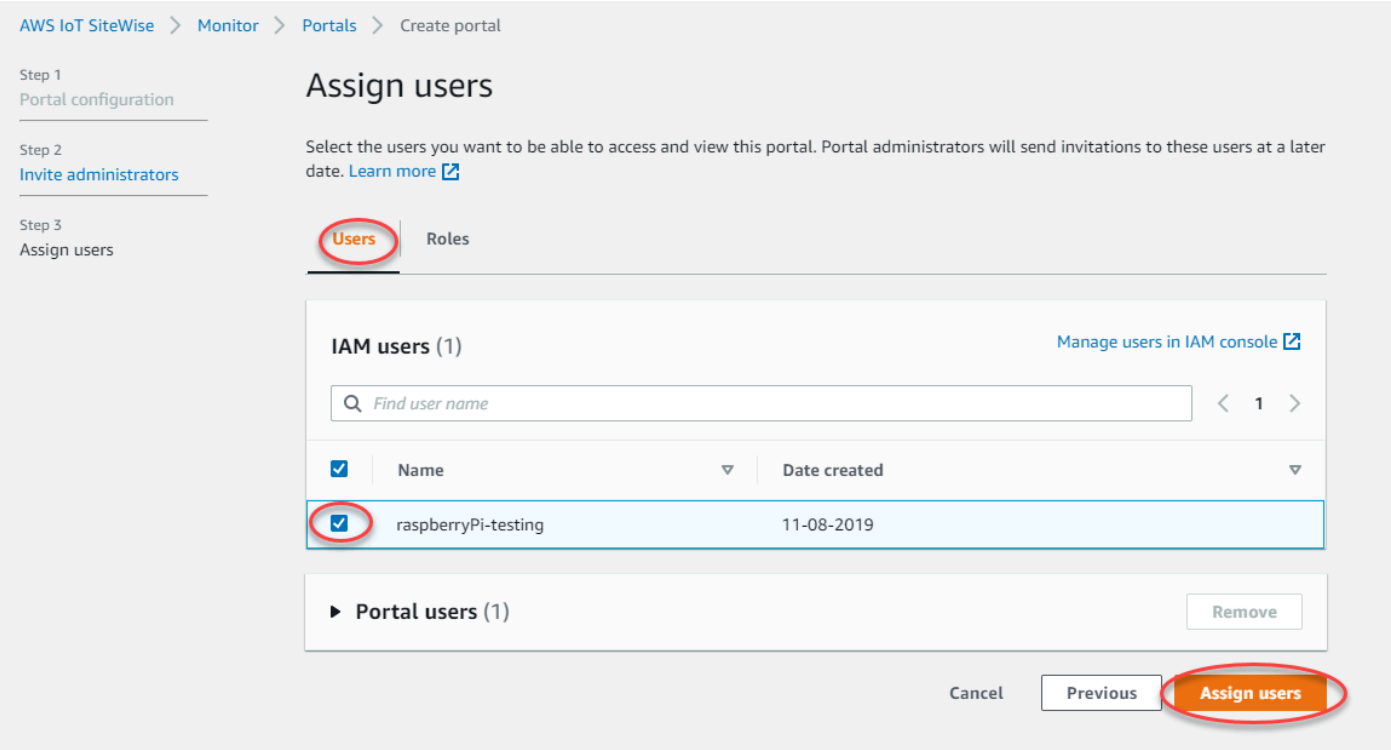
Come aggiungere utenti del portale

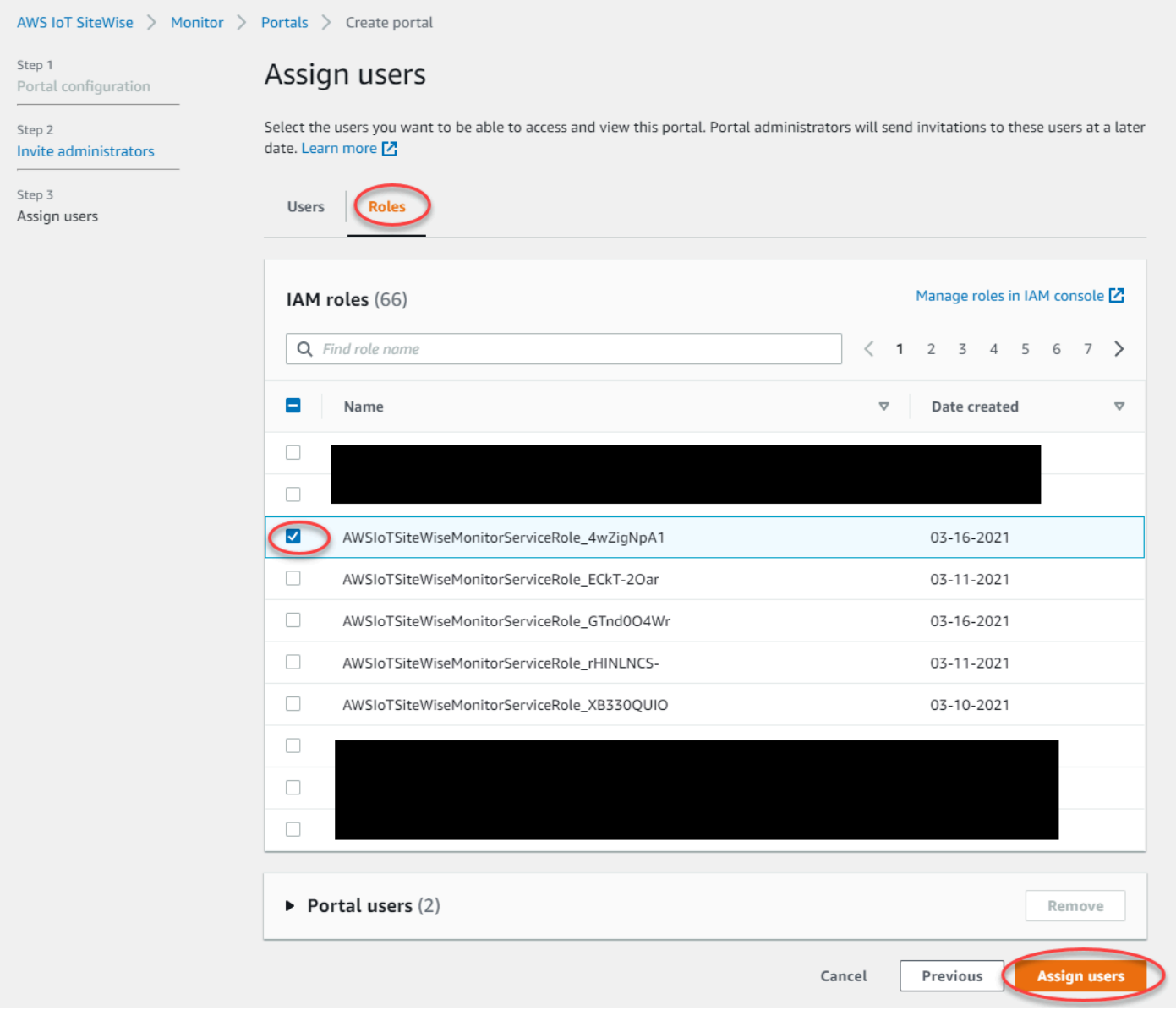
1. Esegui le seguenti opzioni:

   - Scegli utenti IAM per aggiungere un utente IAM come utente del portale.
   - Scegli i ruoli IAM per aggiungere un ruolo IAM come utente del portale.

   Se utilizzi SiteWise Monitor per la prima volta, non è necessario aggiungere l'amministratore del portale come utente del portale.
2. Seleziona le caselle di controllo relative agli utenti o ai ruoli che desideri utilizzare come utenti del portale. In questo modo gli utenti o i ruoli vengono aggiunti all'elenco degli utenti del portale.
3. Se si aggiunge e concede l'accesso a un utente indesiderato, per risolvere basta deselezionarne la casella di controllo.
4. Quando hai finito di selezionare gli utenti, scegli Assegna utenti.

> **Important**
>
> Gli utenti o i ruoli devono disporre dell'`iotsitewise:DescribePortal`autorizzazione per accedere al portale.





Complimenti! Hai creato con successo un portale, hai assegnato gli amministratori del portale e gli utenti assegnati che possono utilizzare quel portale quando invitati a farlo. Gli amministratori del tuo portale possono ora creare progetti e aggiungervi asset. A loro volta, i proprietari di progetto sono in condizione di creare i pannelli di controllo per la visualizzazione dei dati riferiti agli asset di ogni progetto.

È possibile modificare l'elenco degli utenti del portale in un secondo momento. Per ulteriori informazioni, consulta Aggiunta o rimozione di utenti del portale.

Per, all'occorrenza, apportare modifiche al portale, consulta Amministrazione dei portali SiteWise Monitor.

Per iniziare a usare il portale, vedi Guida introduttiva nella SiteWise Monitor Application Guide.

Creazione di pannelli di controllo (AWS Command Line Interface)

Quando definisci visualizzazioni (o widget) nei pannelli di controllo mediante AWS CLI, devi specificare le seguenti informazioni nel documento JSON `dashboardDefinition`. Questa definizione è un parametro delle UpdateDashboardoperazioni CreateDashboardand.

`widgets`

Un elenco delle strutture di definizione di widget ciascuna contenente le seguenti informazioni:

`type`

Il tipo di widget. AWS IoT SiteWise fornisce i seguenti tipi di widget:

- `sc-line-chart`— Un grafico a linee. Per ulteriori informazioni, vedere Grafici a linee nella Guida AWS IoT SiteWise Monitor all'applicazione.
- `sc-scatter-chart`— Un grafico a dispersione. Per ulteriori informazioni, vedere Grafici a dispersione nella Guida dell'AWS IoT SiteWise Monitorapplicazione.
- `sc-bar-chart`— Un grafico a barre. Per ulteriori informazioni, vedere Grafici a barre nella Guida AWS IoT SiteWise Monitor all'applicazione.
- `sc-status-grid`— Un widget di stato che mostra il valore più recente delle proprietà degli asset sotto forma di griglia. Per ulteriori informazioni, consultate Status widgets nella Guida all'AWS IoT SiteWise Monitorapplicazione.
- `sc-status-timeline`— Un widget di stato che mostra i valori storici delle proprietà degli asset sotto forma di sequenza temporale. Per ulteriori informazioni, consultate Status widgets nella Guida all'AWS IoT SiteWise Monitorapplicazione.
- `sc-kpi`— Una visualizzazione degli indicatori chiave di prestazione (KPI). Per ulteriori informazioni, consulta i widget KPI nella Guida all'applicazione. AWS IoT SiteWise Monitor
- `sc-table`— Un widget per tabelle. Per ulteriori informazioni, consultate Table widgets nella Guida all'AWS IoT SiteWise Monitorapplicazione.

`title`

Il titolo del widget.

`x`

La posizione orizzontale del widget, a partire dal lato sinistro della griglia. Questo valore si riferisce alla posizione del widget nella griglia del pannello di controllo.

`y`

La posizione verticale del widget, a partire dalla parte superiore della griglia. Questo valore si riferisce alla posizione del widget nella griglia del pannello di controllo.

`width`

La larghezza del widget, espressa in numero di spazi sulla griglia del pannello di controllo.

`height`

L'altezza del widget, espressa in numero di spazi sulla griglia del pannello di controllo.

`metrics`

Un elenco di strutture di parametri ciascuna delle quali definisce un flusso di dati per questo widget. Ogni struttura dell'elenco deve contenere le seguenti informazioni:

`label`

Un'etichetta da visualizzare per questo parametro.

`type`

Il tipo di origine dati per questo parametro. AWS IoT SiteWise fornisce i seguenti tipi di parametri:

- `iotsitewise`— Il pannello di controllo recupera i dati relativi alla proprietà di un asset in. AWS IoT SiteWise Se scegli questa opzione, devi definire `assetId` e `propertyId` per questo parametro.

`assetId`

(Facoltativo) L'ID di un asset in AWS IoT SiteWise.

Questo campo è obbligatorio se scegli `iotsitewise` per `type` in questo parametro.

`propertyId`

(Facoltativo) L'ID di una proprietà di asset in AWS IoT SiteWise.

Questo campo è obbligatorio se scegli `iotsitewise` per `type` in questo parametro.

`analysis`

(Facoltativo) Una struttura che definisce l'analisi, ad esempio le linee di tendenza, da visualizzare per il widget. Per ulteriori informazioni, consulta Configurazione delle linee di tendenza nella Guida all'AWS IoT SiteWise Monitorapplicazione. È possibile aggiungere una linea di tendenza per ogni proprietà nel widget. La struttura di analisi contiene le seguenti informazioni:

`trends`

(Facoltativo) Un elenco di strutture di tendenza, ciascuna delle quali definisce un'analisi delle tendenze per questo widget. Ogni struttura dell'elenco contiene le seguenti informazioni:

`type`

Il tipo di linea di tendenza. Scegliete la seguente opzione:

- `linear-regression`— Visualizza una linea di regressione lineare. SiteWise Monitor utilizza il metodo dei minimi quadrati per calcolare la regressione lineare.

`annotations`

(Facoltativo) Una struttura di annotazioni che definisce le soglie per il widget. Per ulteriori informazioni, consulta Configurazione delle soglie nella Guida all'applicazione. AWS IoT SiteWise Monitor È possibile aggiungere fino a sei annotazioni per widget. La struttura delle annotazioni contiene le seguenti informazioni:

`y`

(Facoltativo) Un elenco di strutture di annotazioni che definiscono ciascuna una soglia orizzontale per questo widget. Ogni struttura dell'elenco contiene le seguenti informazioni:

`comparisonOperator`

L'operatore di confronto per la soglia. Seleziona una delle seguenti opzioni:

- `LT`— Evidenzia le proprietà che hanno almeno un punto dati inferiore a `value`.
- `GT`— Evidenzia le proprietà che hanno almeno un punto dati maggiore di `value`.
- `LTE`— Evidenzia le proprietà che hanno almeno un punto dati inferiore o uguale a `value`.
- `GTE`— Evidenzia le proprietà che hanno almeno un punto dati maggiore o uguale a `value`.
- `EQ`— Evidenzia le proprietà che hanno almeno un punto dati uguale a `value`.

`value`

Il valore di soglia per confrontare i punti dati con`comparisonOperator`.

`color`

(Facoltativo) Il codice esadecimale a 6 cifre del colore di soglia. La visualizzazione mostra le legende delle proprietà in questo colore per le proprietà con almeno un punto dati che soddisfa la regola della soglia. Il valore predefinito è black (). `#000000`

`showValue`

(Facoltativo) Se mostrare o meno il valore della soglia nei margini del widget. L'impostazione predefinita è `true`.

`properties`

(Facoltativo) Un dizionario semplice di proprietà per il widget. I membri di questa struttura dipendono dal contesto. AWS IoT SiteWisefornisce i seguenti widget che utilizzano: `properties`

- I grafici a linee, i grafici a dispersione e i grafici a barre hanno le seguenti proprietà:

  `colorDataAcrossThresholds`

  (Facoltativo) Se modificare o meno il colore dei dati che superano le soglie in questo widget. Quando abiliti questa opzione, i dati che superano una soglia vengono visualizzati nel colore che scegli. L'impostazione predefinita è `true`.

- Le griglie di stato hanno le seguenti proprietà:

  `labels`

  (Facoltativo) Una struttura che definisce le etichette da visualizzare nella griglia di stato. La struttura delle etichette contiene le seguenti informazioni:

  `showValue`

  (Facoltativo) Se visualizzare o meno l'unità e il valore per ogni proprietà dell'asset in questo widget. L'impostazione predefinita è `true`.

Example Esempio di definizione del pannello di controllo

L'esempio seguente definisce un pannello di controllo da un payload archiviato in un file JSON.

```
aws iotsitewise create-dashboard \
```

```
  --project-id a1b2c3d4-5678-90ab-cdef-eeeeeEXAMPLE \
  --dashboard-name "Wind Farm Dashboard" \
  --dashboard-definition file://dashboard-definition.json
```

L'esempio JSON seguente per `dashboard-definition.json` definisce il pannello di controllo con i seguenti widget di visualizzazione:

- Un grafico a linee che visualizza la potenza totale del parco eolico in alto a sinistra del pannello di controllo. Questo grafico a linee include una soglia che indica quando il parco eolico produce meno energia della potenza minima prevista. Questo grafico a linee include anche una linea di tendenza alla regressione lineare.
- Un grafico a barre che visualizza la velocità del vento per quattro turbine in alto a destra del pannello di controllo.

> **Note**
>
> Questo esempio rappresenta le visualizzazioni di grafici a linee e a barre su un pannello di controllo. Questo pannello di controllo è simile al pannello di controllo del parco eolico di esempio.

```
{
  "widgets": [
    {
      "type": "sc-line-chart",
      "title": "Total Average Power",
      "x": 0,
      "y": 0,
      "height": 3,
      "width": 3,
      "metrics": [
        {
          "label": "Power",
          "type": "iotsitewise",
          "assetId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
          "propertyId": "a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
          "analysis": {
            "trends": [
              {
                "type": "linear-regression"
```

```
            }
          ]
        }
      }
    ],
    "annotations": {
      "y": [
        {
          "comparisonOperator": "LT",
          "value": 20000,
          "color": "#D13212",
          "showValue": true
        }
      ]
    }
  },
  {
    "type": "sc-bar-chart",
    "title": "Wind Speed",
    "x": 3,
    "y": 3,
    "height": 3,
    "width": 3,
    "metrics": [
      {
        "label": "Turbine 1",
        "type": "iotsitewise",
        "assetId": "a1b2c3d4-5678-90ab-cdef-2a2a2EXAMPLE",
        "propertyId": "a1b2c3d4-5678-90ab-cdef-55555EXAMPLE"
      },
      {
        "label": "Turbine 2",
        "type": "iotsitewise",
        "assetId": "a1b2c3d4-5678-90ab-cdef-2b2b2EXAMPLE",
        "propertyId": "a1b2c3d4-5678-90ab-cdef-55555EXAMPLE"
      },
      {
        "label": "Turbine 3",
        "type": "iotsitewise",
        "assetId": "a1b2c3d4-5678-90ab-cdef-2c2c2EXAMPLE",
        "propertyId": "a1b2c3d4-5678-90ab-cdef-55555EXAMPLE"
      },
      {
        "label": "Turbine 4",
```

```
          "type": "iotsitewise",
          "assetId": "a1b2c3d4-5678-90ab-cdef-2d2d2EXAMPLE",
          "propertyId": "a1b2c3d4-5678-90ab-cdef-55555EXAMPLE"
        }
      ]
    }
  ]
}
```

Attivazione degli allarmi per i tuoi portali

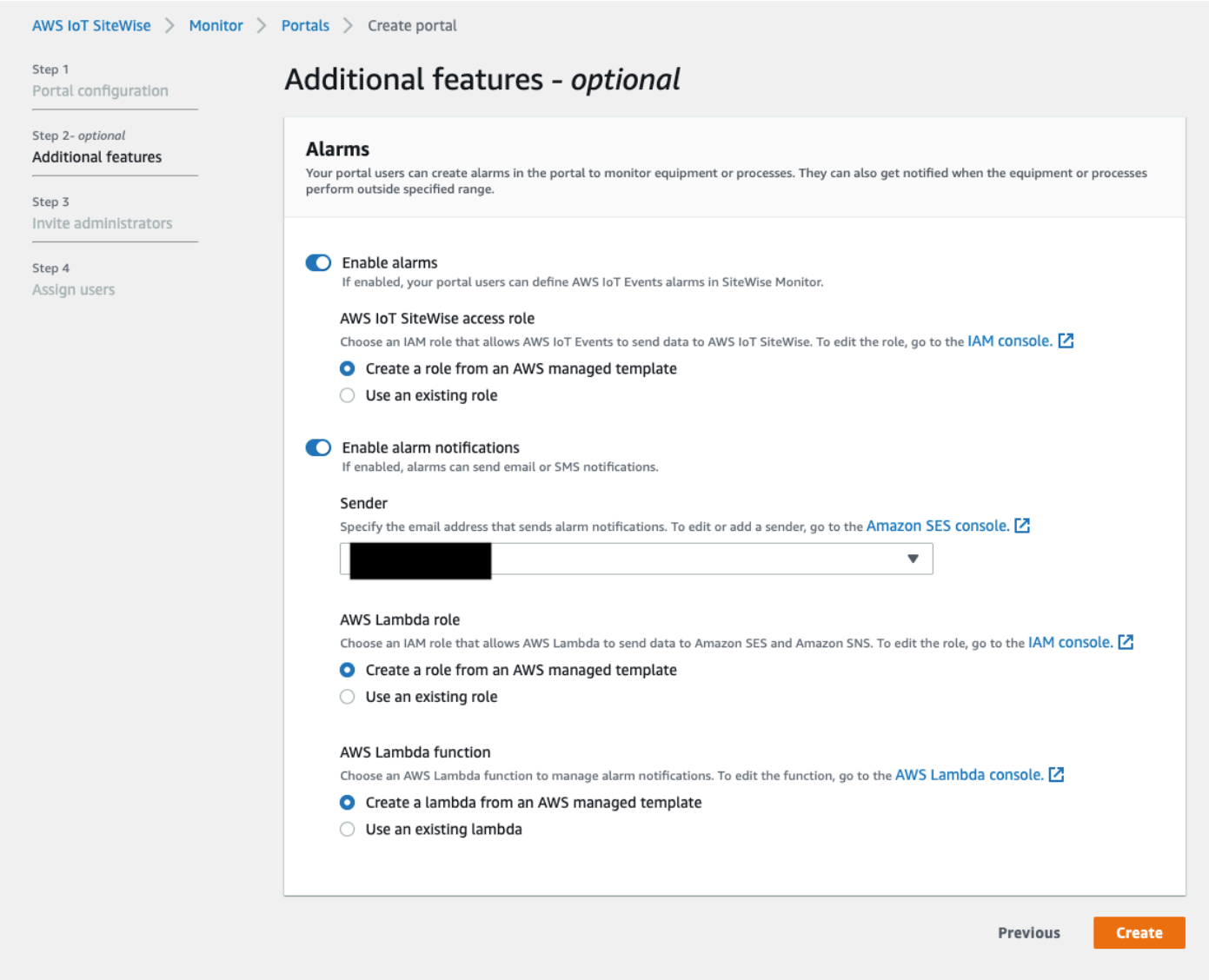
È possibile abilitare la funzionalità di allarme supportata da AWS IoT Events for your portals in modo che gli amministratori del portale possano creare, modificare ed eliminare modelli di AWS IoT Events allarme nei portali Monitor. SiteWise I proprietari dei progetti possono configurare gli allarmi. I visualizzatori del progetto possono visualizzare i dettagli degli allarmi. Questa sezione spiega come utilizzare la AWS IoT SiteWise console per abilitare la funzionalità di allarme per i portali.

Important

- Non puoi creare allarmi esterni nei tuoi portali.
- Se desideri inviare notifiche di allarme, devi scegliere IAM Identity Center per il servizio di autenticazione degli utenti.
- La funzione di notifica degli allarmi non è disponibile in Cina (Pechino) Regione AWS.

Quando configuri e crei un portale, puoi abilitare gli allarmi e le notifiche di allarme nella Fase 2 Funzionalità aggiuntive. In base al servizio di autenticazione utente, scegli una delle seguenti opzioni:

IAM Identity Center



Per abilitare gli allarmi per un portale

1. (Facoltativo) Scegli Abilita allarmi.

   - Per il ruolo di AWS IoT SiteWise accesso, utilizza un ruolo esistente o crea un ruolo con le autorizzazioni richieste. Questo ruolo richiede l'`iotevents:BatchPutMessage`autorizzazione e una relazione di fiducia che `iotevents.amazonaws.com` consenta `iot.amazonaws.com` e assuma il ruolo.

2. (Facoltativo) Scegli Abilita notifiche di allarme.

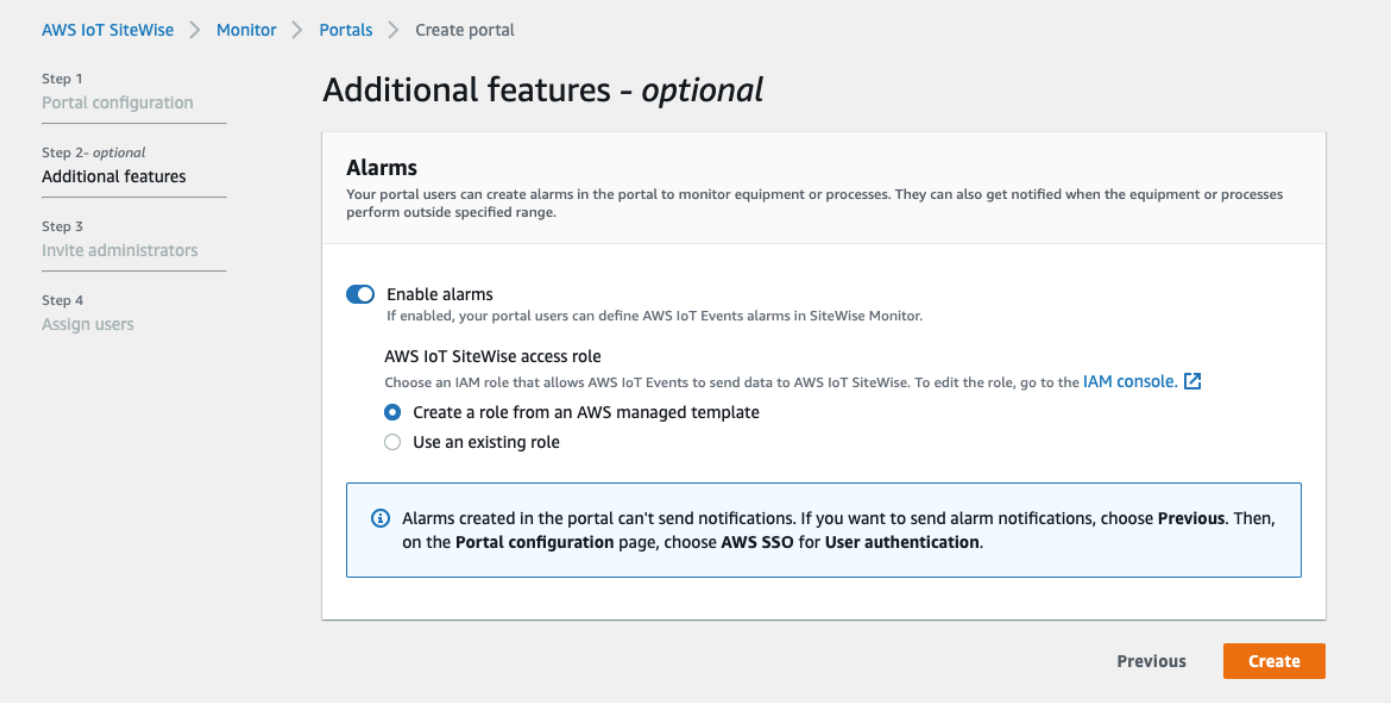
   a. Per Mittente, scegli il mittente.

> **Important**
>
> È necessario verificare l'indirizzo e-mail del mittente in Amazon SES. Per ulteriori informazioni, consulta la sezione Verifica degli indirizzi e-mail in Amazon SES, nella Amazon Simple Email Service Developer Guide.

b. Per AWS Lambda il ruolo, usa un ruolo esistente o crea un ruolo con le autorizzazioni richieste. Questo ruolo richiede le `sso-directory:DescribeUser` autorizzazioni `lambda:InvokeFunction` e una relazione di fiducia che `lambda.amazonaws.com` consenta `iotevents.amazonaws.com` e assuma il ruolo.

c. Per quanto riguarda AWS Lambda le funzioni, scegli una funzione Lambda esistente o crea una funzione che gestisca le notifiche di allarme. Per ulteriori informazioni, consulta Gestione delle notifiche di allarme nella Guida per gli AWS IoT Events sviluppatori.

IAM



Per abilitare gli allarmi per un portale

- (Facoltativo) Scegli Abilita allarmi.

- Per il ruolo di AWS IoT SiteWise accesso, utilizza un ruolo esistente o crea un ruolo con le autorizzazioni richieste. Questo ruolo richiede l'`iotevents:BatchPutMessage`autorizzazione e una relazione di fiducia che `iotevents.amazonaws.com` consenta `iot.amazonaws.com` e assuma il ruolo.

Per ulteriori informazioni sugli allarmi in SiteWise Monitor, consulta Monitoraggio con allarmi nella Guida all'AWS IoT SiteWise applicazione.

Attivazione del portale all'edge

Dopo aver abilitato il portale sull'edge, questo portale è disponibile su tutti i gateway SiteWise Edge con il pacchetto di elaborazione dati abilitato nell'account.

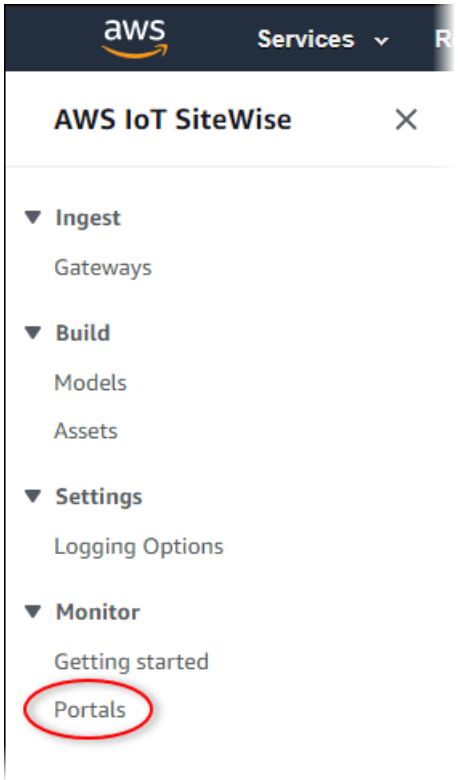
Per abilitare il portale sull'edge

1. Nella sezione Configurazione Edge, attiva Abilita questo portale all'edge.
2. Scegli Create (Crea).

Amministrazione dei portali SiteWise Monitor

Potrebbe essere necessario aggiornare i dettagli del portale, cambiare gli amministratori o aggiungere utenti ai portali. Questa sezione spiega come completare queste attività amministrative di base per i portali SiteWise Monitor.

1. Accedi alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, si deve selezionare Monitor (Monitoraggio), Portals (Portali).



3. Bisogna, infine, scegliere un portale e selezionare View details (Visualizza dettagli) (o scegliere Portal name (Nome portale)).
4. È possibile, a questo punto, svolgere le seguenti attività amministrative:

   - Modifica del nome, della descrizione, dell'e-mail di supporto, del marchio e delle autorizzazioni di un portale
   - Aggiunta o rimozione di amministratori del portale
   - Invio di e-mail di invito agli amministratori del portale
   - Aggiunta o rimozione di utenti del portale
   - Eliminazione di un portale

Per informazioni su come creare un portale, consultare Guida introduttiva con AWS IoT SiteWise Monitor.

Argomenti

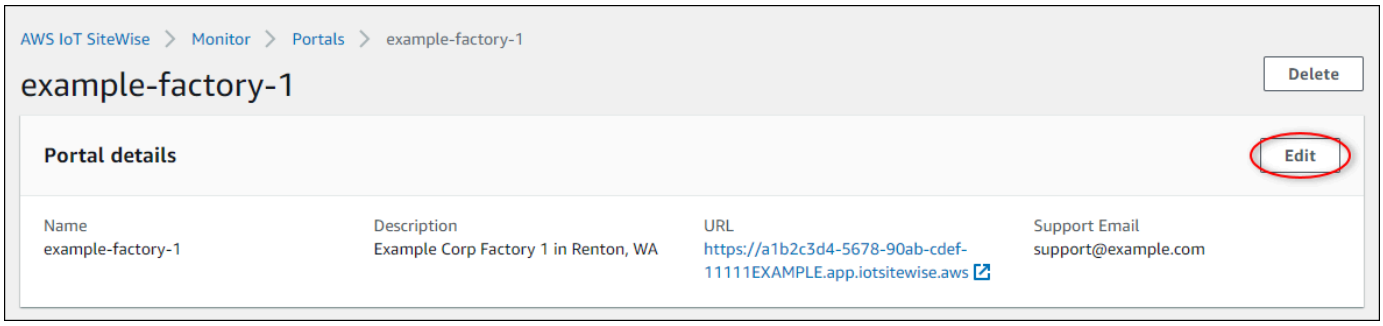
- Modifica del nome, della descrizione, dell'e-mail di supporto, del marchio e delle autorizzazioni di un portale
- Aggiunta o rimozione di amministratori del portale

- Invio di e-mail di invito agli amministratori del portale
- Aggiunta o rimozione di utenti del portale
- Eliminazione di un portale

Modifica del nome, della descrizione, dell'e-mail di supporto, del marchio e delle autorizzazioni di un portale

Puoi modificare il nome, la descrizione, l'e-mail di supporto, il marchio e le autorizzazioni di un portale.

1. Alla pagina con i dettagli del portale, nella sezione Portal details (Dettagli portale), selezionare Edit (Modifica).

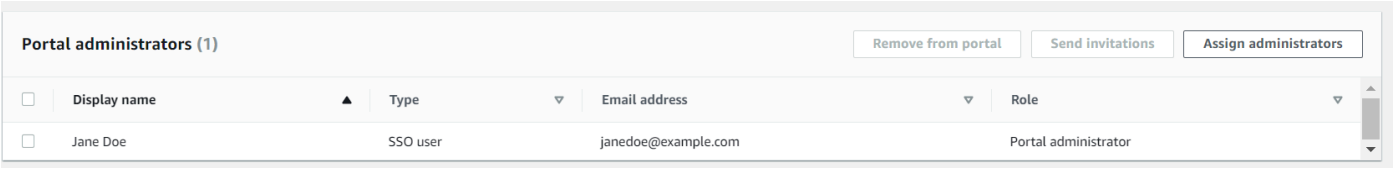


2. Aggiornare i campi Name (Nome), Description (Descrizione), Portal branding (Marchio del portale), Support contact email E-mail di contatto di supporto) o Permissions (Autorizzazioni).
3. Al termine, selezionare Save (Salva).

Aggiunta o rimozione di amministratori del portale

In pochi passaggi, è possibile aggiungere o rimuovere gli utenti nominati amministratori di un portale. In base al servizio di autenticazione utente, scegli una delle seguenti opzioni.

IAM Identity Center

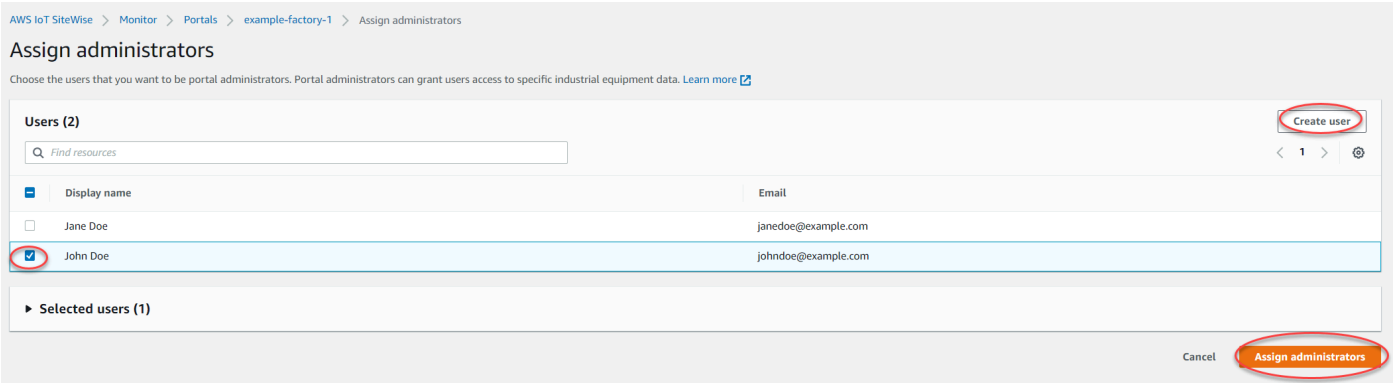


Come aggiungere amministratori del portale

1. Nella pagina dei dettagli del portale, nella sezione Amministratori del portale, scegli Assegna amministratori.
2. Nella pagina Assegna amministratori, seleziona le caselle di controllo relative agli utenti da aggiungere al portale come amministratori.

> **Note**
>
> Se utilizzi IAM Identity Center come archivio di identità e hai effettuato l'accesso al tuo account di AWS Organizations gestione, puoi scegliere Crea utente per creare un utente IAM Identity Center. IAM Identity Center invia al nuovo utente un'e-mail per consentirgli di impostare la password. È quindi possibile assegnare l'utente al portale come amministratore. Per ulteriori informazioni, consulta la sezione Gestione delle identità in IAM Identity Center.

3. Scegli Assegna amministratori.

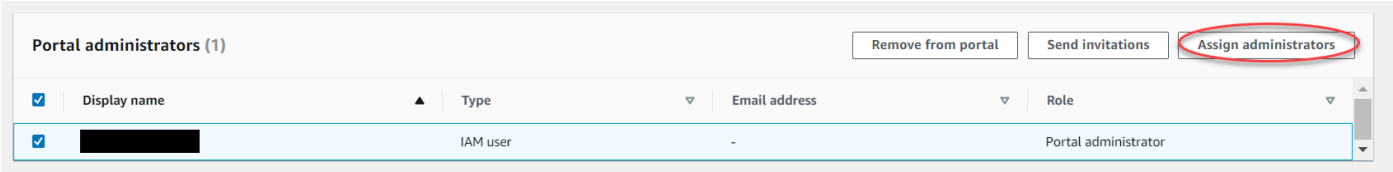


Come rimuovere amministratori del portale

- Alla pagina con i dettagli del portale, nella sezione Portal administrators (Amministratori portale), occorre spuntare la casella di controllo di ogni utente da rimuovere, per poi selezionare Remove from portal (Rimuovi dal portale).

> **Note**
>
> Ti consigliamo di selezionare almeno un amministratore del portale.

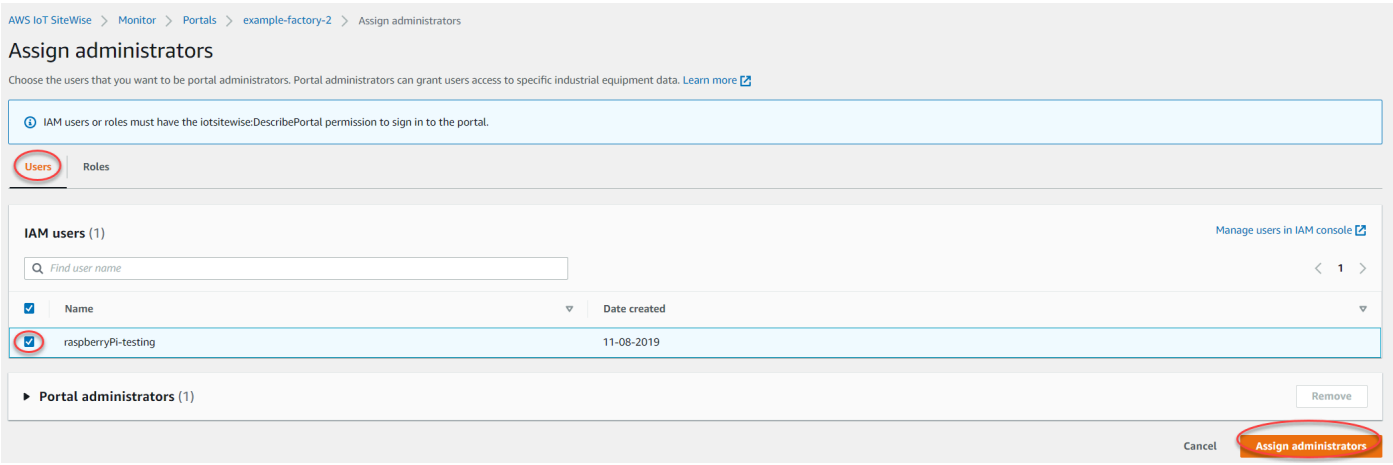
IAM

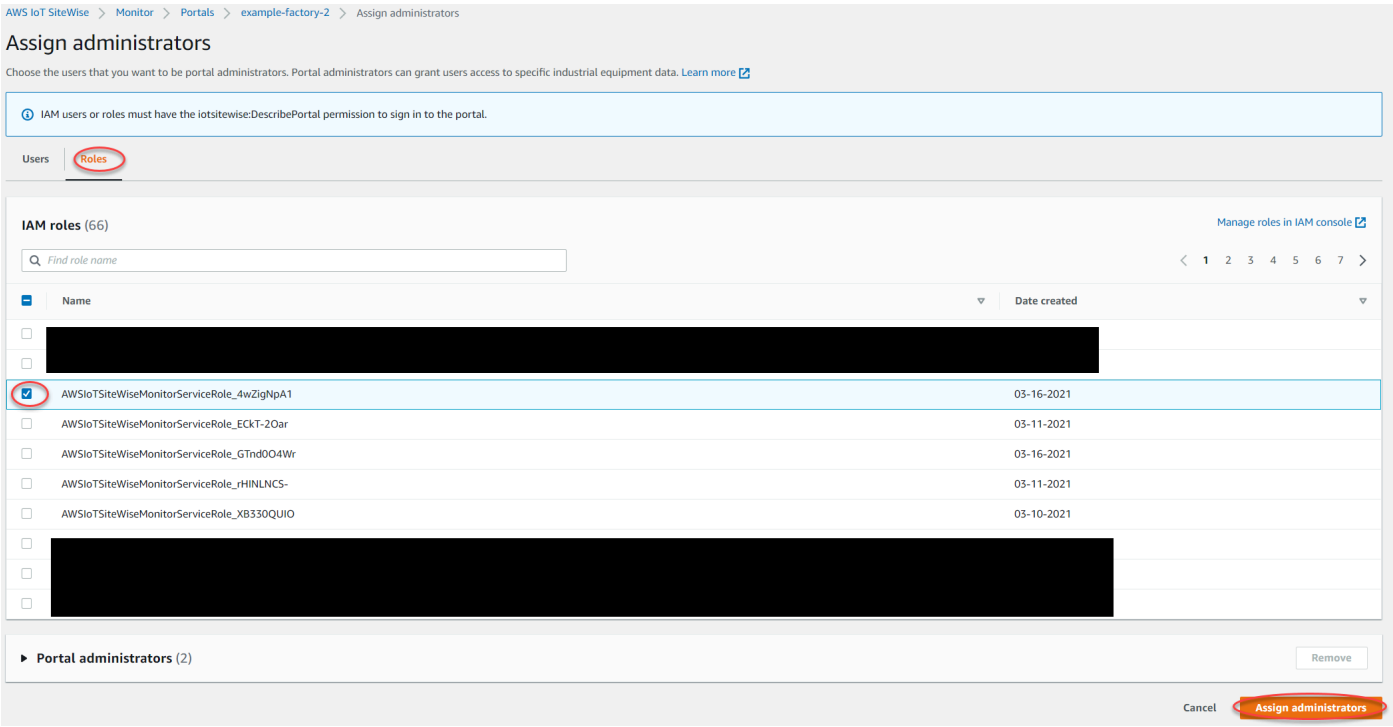


Come aggiungere amministratori del portale

1. Nella pagina dei dettagli del portale, nella sezione Amministratori del portale, scegli Assegna amministratori.
2. Nella pagina Assegna amministratori, procedi come segue:
   - Scegli utenti IAM, se desideri aggiungere un utente IAM come amministratore del portale.
   - Scegli i ruoli IAM, se desideri aggiungere un ruolo IAM come amministratore del portale.
3. Seleziona le caselle di controllo relative agli utenti o ai ruoli che desideri utilizzare come amministratori del portale. In questo modo gli utenti o i ruoli vengono aggiunti all'elenco degli amministratori del portale.
4. Scegli Assegna amministratori.

> **Important**
>
> Gli utenti o i ruoli devono disporre dell'`iotsitewise:DescribePortal`autorizzazione per accedere al portale.





Come rimuovere amministratori del portale

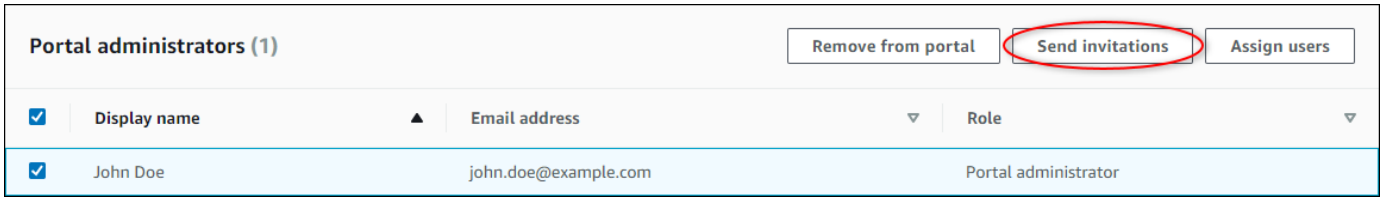
- Alla pagina con i dettagli del portale, nella sezione Portal administrators (Amministratori portale), occorre spuntare la casella di controllo di ogni utente da rimuovere, per poi selezionare Remove from portal (Rimuovi dal portale).

> **Note**
>
> Non è consigliabile lasciare un portale senza amministratori.

Invio di e-mail di invito agli amministratori del portale

È possibile inviare inviti via e-mail agli amministratori del portale.

1. Nella pagina con i dettagli del portale, selezionare le caselle di controllo per gli amministratori del portale nella sezione Portal administrators (Amministratori portale).



2. Bisogna poi selezionareSend invitations (Manda inviti). Viene visualizzato il client di posta elettronica e nel corpo del messaggio viene popolato un invito.

   È possibile personalizzare il messaggio e-mail prima di inviarlo agli amministratori del portale.

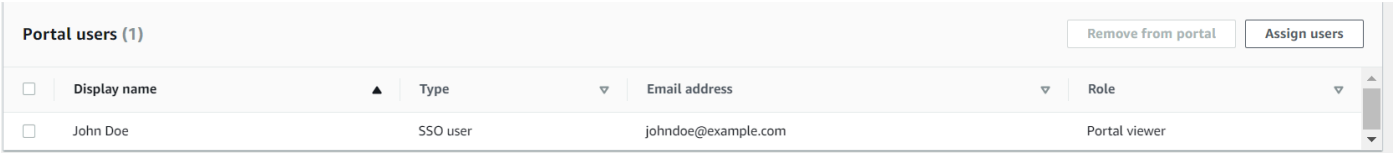
Aggiunta o rimozione di utenti del portale

Puoi scegliere quali utenti hanno accesso al portale. Gli utenti del portale vengono visualizzati nell'elenco degli utenti all'interno di un portale SiteWise Monitor. Da questo elenco, gli amministratori del portale possono aggiungere proprietari di progetti e i proprietari di progetti possono aggiungere visualizzatori di progetti.

> **Note**
>
> Gli amministratori del portale e gli utenti del portale possono contattarti tramite l'e-mail di supporto di un portale se hanno bisogno di aggiungere o rimuovere un utente.

In base al servizio di autenticazione utente, scegli una delle seguenti opzioni.

IAM Identity Center



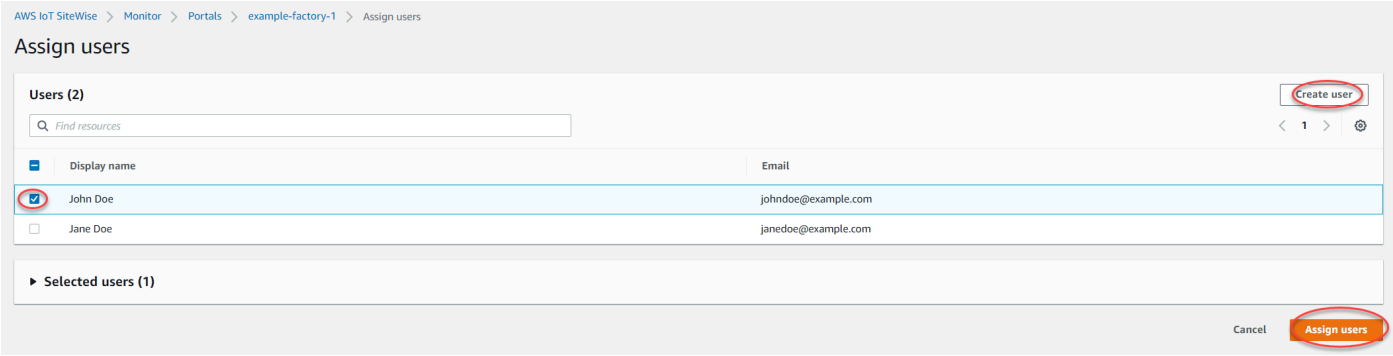
Come aggiungere utenti del portale

1. Nella pagina dei dettagli del portale, nella sezione Utenti del portale, scegli Assegna utenti.
2. Nella pagina Assegna utenti, seleziona la casella di controllo relativa agli utenti da aggiungere al portale.

   > **Note**
   >
   > Se utilizzi IAM Identity Center come archivio di identità e hai effettuato l'accesso al tuo account di AWS Organizations gestione, puoi scegliere Crea utente per creare un utente IAM Identity Center. IAM Identity Center invia al nuovo utente un'e-mail per consentirgli di impostare la password. È quindi possibile assegnare l'utente al portale

come utente. Per ulteriori informazioni, consulta la sezione Gestione delle identità in IAM Identity Center.

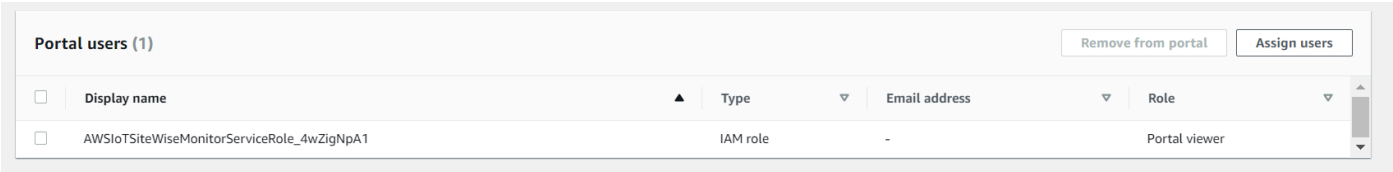
3. Scegliere Assign users (Assegna utenti).



Come rimuovere utenti del portale

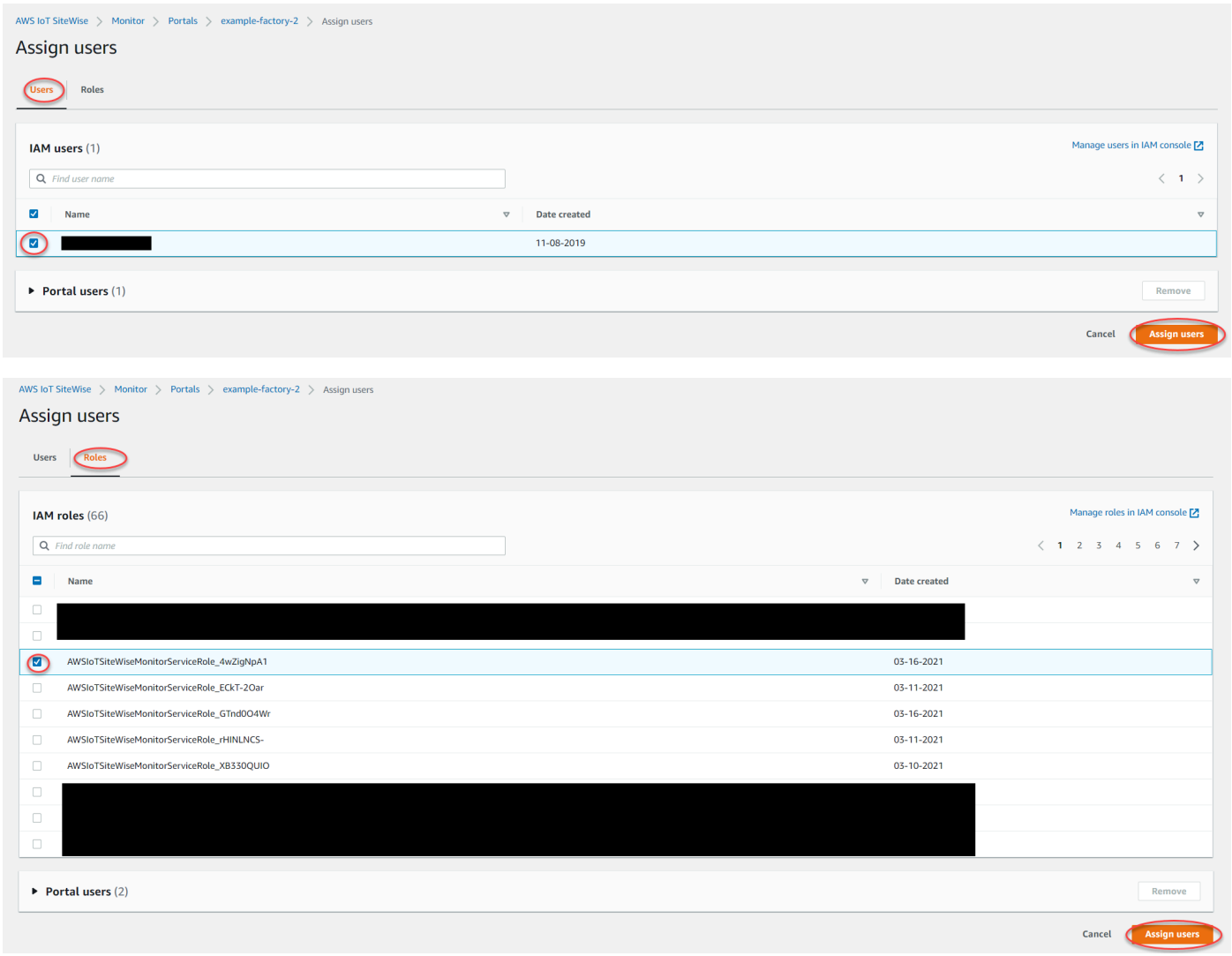
- Nella pagina dei dettagli del portale, nella sezione Utenti del portale, seleziona la casella di controllo relativa agli utenti da rimuovere dal portale, quindi scegli Rimuovi dal portale.

IAM



Come aggiungere utenti del portale

1. Nella pagina dei dettagli del portale, nella sezione Utenti del portale, scegli Assegna utenti.
2. Nella pagina Assegna utenti, procedi come segue:
   - Scegli utenti IAM per aggiungere un utente IAM come utente del portale.
   - Scegli i ruoli IAM per aggiungere un ruolo IAM come utente del portale.
3. Seleziona le caselle di controllo relative agli utenti o ai ruoli che desideri aggiungere come utenti del portale. In questo modo gli utenti o i ruoli vengono aggiunti all'elenco degli utenti del portale.
4. Scegliere Assign users (Assegna utenti).



Come rimuovere utenti del portale

- Nella pagina dei dettagli del portale, nella sezione Utenti del portale, seleziona la casella di controllo relativa agli utenti da rimuovere dal portale, quindi scegli Rimuovi dal portale.

> **Important**
>
> Gli utenti o i ruoli devono disporre dell'`iotsitewise:DescribePortal`autorizzazione per accedere al portale.

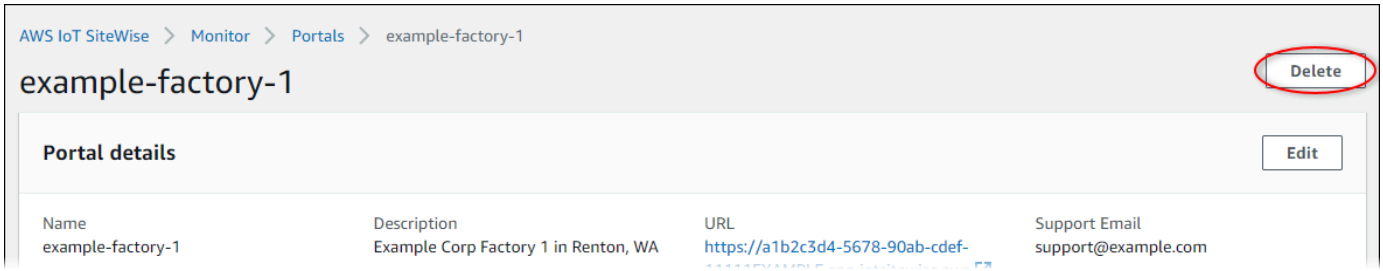
Eliminazione di un portale

Puoi eliminare un portale se lo hai creato a scopo di test o se è un duplicato di un portale già esistente.

> **Note**
>
> Prima di poter eliminare un portale, è necessario eliminare manualmente tutti i pannelli di controllo e i progetti che contiene. Per ulteriori informazioni, consulta Eliminazione di progetti ed Eliminazione di dashboard nella SiteWise Monitor Application Guide.

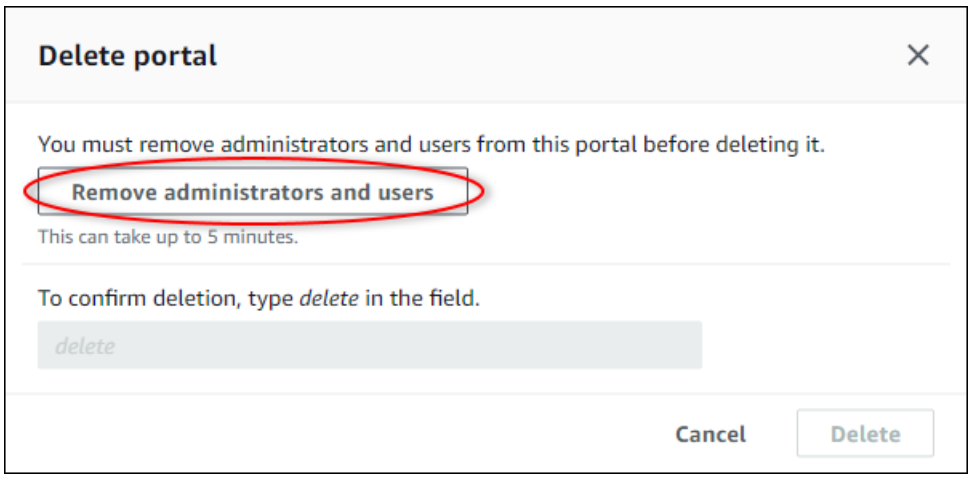
1. Nella pagina con i dettagli del portale, selezionare Delete (Elimina).

   > **Important**
   >
   > Quando si elimina un portale, si perdono tutti i progetti in esso contenuti, con i relativi pannelli di controllo. Questa operazione non può essere annullata. I dati degli asset non subiscono variazioni.

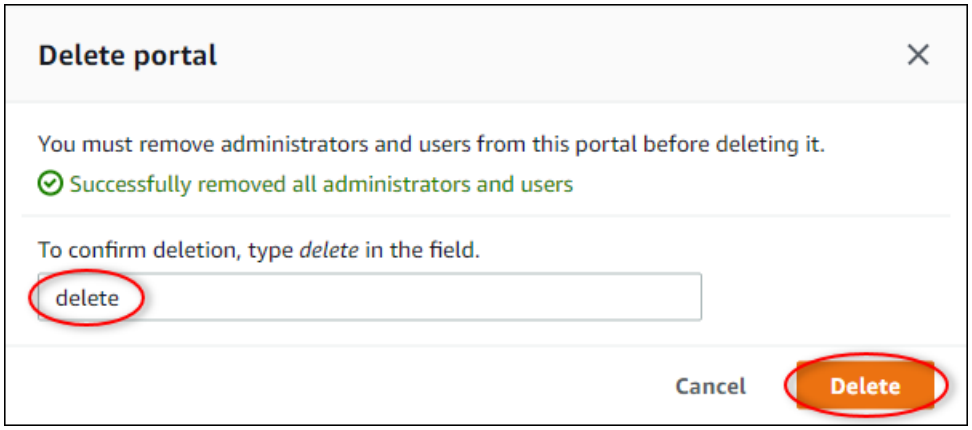


2. Nella finestra di dialogo Elimina portali, scegli Rimuovi amministratori e utenti.

   Per poter eliminare definitivamente un portale, bisogna innanzitutto rimuoverne tutti gli amministratori e utenti. Se il portale non dispone di amministratori o utenti, il pulsante non viene visualizzato ed è possibile passare direttamente alla fase successiva.



3. Se si è certi di voler eliminare l'intero portale, immettere **`delete`** nel campo per confermare l'eliminazione.



4. Scegli Delete (Elimina).

Monitoraggio dei dati con l'applicazione dashboard IoT

L'applicazione dashboard IoT è un'applicazione dashboard open source in cui è possibile visualizzare e interagire con i dati operativi. Puoi utilizzare l'applicazione dashboard IoT AWS Cloud Development Kit (AWS CDK) per implementare.

Di seguito sono riportati alcuni esempi delle funzionalità di visualizzazione dei dati personalizzabili nell'applicazione dashboard IoT:

- Support per più proprietà in un unico grafico a linee.
- Ricerca avanzata di risorse e proprietà.

I clienti del settore manifatturiero, della logistica, dell'energia e di altri settori possono utilizzare l'applicazione dashboard IoT per affrontare sfide specifiche come il monitoraggio delle prestazioni delle apparecchiature, l'ottimizzazione dell'efficienza operativa e le decisioni basate sui dati. Per ulteriori informazioni, consulta il GitHub repository per l'applicazione dashboard IoT.

Interroga dati da AWS IoT SiteWise

Puoi utilizzare le operazioni AWS IoT SiteWise API per interrogare i valori correnti, i valori storici e gli aggregati delle proprietà degli asset su intervalli di tempo specifici.

Utilizza queste funzionalità per ottenere informazioni dettagliate sui tuoi dati. Ad esempio, scopri tutte le tue risorse con un determinato valore di proprietà o crea una rappresentazione personalizzata dei tuoi dati. Puoi anche utilizzare le operazioni API per sviluppare soluzioni software che si integrano con i dati industriali archiviati nelle tue AWS IoT SiteWise risorse. È inoltre possibile esplorare i dati degli asset in tempo reale in AWS IoT SiteWise Monitor. Per informazioni su come configurare SiteWise Monitor, consultaMonitoraggio dei dati con AWS IoT SiteWise Monitor.

Le operazioni descritte in questa sezione restituiscono oggetti di valore delle proprietà che contengono strutture di timestamp, quality, value (TQV):

- `timestamp` contiene l'orario UTC (epoca (Unix epoch)) corrente in secondi, con offset in nanosecondi.
- `quality` contiene una delle seguenti stringhe che indicano la qualità del punto dati:
  - `GOOD`— I dati non sono interessati da alcun problema.
  - `BAD`— I dati sono interessati da un problema come il guasto del sensore.
  - `UNCERTAIN`— I dati sono influenzati da un problema come l'imprecisione del sensore.
- `value` contiene uno dei seguenti campi, a seconda del tipo di proprietà:
  - `booleanValue`
  - `doubleValue`
  - `integerValue`
  - `stringValue`

Argomenti

Interrogazione dei valori delle proprietà dell'asset corrente

Questo tutorial mostra due modi per ottenere il valore corrente di una proprietà di un asset. È possibile utilizzare la AWS IoT SiteWise console o utilizzare l'API in AWS Command Line Interface (AWS CLI).

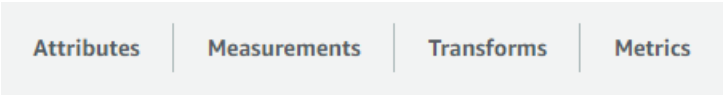
Argomenti

Interroga il valore corrente di una proprietà dell'asset (console)

È possibile utilizzare la AWS IoT SiteWise console per visualizzare il valore corrente di una proprietà di un asset.

Per ottenere il valore corrente di una proprietà di asset (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Asset.
3. Scegli l'asset con la proprietà su cui eseguire la query.
4. Scegliete l'icona a forma di freccia per espandere una gerarchia di risorse e trovare la risorsa desiderata.
5. Scegli la scheda per il tipo di proprietà. Ad esempio, scegli Misurazioni per visualizzare il valore corrente di una proprietà di misurazione.

6. Trova la proprietà da visualizzare. Il valore corrente viene visualizzato nella colonna Valore più recente.

Interroga il valore corrente di una proprietà dell'asset ()AWS CLI

È possibile utilizzare AWS Command Line Interface (AWS CLI) per interrogare il valore corrente di una proprietà dell'asset.

Utilizzate l'GetAssetPropertyValueoperazione per interrogare il valore corrente di una proprietà dell'asset.

Per identificare la proprietà di un asset, specificate una delle seguenti opzioni:

- La proprietà `assetId` e `propertyId` della risorsa a cui vengono inviati i dati.
- Il`propertyAlias`, che è un alias del flusso di dati (ad esempio,`/company/windfarm/3/turbine/7/temperature`). Per utilizzare questa opzione, è necessario prima impostare l'alias della proprietà dell'asset. Per impostare gli alias delle proprietà, vedere. Mappatura dei flussi di dati industriali alle proprietà degli asset

Per ottenere il valore corrente di una proprietà di un asset ()AWS CLI

- Esegui il comando seguente per ottenere il valore corrente della proprietà di asset. Sostituisci *`asset-id`* con l'ID dell'asset e *`property-id`* con l'ID della proprietà.

```
aws iotsitewise get-asset-property-value \
  --asset-id asset-id \
  --property-id property-id
```

L'operazione restituisce una risposta contenente il TQV attuale della proprietà nel formato seguente.

```
{
  "propertyValue": {
    "value": {
      "booleanValue": Boolean,
      "doubleValue": Number,
      "integerValue": Number,
      "stringValue": "String"
    },
    "timestamp": {
      "timeInSeconds": Number,
      "offsetInNanos": Number
    },
    "quality": "String"
  }
}
```

Esecuzione di query sui valori cronologici delle proprietà degli asset

È possibile utilizzare l'GetAssetPropertyValueHistoryoperazione AWS IoT SiteWise API per interrogare i valori storici di una proprietà dell'asset.

Per identificare una proprietà di un asset, specificate una delle seguenti opzioni:

- La proprietà `assetId` e `propertyId` della risorsa a cui vengono inviati i dati.
- Il`propertyAlias`, che è un alias del flusso di dati (ad esempio,`/company/windfarm/3/turbine/7/temperature`). Per utilizzare questa opzione, è necessario prima impostare l'alias della proprietà dell'asset. Per impostare gli alias delle proprietà, vedere. Mappatura dei flussi di dati industriali alle proprietà degli asset

Passa i seguenti parametri per affinare i risultati:

- `startDate`— L'inizio esclusivo dell'intervallo da cui interrogare i dati storici, espresso in secondi nell'epoca Unix.
- `endDate`— La fine inclusiva dell'intervallo da cui interrogare i dati storici, espressa in secondi nell'epoca Unix.
- `maxResults`— Il numero massimo di risultati da restituire in una richiesta. I valori predefiniti sono i risultati. `20`
- `nextToken`— Un token di impaginazione restituito da una precedente chiamata di questa operazione.
- `timeOrdering`— L'ordine da applicare ai valori restituiti: `ASCENDING` o. `DESCENDING`
- `qualities`— La qualità per filtrare i risultati in base a: `GOODBAD`, o`UNCERTAIN`.

Argomenti

- Interroga la cronologia dei valori per una proprietà dell'asset (AWS CLI)

Interroga la cronologia dei valori per una proprietà dell'asset (AWS CLI)

Per interrogare la cronologia dei valori di una proprietà dell'asset (AWS CLI)

1. Esegui il comando seguente per ottenere la cronologia dei valori per la proprietà di asset. Questo comando esegue una query per la cronologia della proprietà su un intervallo di 10 minuti.

Sostituisci *asset-id* con l'ID dell'asset e *property-id* con l'ID della proprietà. Sostituisci i parametri di data con l'intervallo per la query.

```
aws iotsitewise get-asset-property-value-history \
  --asset-id asset-id \
  --property-id property-id \
  --start-date 1575216000 \
  --end-date 1575216600
```

L'operazione restituisce una risposta che contiene i TQV storici della proprietà nel seguente formato:

```
{
  "assetPropertyValueHistory": [
    {
      "value": {
        "booleanValue": Boolean,
        "doubleValue": Number,
        "integerValue": Number,
        "stringValue": "String"
      },
      "timestamp": {
        "timeInSeconds": Number,
        "offsetInNanos": Number
      },
      "quality": "String"
    }
  ],
  "nextToken": "String"
}
```

2. Se esistono più valori, è possibile passare il token di impaginazione dal `nextToken` campo a una successiva chiamata all'operazione. GetAssetPropertyValueHistory

Esecuzione di query sugli aggregati delle proprietà di asset

AWS IoT SiteWise calcola automaticamente i valori aggregati delle proprietà degli asset, che sono un insieme di metriche di base calcolate su più intervalli di tempo. AWS IoT SiteWise calcola i seguenti aggregati ogni minuto, ora e giorno per le proprietà degli asset:

- media: la media (media) dei valori di una proprietà in un intervallo di tempo.
- count: il numero di punti dati per una proprietà in un intervallo di tempo.
- maximum — Il massimo dei valori di una proprietà in un intervallo di tempo.
- minimo — Il minimo dei valori di una proprietà in un intervallo di tempo.
- deviazione standard: la deviazione standard dei valori di una proprietà in un intervallo di tempo.
- sum — La somma dei valori di una proprietà in un intervallo di tempo.

Per le proprietà non numeriche, come stringhe e valori booleani, calcola solo l'aggregato di conteggio. AWS IoT SiteWise

Puoi anche calcolare parametri personalizzati per i dati di asset. Con le proprietà metriche, definisci aggregazioni specifiche per la tua operazione. Le proprietà metriche offrono funzioni di aggregazione e intervalli di tempo aggiuntivi che non sono precalcolati per l'API. AWS IoT SiteWise Per ulteriori informazioni, consulta Aggregazione di dati da proprietà e altre risorse (metriche).

Argomenti

- Aggregati per una proprietà di asset (API)
- Aggregati per una proprietà di asset ()AWS CLI

Aggregati per una proprietà di asset (API)

Puoi utilizzare l' AWS IoT SiteWise API per ottenere aggregati per una proprietà di un asset.

Utilizzate l'GetAssetPropertyAggregatesoperazione per interrogare gli aggregati di una proprietà di un asset.

Per identificare la proprietà di un asset, specificate una delle seguenti opzioni:

- La proprietà `assetId` e `propertyId` della risorsa a cui vengono inviati i dati.
- Il`propertyAlias`, che è un alias del flusso di dati (ad esempio,`/company/windfarm/3/turbine/7/temperature`). Per utilizzare questa opzione, è necessario prima impostare l'alias della proprietà dell'asset. Per impostare gli alias delle proprietà, vedere. Mappatura dei flussi di dati industriali alle proprietà degli asset

È inoltre necessario passare i seguenti parametri obbligatori:

- `aggregateTypes`— L'elenco degli aggregati da recuperare. Puoi specificare uno qualsiasi di `AVERAGE`, `COUNT`, `MAXIMUM`, `MINIMUM`, `STANDARD_DEVIATION` e `SUM`.
- `resolution`— L'intervallo di tempo per il quale recuperare la metrica: `1m` (1 minuto), (1 ora) o `1h` `1d` (1 giorno).
- `startDate`— L'inizio esclusivo dell'intervallo da cui interrogare i dati storici, espresso in secondi nell'epoca Unix.
- `endDate`— La fine inclusiva dell'intervallo da cui interrogare i dati storici, espressa in secondi nell'epoca Unix.

È anche possibile passare uno dei seguenti parametri per perfezionare i risultati:

- `maxResults`— Il numero massimo di risultati da restituire in una richiesta. I valori predefiniti sono i risultati. `20`
- `nextToken`— Un token di impaginazione restituito da una precedente chiamata di questa operazione.
- `timeOrdering`— L'ordine da applicare ai valori restituiti: `ASCENDING` o. `DESCENDING`
- `qualities`— La qualità per filtrare i risultati in base a: `GOODBAD`, o`UNCERTAIN`.

> **Note**
>
> L'GetAssetPropertyAggregatesoperazione restituisce un TQV con un formato diverso rispetto alle altre operazioni descritte in questa sezione. La struttura di `value` annovera un campo per ogni `aggregateTypes` incluso nella richiesta. `timestamp` contiene l'orario in cui si è verificata l'aggregazione, in secondi nel formato epoca (Unix epoch).

Aggregati per una proprietà di asset ()AWS CLI

Per interrogare gli aggregati per una proprietà di un asset ()AWS CLI

1. Esegui il comando seguente per ottenere aggregati per la proprietà di asset. Questo comando esegue la query per la media e la somma con una risoluzione di 1 ora per uno specifico intervallo di 1 ora. Sostituisci *`asset-id`* con l'ID dell'asset e *`property-id`* con l'ID della proprietà. Sostituisci i parametri con gli aggregati e l'intervallo per la query.

```
aws iotsitewise get-asset-property-aggregates \
  --asset-id asset-id \
  --property-id property-id \
  --start-date 1575216000 \
  --end-date 1575219600 \
  --aggregate-types AVERAGE SUM \
  --resolution 1h
```

L'operazione restituisce una risposta contenente i TQV storici della proprietà nel formato seguente. La risposta include solo gli aggregati richiesti.

```
{
  "aggregatedValues": [
    {
      "timestamp": Number,
      "quality": "String",
      "value": {
        "average": Number,
        "count": Number,
        "maximum": Number,
        "minimum": Number,
        "standardDeviation": Number,
        "sum": Number
      }
    }
  ],
  "nextToken": "String"
}
```

2. Se esistono più valori, è possibile passare il token di impaginazione dal `nextToken` campo a una successiva chiamata all'GetAssetPropertyAggregatesoperazione.

AWS IoT SiteWise linguaggio di interrogazione

Con l'operazione dell'ExecuteQueryAPI di recupero AWS IoT SiteWise dei dati, è possibile recuperare informazioni sulle definizioni strutturali dichiarative e sui dati delle serie temporali ad esse associati, da quanto segue:

- modelli

- risorse
- misurazioni
- metriche
- trasforma
- aggregati

Questo può essere fatto con istruzioni di query simili a SQL, in un'unica richiesta API.

> **Note**
>
> Questa funzionalità è disponibile in tutte le regioni in cui entrambe AWS IoT SiteWise AWS IoT TwinMaker sono disponibili, ad eccezione di AWS GovCloud (Stati Uniti occidentali).

Argomenti

Prerequisiti

AWS IoT SiteWise richiede le autorizzazioni per l'integrazione in AWS IoT TwinMaker modo da poter organizzare e modellare i dati industriali.

Prima di poter recuperare informazioni su modelli, risorse, misurazioni, metriche, trasformazioni e aggregati, assicuratevi che siano soddisfatti i seguenti prerequisiti:

- Ruoli collegati ai servizi per entrambi e configurazione in. AWS IoT SiteWise AWS IoT TwinMaker Account AWS Per ulteriori informazioni sui ruoli collegati al servizio, consulta Utilizzo dei ruoli collegati al servizio nella Guida per l'utente IAM.
- Un' AWS IoT SiteWise integrazione abilitata per il tuo ruolo IAM. Per ulteriori informazioni, consulta Integrazione di AWS IoT SiteWise e AWS IoT TwinMaker.
- Un' AWS IoT TwinMaker area di lavoro con ID `IoTSiteWiseDefaultWorkspace` nel tuo account nella regione. Per ulteriori informazioni, consulta Using the IoTSiteWiseDefaultWorkspace in the AWS IoT TwinMaker User Guide.

- Sono abilitate le modalità di prezzo in bundle standard o a più livelli. AWS IoT TwinMaker Per ulteriori informazioni, consulta le modalità di AWS IoT TwinMaker prezzo di Switch nella Guida per l'AWS IoT TwinMaker utente.

Riferimento al linguaggio di interrogazione

AWS IoT SiteWise supporta un linguaggio di interrogazione avanzato per lavorare con i dati. I tipi di dati, gli operatori, le funzioni e i costrutti disponibili sono descritti nei seguenti argomenti.

Vedere Query di esempio per scrivere interrogazioni con il linguaggio di AWS IoT SiteWise interrogazione.

Argomenti

Comprendere le opinioni

Questa sezione fornisce informazioni per aiutarti a comprendere le visualizzazioni in AWS IoT SiteWise, ad esempio i metadati di processo e i dati di telemetria.

Le tabelle seguenti forniscono i nomi e le descrizioni delle viste.

Modello di dati

Nome della vista	Descrizione della vista
asset	Contiene informazioni sulla derivazione dell'asset e del modello.
asset_property	Contiene informazioni sulla struttura della proprietà dell'asset.
raw_time_series	Contiene i dati storici delle serie temporali.

Nome della vista	Descrizione della vista
latest_value_time_series	Contiene il valore più recente della serie temporale.
precomputed_aggregates	Contiene i valori delle proprietà aggregati degli asset calcolati automaticamente. Sono un insieme di metriche di base calcolate su più intervalli di tempo.

Le viste seguenti elencano i nomi delle colonne per le query insieme ai dati di esempio.

Visualizza: risorsa

asset_id	nome_risorsa	descrizione_risorsa	asset_model_id
88898498-0b8b-42b5-bf57-16180bc3d3a0	WindTurbine UN	WindTurbine Risorsa A	17847250-5bf0-4f74-b775-cc03f05e7cb8
17847250-5bf0-4f74-b775-cc03f05e7cb8	Modello di investimento per turbine eoliche	Rappresenta una turbina in un parco eolico.	

Visualizza: asset_property

property_id	id_risorsa	nome_proprietà	tipo_dati_proprietà	property_alias	asset_composite_model_id
b29be434-b000-4d74-b809-75287d83bcd6	88898498-0b8b-42b5-bf57-16180bc3d3a0	temperatura del motore	Doppio	`Rochester 2/44///Line-5/Bus-2/Machine-5/Temperature`	
3b458f00-24e7-458a	88898498-0b8b-42b5	direzione del vento	Doppio	`/company/windfarm/`	2f458n00-56e7-458h

property_id	id_risorsa	nome_proprietà	tipo_dati_proprietà	property_alias	asset_composite_model_id
-b4e8-c6026eff654a	-bf57-16180bc3d3a0			3/turbine/7/winddirection	-b4e8-c6026eff985g

Visualizza: raw_time_series

asset_id	id_proprietà	property_alias	timestamp dell'evento	qualità	valore_booleano	valore_int_	valore_doppio	valore_stringa
888984980b8b-42b5-bf57-16180bc3d3a	b29be434-b000-4d74-b809-75287d83bcd	Rochest 2/44/// Line-5/Bus-2/Machine-5/Temperature	1575219600	BUONO			115.0	
888984980b8b-42b5-bf57-16180bc3d3a	3b458f00-24e7-458a-b4e8-c6026eff654a	/company/windfarm/3/turbine/7/winddirection	1575219337	BUONO			348,75	

> **Note**
>
> È necessario includere una clausola di filtro `event_timestamp` nella colonna per interrogare la vista. `raw_time_series` Si tratta di un filtro obbligatorio e senza di esso l'interrogazione avrà esito negativo.
>
> Example query
>
> ```
> SELECT event_timestamp, double_value FROM raw_time_series WHERE event_timestamp
>  > 1234567890
> ```

Visualizza: latest_value_time_series

asset_id	id_proprietà	property_alias	timestamp dell'evento	qualità	valore_booleano	valore_int_	valore_doppio	valore_stringa
88898498-0b8b-42b5-bf57-16180bc3d3a	3b458f00-24e7-458a-b4e8-c6026eff654a	/company/windfarm/3/turbine/7/winddirection	1575219600	BUONO			355,39	

Visualizza: precomputed_aggregates

asset_id	id_proprietà	property alias	timestamp dell'evento	risoluzione	somma_ore	valore_conteggio	valore_medio	valore_massimo	valore_minimo	stdev_value
888984-0b8b-42-bf57-16	b29be4-b000-4c-b809-75	Roches 2/44// Line-5/	157521-0	15 min	1105,48	15	73,4	80,6	68	3,64

asset_ic	id_propr età	property alias	timestar dell'eve to	risoluzic ne	somma_ ore	valore_c nteggio	valore_r dio	valore_r ssimo	valore_r nimo	stdev_val ue
80bc3d:	87d83b	Bus-2/ Machin -5/ Temper ature								

Tipi di dati supportati

AWS IoT SiteWise il linguaggio di interrogazione supporta i seguenti tipi di dati.

Visualizza: risorsa

Tipo di dati	Descrizione
`STRING`	Una stringa di lunghezza massima di 1024 byte.
`INTEGER`	Un numero intero con segno a 32 bit con un intervallo da. `-2,147,483,648 to 2,147,483,647`
`DOUBLE`	Un numero a virgola mobile con intervallo – `10^100 to 10^100` e `IEEE 754` precisione doppia.
`BOOLEAN`	`true` o `false`.

> **Note**
>
> I dati a doppia precisione non sono esatti. Alcuni valori non vengono convertiti esattamente e non rappresenteranno tutti i numeri reali a causa della precisione limitata. I dati a virgola mobile nella query potrebbero non corrispondere allo stesso valore rappresentato

internamente. Il valore viene arrotondato se la precisione di un numero di input è troppo elevata.

Recupera i dati con un'istruzione SELECT

L'`SELECT`istruzione viene utilizzata per recuperare dati da una o più viste. AWS IoT SiteWise supporta un implicito `JOIN` delle visualizzazioni. È possibile elencare le viste da unire (nella `FROM` clausola dell'`SELECT`istruzione), utilizzando le virgole per separarle.

Example

Usa la seguente dichiarazione: `SELECT`

```
SELECT select_expr [, ...]
[ FROM from_item [, ...] ]
[ WHERE [LIKE condition ESCAPE condition] ]
```

Nell'esempio precedente, la `LIKE` clausola specifica le condizioni di ricerca e filtraggio utilizzando wild card. AWS IoT SiteWise supporta `percentage (%)` come carattere wild card.

Example da usare **%** in una condizione:

```
Prefix search: String%
Infix search: %String%
Suffix search: %String
```

Example per cercare una risorsa:

```
SELECT asset_name, asset_description FROM asset WHERE asset_name LIKE 'Wind%'
```

Example per cercare una risorsa utilizzando una condizione ESCAPE:

```
SELECT asset_name, asset_description FROM asset WHERE asset_name LIKE 'room\%' ESCAPE
 '\'
```

Operatori logici

AWS IoT SiteWise supporta i seguenti operatori logici.

Operatori logici

Operatore	Descrizione	Esempio
AND	TRUEse entrambi i valori sono veri	a AND b

Se a o b èFALSE, l'espressione precedente restituisce false. Affinché un AND operatore restituisca vero, è necessario che sia a che b siano veri.

Example

```
SELECT a.asset_name
FROM asset as a, latest_value_time_series as t
WHERE t.int_value > 30 AND t.event_timestamp > 1234567890
```

Operatori di confronto

AWS IoT SiteWise supporta i seguenti operatori di confronto.

Operatori logici

Operatore	Descrizione
<	Minore di
>	Maggiore di
<=	Minore o uguale a
>=	Maggiore o uguale a
=	Equals
!=	Non uguale

Query di esempio

Filtraggio dei metadati

L'esempio seguente riguarda il filtraggio dei metadati con un'`SELECT`istruzione con il linguaggio di interrogazione: AWS IoT SiteWise

```
SELECT a.asset_name, p.property_name
FROM asset a, asset_property p
WHERE a.asset_id = p.asset_id AND a.asset_name LIKE '%windmill%'
```

Filtraggio dei valori

Di seguito è riportato un esempio di filtraggio dei valori mediante un'`SELECT`istruzione con il linguaggio di AWS IoT SiteWise interrogazione:

```
SELECT a.asset_name FROM asset a, raw_time_series r
WHERE a.asset_id = r.asset_id AND r.int_value > 30  AND r.event_timestamp > 1234567890
 AND r.event_timestamp < 1234567891
```

Interazione con altri servizi AWS

AWS IoT SiteWise può pubblicare i dati degli asset sul broker di messaggi di pubblicazione e sottoscrizione AWS IoT MQTT, in modo da poter interagire con i dati degli asset provenienti da altri servizi. AWS AWS IoT SiteWise assegna a ciascuna proprietà degli asset un argomento MQTT univoco che potete utilizzare per indirizzare i dati degli asset ad altri AWS servizi utilizzando le regole di base. AWS IoT Ad esempio, puoi configurare le regole di AWS IoT base per eseguire le seguenti attività:

- Identificare un guasto nell'apparecchiatura e informare il personale appropriato, inviando i dati ad AWS IoT Events.
- Storicizza determinati dati di asset per utilizzarli in soluzioni software esterne inviando dati ad Amazon DynamoDB.
- Generare rapporti settimanali, attivando una funzione AWS Lambda.

Puoi seguire un tutorial che illustra i passaggi necessari per configurare una regola che memorizza i valori delle proprietà in DynamoDB. Per ulteriori informazioni, consulta Pubblicazione degli aggiornamenti dei valori delle proprietà su Amazon DynamoDB.

Per ulteriori informazioni su come configurare una regola, consulta Rules nella AWS IoT Developer Guide.

Puoi anche riutilizzare i dati di altri AWS servizi in AWS IoT SiteWise. Per importare dati tramite l'azione della AWS IoT SiteWise regola, vedereAcquisizione di dati tramite regole AWS IoT Core.

Argomenti

- Informazioni sugli argomenti MQTT delle proprietà degli asset
- Utilizzo delle notifiche sulle proprietà degli asset
- Esporta i dati su Amazon S3 con notifiche sulle proprietà degli asset
- Integrazione con Grafana
- Integrazione di AWS IoT SiteWise e AWS IoT TwinMaker
- Rilevamento di anomalie nelle apparecchiature con Amazon Lookout for Equipment

Informazioni sugli argomenti MQTT delle proprietà degli asset

A ogni proprietà di asset è assegnato un percorso di argomento MQTT univoco nel formato seguente.

```
$aws/sitewise/asset-models/assetModelId/assets/assetId/properties/propertyId
```

> **Note**
>
> AWS IoT SiteWise non supporta il carattere jolly del filtro degli argomenti # (a più livelli) nel motore di regole Core. AWS IoT È invece possibile utilizzare il carattere jolly + (a livello singolo). Puoi, ad esempio, avvalerti del filtro di argomenti che segue per recuperare tutti gli aggiornamenti relativi a un particolare modello di asset.
>
> ```
> $aws/sitewise/asset-models/assetModelId/assets/+/properties/+
> ```
>
> Per ulteriori informazioni sui caratteri jolly dei filtri per argomenti, consulta gli argomenti nella Guida AWS IoT principale per gli sviluppatori.

Utilizzo delle notifiche sulle proprietà degli asset

È possibile abilitare le notifiche sulle proprietà su cui pubblicare AWS IoT Core gli aggiornamenti dei dati degli asset e quindi eseguire query sui dati. Con le notifiche sulle proprietà degli asset, AWS IoT SiteWise fornisce un AWS CloudFormation modello che puoi utilizzare per esportare AWS IoT SiteWise i dati in Amazon S3.

> **Note**
>
> I dati degli asset vengono inviati AWS IoT Core ogni volta che vengono ricevuti da AWS IoT SiteWise, indipendentemente dal fatto che il valore sia cambiato.

Argomenti

- Abilitazione delle notifiche delle proprietà di asset (console)
- Attivazione delle notifiche sulle proprietà degli asset ()AWS CLI
- Esecuzione di query sui messaggi di notifica delle proprietà degli asset

Abilitazione delle notifiche delle proprietà di asset (console)

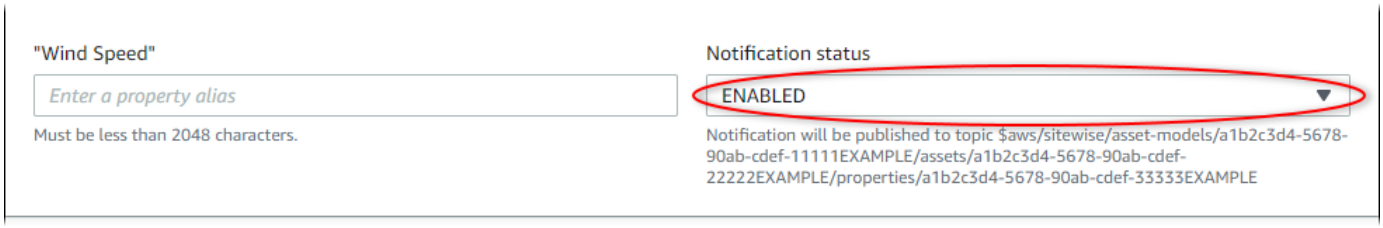
Per impostazione predefinita, AWS IoT SiteWise non pubblica gli aggiornamenti dei valori delle proprietà. Puoi utilizzare la AWS IoT SiteWise console per abilitare le notifiche per la proprietà di una risorsa.

Per abilitare o disabilitare le notifiche per una proprietà di asset (console)

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Asset.
3. Scegli l'asset per abilitare le notifiche di una proprietà.

> **Tip**
>
> Puoi scegliere l'icona a forma di freccia per espandere una gerarchia di asset e trovare il tuo asset.

4. Scegli Modifica.
5. Per lo stato di notifica della proprietà di asset scegli ABILITATO.



Puoi inoltre scegliere DISABILITATO per disabilitare le notifiche per la proprietà di asset.

6. Selezionare Salva.

Attivazione delle notifiche sulle proprietà degli asset ()AWS CLI

Per impostazione predefinita, AWS IoT SiteWise non pubblica gli aggiornamenti dei valori delle proprietà. È possibile utilizzare AWS Command Line Interface (AWS CLI) per abilitare o disabilitare le notifiche per una proprietà di un asset.

Per completare questa procedura, è necessario conoscere l'elemento `assetId` dell'asset e l'elemento `propertyId` della proprietà. Puoi anche usare l'ID esterno. Se hai creato una risorsa e non la conosci`assetId`, utilizza l'ListAssetsAPI per elencare tutte le risorse per un modello specifico.

Utilizzate l'DescribeAssetoperazione per visualizzare le proprietà della risorsa, compresi gli ID delle proprietà.

Utilizzate l'UpdateAssetPropertyoperazione per abilitare o disabilitare le notifiche per la proprietà di una risorsa. Specifica i seguenti parametri:

- `assetId`— L'ID della risorsa.
- `propertyId`— L'ID della proprietà dell'asset.
- `propertyNotificationState`— Lo stato di notifica del valore della proprietà: `ENABLED` o`DISABLED`.
- `propertyAlias`— L'alias della proprietà. Specificare l'alias esistente della proprietà quando si aggiorna lo stato di notifica. Se si omette questo parametro, l'alias esistente della proprietà viene rimosso.

Per abilitare o disabilitare le notifiche per una proprietà di asset (CLI)

1. Esegui il comando seguente per recuperare l'alias della proprietà di asset. Sostituisci *`asset-id`* con l'ID dell'asset e *`property-id`* con l'ID della proprietà.

```
aws iotsitewise describe-asset-property \
  --asset-id asset-id \
  --property-id property-id
```

   L'operazione restituisce una risposta contenente i dettagli della proprietà di asset nel formato seguente. L'alias della proprietà si trova in `assetProperty.alias` nell'oggetto JSON.

```
{
  "assetId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
  "assetName": "Wind Turbine 7",
  "assetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
  "assetProperty": {
    "id": "a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
    "name": "Wind Speed",
    "alias": "/company/windfarm/3/turbine/7/windspeed",
    "notification": {
      "topic": "$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/
assets/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE/properties/a1b2c3d4-5678-90ab-
cdef-33333EXAMPLE",
      "state": "DISABLED"
```

```
    },
    "dataType": "DOUBLE",
    "unit": "m/s",
    "type": {
      "measurement": {}
    }
  }
}
```

2. Esegui il comando seguente per abilitare le notifiche per la proprietà di asset. Sostituisci *property-alias* con l'alias della proprietà della risposta del comando precedente oppure ometti `--property-alias` per aggiornare la proprietà senza un alias.

```
aws iotsitewise update-asset-property \
  --asset-id asset-id \
  --property-id property-id \
  --property-notification-state ENABLED \
  --property-alias property-alias
```

   Puoi inoltre passare `--property-notification-state DISABLED` per disabilitare le notifiche per la proprietà di asset.

Esecuzione di query sui messaggi di notifica delle proprietà degli asset

Per interrogare le notifiche sulle proprietà degli asset, crea AWS IoT Core regole costituite da istruzioni SQL.

AWS IoT SiteWise pubblica gli aggiornamenti dei dati delle proprietà degli asset su AWS IoT Core nel seguente formato.

```
{
  "type": "PropertyValueUpdate",
  "payload": {
    "assetId": "String",
    "propertyId": "String",
    "values": [
      {
        "timestamp": {
          "timeInSeconds": Number,
          "offsetInNanos": Number
        },
```

```
        "quality": "String",
        "value": {
          "booleanValue": Boolean,
          "doubleValue": Number,
          "integerValue": Number,
          "stringValue": "String"
        }
      }
    ]
  }
}
```

Ogni struttura nell'`values`elenco è una struttura timestamp-quality-value (TQV).

- `timestamp` contiene l'orario UTC (epoca (Unix epoch)) corrente in secondi, con offset in nanosecondi.
- `quality` contiene una delle seguenti stringhe che indicano la qualità del punto dati:
  - `GOOD`— I dati non sono interessati da alcun problema.
  - `BAD`— I dati sono interessati da un problema come il guasto del sensore.
  - `UNCERTAIN`— I dati sono influenzati da un problema come l'imprecisione del sensore.
- `value` contiene uno dei seguenti campi, a seconda del tipo di proprietà:
  - `booleanValue`
  - `doubleValue`
  - `integerValue`
  - `stringValue`

Per analizzare i valori al di fuori dell'array `values`, è necessario utilizzare query complesse su oggetti nidificati nelle istruzioni SQL delle regole. Per ulteriori informazioni, consultate la sezione Interrogazioni con oggetti annidati nella Guida per gli AWS IoT sviluppatori oppure consultate il Pubblicazione degli aggiornamenti dei valori delle proprietà su Amazon DynamoDB tutorial per un esempio specifico di analisi dei messaggi di notifica delle proprietà degli asset.

Example Query di esempio per estrarre l'array dei valori

Nell'istruzione seguente viene illustrato come eseguire una query sull'array dei valori delle proprietà aggiornati per una proprietà di tipo doppio specifica su tutti gli asset con tale proprietà.

```
SELECT
```

```
  (SELECT VALUE (value.doubleValue) FROM payload.values) AS windspeed
FROM
  '$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/assets/+/
properties/a1b2c3d4-5678-90ab-cdef-33333EXAMPLE'
WHERE
  type = 'PropertyValueUpdate'
```

L'istruzione della query della regola precedente restituisce i dati nel formato seguente.

```
{
  "windspeed": [
    26.32020195042838,
    26.282584572975477,
    26.352566977372508,
    26.283084346171442,
    26.571883739599322,
    26.60684140743005,
    26.628738636715045,
    26.273486932802125,
    26.436379105473964,
    26.600590095377303
  ]
}
```

Example Query di esempio per estrarre un singolo valore

Nell'istruzione seguente viene illustrato come eseguire una query del primo valore dall'array dei valori delle proprietà per una proprietà di tipo doppio specifica su tutti gli asset con tale proprietà.

```
SELECT
  get((SELECT VALUE (value.doubleValue) FROM payload.values), 0) AS windspeed
FROM
  '$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/assets/+/
properties/a1b2c3d4-5678-90ab-cdef-33333EXAMPLE'
WHERE
  type = 'PropertyValueUpdate'
```

L'istruzione della query della regola precedente restituisce i dati nel formato seguente.

```
{
  "windspeed": 26.32020195042838
}
```

> **Important**
>
> Questa istruzione di query regola ignora gli aggiornamenti di valore diversi dal primo in ogni batch. Ogni lotto può contenere fino a 10 valori. Se è necessario includere i valori rimanenti, è necessario impostare una soluzione più complessa per l'output dei valori delle proprietà delle risorse ad altri servizi. Ad esempio, potete impostare una regola con un' AWS Lambda azione per ripubblicare ogni valore dell'array su un altro argomento e impostare un'altra regola per interrogare quell'argomento e pubblicare ogni valore nell'azione della regola desiderata.

Esporta i dati su Amazon S3 con notifiche sulle proprietà degli asset

Puoi esportare i dati in entrata AWS IoT SiteWise da un bucket Amazon S3 nel tuo account. Puoi eseguire il backup dei dati in un formato che puoi utilizzare per creare report storici o per analizzare i dati con metodi complessi.

> **Note**
>
> AWS IoT SiteWise supporta anche lo storage a freddo che consente di salvare i dati in un bucket Amazon S3 gestito dal cliente. Per ulteriori informazioni sui livelli di storage supportati, consulta. Gestione dell'archiviazione dei dati

AWS IoT SiteWise fornisce questa funzionalità come AWS CloudFormation modello. Quando crei uno stack dal modello, AWS CloudFormation crea AWS le risorse necessarie per lo streaming dei dati in entrata AWS IoT SiteWise da un bucket S3.

Quindi, il bucket S3 riceve tutti i dati sulle proprietà degli asset inviati dai messaggi di aggiornamento del valore delle proprietà. AWS IoT SiteWise Il bucket S3 riceve anche i metadati degli asset, che includono i nomi degli asset e delle proprietà, nonché altre informazioni.

Per ulteriori informazioni su come abilitare i messaggi di aggiornamento del valore delle proprietà delle proprietà degli asset da esportare in Amazon S3, consulta. Interazione con altri servizi AWS

Questa funzionalità archivia i dati sulle proprietà e i metadati degli asset nel formato Apache Parquet in Amazon S3. Parquet è un formato di dati a colonna che consente di risparmiare spazio e di eseguire query più rapidamente rispetto ai formati orientati alle righe come JSON.

> **Note**
>
> Quando questa funzionalità recupera i metadati delle risorse, supporta fino a circa 1.500 risorse. Questa limitazione si applica solo ai metadati degli asset. Questa limitazione non si applica al numero di risorse supportate quando la funzionalità esporta i dati sulle proprietà delle risorse.

Il nome di ogni risorsa include un prefisso che è possibile personalizzare quando si crea lo stack. Le risorse includono le seguenti:

- Un bucket Amazon S3
- AWS Lambda funzioni
- Qualsiasi AWS IoT Core regola
- AWS Identity and Access Management ruoli
- Uno stream Amazon Data Firehose
- Un database AWS Glue

Per un elenco completo, consulta Risorse create dal modello.

> **Important**
>
> Ti verranno addebitate le risorse create e consumate da questo AWS CloudFormation modello. Questi costi includono l'archiviazione e il trasferimento dei dati per più AWS servizi.

Argomenti

Crea lo AWS CloudFormation stack

È necessario creare uno stack in AWS CloudFormation per esportare i dati degli asset in Amazon S3.

Per esportare dati in Amazon S3

1. Aprire il modello AWS CloudFormation e accedere alla AWS Management Console.
2. Nella parte inferiore della pagina Create stack (Crea stack), seleziona Next (Avanti).
3. Nella pagina Specify stack details, inserisci un valore BucketNameper il bucket S3 creato da questo modello per ricevere i dati degli asset. Questo nome bucket deve essere univoco a livello globale. Per ulteriori informazioni, consulta le Regole per la denominazione dei bucket nella Guida per l'utente di Amazon Simple Storage Service.
4. (Facoltativo) Modificare uno qualsiasi degli altri parametri del modello:

   - GlobalResourcePrefix— Un prefisso per i nomi delle risorse globali, come i ruoli IAM, create da questo modello.
   - LocalResourcePrefix— Un prefisso per i nomi delle risorse create da questo modello nella regione corrente.

   > **Note**
   >
   > Se crei questo modello più volte, dovresti modificare i parametri del nome del bucket e del prefisso della risorsa per evitare conflitti tra i nomi delle risorse.

5. Seleziona Successivo.
6. Nella pagina Configure stack options (Configura opzioni pila), scegliere Next (Successivo).
7. Nella parte inferiore della pagina, seleziona la casella di controllo che dice Riconosco che AWS CloudFormation potrebbe creare risorse IAM.
8. Seleziona Crea stack.

   La creazione dello stack richiede alcuni minuti. Se non è possibile creare lo stack, l'account potrebbe non disporre di autorizzazioni sufficienti oppure è possibile che il nome bucket immesso esista già. Usare le fasi seguenti per eliminare lo stack e riprovare:

   a. Scegli Delete (Elimina) nell'angolo in alto a destra.

      L'eliminazione dello stack richiede alcuni minuti.

> **Note**
>
> AWS CloudFormation non elimina i bucket o i gruppi di CloudWatch log S3. È possibile eliminare queste risorse nelle console per tali servizi.

b. Se non è possibile eliminare lo stack, scegliere nuovamente Delete (Elimina).

c. Se lo stack non riesce a eliminare nuovamente lo stack, segui i passaggi nella AWS CloudFormation console per ignorare le risorse che non sono state eliminate e riprova.

9. Dopo che lo AWS CloudFormation stack è stato creato correttamente, segui la procedura successiva per esplorare i dati sulle proprietà degli asset in Amazon S3.

> **Important**
>
> Dopo aver creato lo stack, puoi vedere le nuove risorse nel tuo account. AWS Se si eliminano o si modificano queste risorse, la caratteristica potrebbe smettere di funzionare correttamente. Ti consigliamo di non modificare queste risorse a meno che non desideri interrompere l'invio dei dati al bucket o desideri personalizzare questa caratteristica.

Visualizza i tuoi dati in Amazon S3

Dopo aver creato la funzionalità, puoi visualizzare i dati sulle proprietà e i metadati degli asset in Amazon S3.

> **Note**
>
> Aggiornamenti dei metadati degli asset ogni sei ore. Potrebbe essere necessario attendere fino a sei ore per visualizzare i metadati delle risorse nel bucket S3.

Questa caratteristica archivia i dati delle proprietà di asset nelle colonne seguenti, in cui ogni riga contiene un punto dati:

- type — Il tipo di notifica della proprietà (). `PropertyValueUpdate`
- asset_id — L'ID dell'asset che ha ricevuto un punto dati.
- asset_property_id — L'ID della proprietà che ha ricevuto un punto dati per l'asset.

- time_in_seconds — L'ora in cui i dati sono stati ricevuti, espressa in secondi nell'epoca Unix.
- offset_in_nanos — L'offset in nanosecondi da. `timeInSeconds`
- asset_property_quality — La qualità del punto dati:,, o. `GOOD` `UNCERTAIN` `BAD`
- asset_property_value — Il valore del punto dati.
- asset_property_data_type — Il tipo di dati della proprietà dell'asset:,, o. `boolean` `double` `integer` `string`

Questa caratteristica archivia i metadati degli asset nelle colonne seguenti, in cui ogni riga contiene una proprietà di asset:

- asset_id — L'ID della risorsa.
- asset_name — Il nome della risorsa.
- asset_model_id — L'ID del modello dell'asset.
- asset_property_id — L'ID della proprietà dell'asset.
- asset_property_name — Il nome della proprietà dell'asset.
- asset_property_data_type — Il tipo di dati della proprietà dell'asset:,, o. `BOOLEAN` `DOUBLE` `INTEGER` `STRING`
- asset_property_unit — L'unità della proprietà dell'asset.
- asset_property_alias — L'alias della proprietà dell'asset.

Per visualizzare i AWS IoT SiteWise dati in Amazon S3

1. Accedi alla console Amazon S3.
2. Dall'elenco dei bucket, selezionare il bucket con il nome scelto al momento della creazione del modello.
3. Nel bucket, scegliere una delle seguenti cartelle:
   - `asset-property-updates`— Questa cartella contiene i dati sulle proprietà degli asset esportati da. AWS IoT SiteWise
   - `asset-metadata`— Questa cartella contiene i dettagli delle risorse esportati da. AWS IoT SiteWise
4. Scegliere l'oggetto da visualizzare.
5. Nella pagina dell'oggetto, eseguire le operazioni seguenti:

a. Scegliere la scheda Select from (Seleziona da).

   In questo pannello è possibile visualizzare l'anteprima dei record dei file Parquet.

b. In File format (Formato file), scegliere Parquet.

c. Per mostrare il contenuto del file in formato JSON, scegliete Mostra anteprima del file.

> **Note**
>
> Se i nuovi dati non vengono visualizzati nel bucket, verifica di aver abilitato le notifiche di aggiornamento del valore delle proprietà per le proprietà di asset. Per ulteriori informazioni, consulta Interazione con altri servizi AWS.

Per ulteriori informazioni su come analizzare i dati di asset archiviati nel bucket S3, consulta Analizza i dati esportati con Amazon Athena.

Analizza i dati esportati con Amazon Athena

Dopo aver archiviato i dati sulle proprietà degli asset in Amazon S3, puoi utilizzare diversi AWS servizi per generare report o analizzare e interrogare i tuoi dati:

- Esegui query SQL sui tuoi dati utilizzando Amazon Athena.
- Esegui analisi di big data con Amazon EMR.
- Cerca e analizza i tuoi dati utilizzando Amazon OpenSearch Service.

Puoi trovare altri AWS servizi in grado di interagire con i tuoi dati in Amazon S3 elencati in Analytics nel. AWS Management Console

> **Note**
>
> Lo stack crea un AWS Glue database per formattare i dati delle proprietà degli asset. Non è possibile eseguire query su questo database per i dati di asset. Segui i passaggi descritti in questa sezione per creare un AWS Glue database su cui eseguire query.

In questo tutorial, imparerai come configurare i prerequisiti per utilizzare Amazon Athena e come utilizzare Athena per eseguire query SQL sui dati degli asset esportati. AWS IoT SiteWise Per interrogare i dati con Athena, devi prima compilarli AWS Glue Data Catalog con i dati delle tue risorse. Il Data Catalog contiene database e tabelle e Athena può accedere ai dati in esso contenuti. Potete creare un AWS Glue crawler che aggiorni regolarmente il Data Catalog con i dati degli asset esportati.

Argomenti

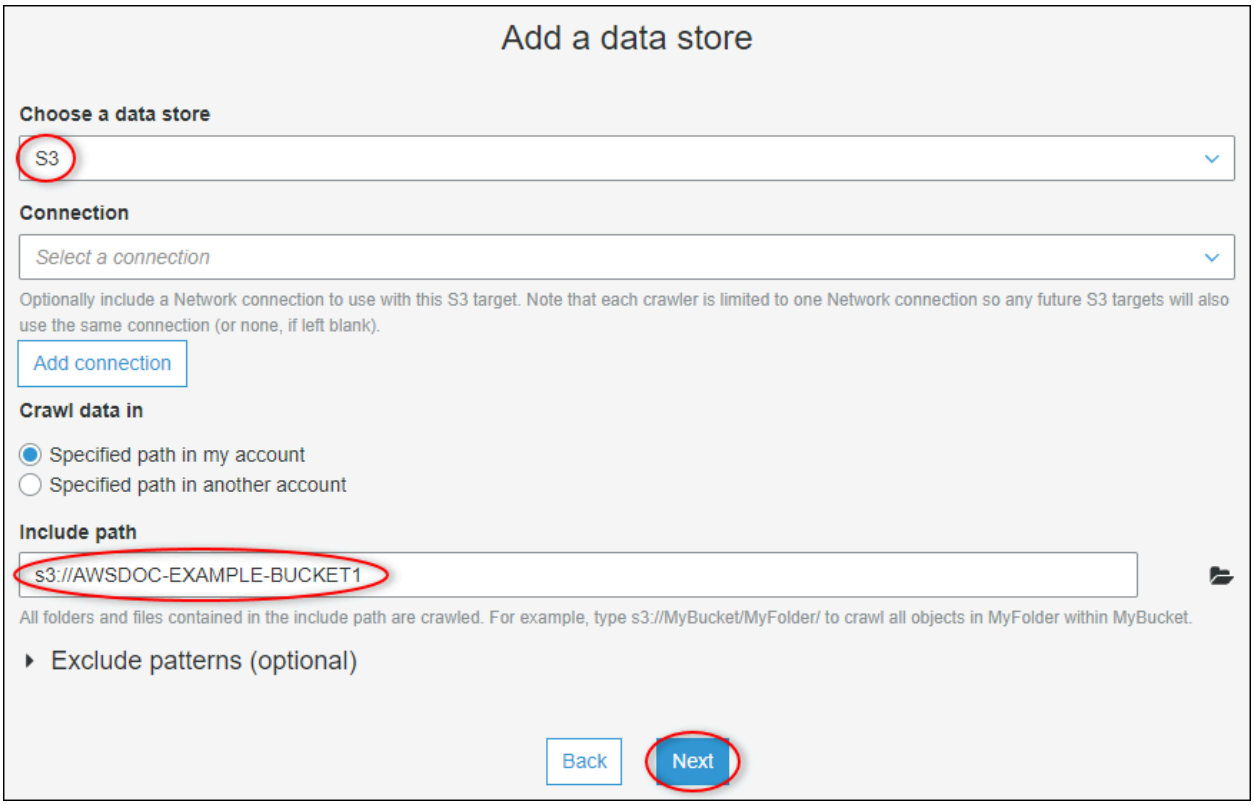
Configurazione di un crawler per compilare il file AWS Glue Data Catalog

AWS Glue i crawler eseguono la scansione degli archivi dati per popolare le tabelle in. AWS Glue Data Catalog In questa procedura, create ed eseguite un AWS Glue crawler per il bucket S3 che contiene i dati degli asset esportati. Il crawler crea una tabella per gli aggiornamenti delle proprietà di asset e una tabella per i metadati di asset. Quindi, puoi eseguire query SQL su queste tabelle con Athena. Per ulteriori informazioni, consulta Population the AWS Glue Data Catalog and Defining crawler nella Developer Guide.AWS Glue

Per creare un crawler AWS Glue

1. Passare alla console AWS Glue.
2. Nel riquadro di navigazione, selezionare Crawlers (Crawler).
3. Scegli Add crawler (Aggiungi crawler).
4. Nella pagina Aggiungi crawler eseguire le operazioni seguenti:
    a. Immettere un nome per il crawler, ad esempio **`IoTSiteWiseDataCrawler`**, quindi scegliere Avanti.
    b. Per Tipo di origine crawler, scegliere Datastore, quindi scegliere Avanti.
    c. Nella pagina Aggiungi un datastore, eseguire le operazioni seguenti:
        i. Per Scegli un datastore, scegliere S3.
        ii. In Includi percorso, immettere **`s3://`*`DOC-EXAMPLE-BUCKET1`*** per aggiungere il bucket dei dati di asset come datastore. Sostituisci *`DOC-EXAMPLE-BUCKET1 con il nome del bucket che hai`* scelto quando hai creato lo stack.

iii. Seleziona Successivo.



d. Nella pagina Aggiungi un altro datastore, scegliere No, quindi selezionare Avanti.

e. Nella pagina Scegli un ruolo IAM, procedi come segue:

   i. Per creare un nuovo ruolo di servizio che AWS Glue consenta di accedere al bucket S3, scegli Crea un ruolo IAM.

   ii. Immettere un suffisso per il nome del ruolo, ad esempio **`IoTSiteWiseDataCrawler`**.

   iii. Seleziona Successivo.

f. Per Frequenza, scegliere Oraria, quindi Avanti. Il crawler aggiorna le tabelle con nuovi dati ogni volta che viene eseguito, in modo da poter scegliere la frequenza più adatta al caso d'uso.

g. Nella pagina Configura output del crawler, eseguire le operazioni seguenti:

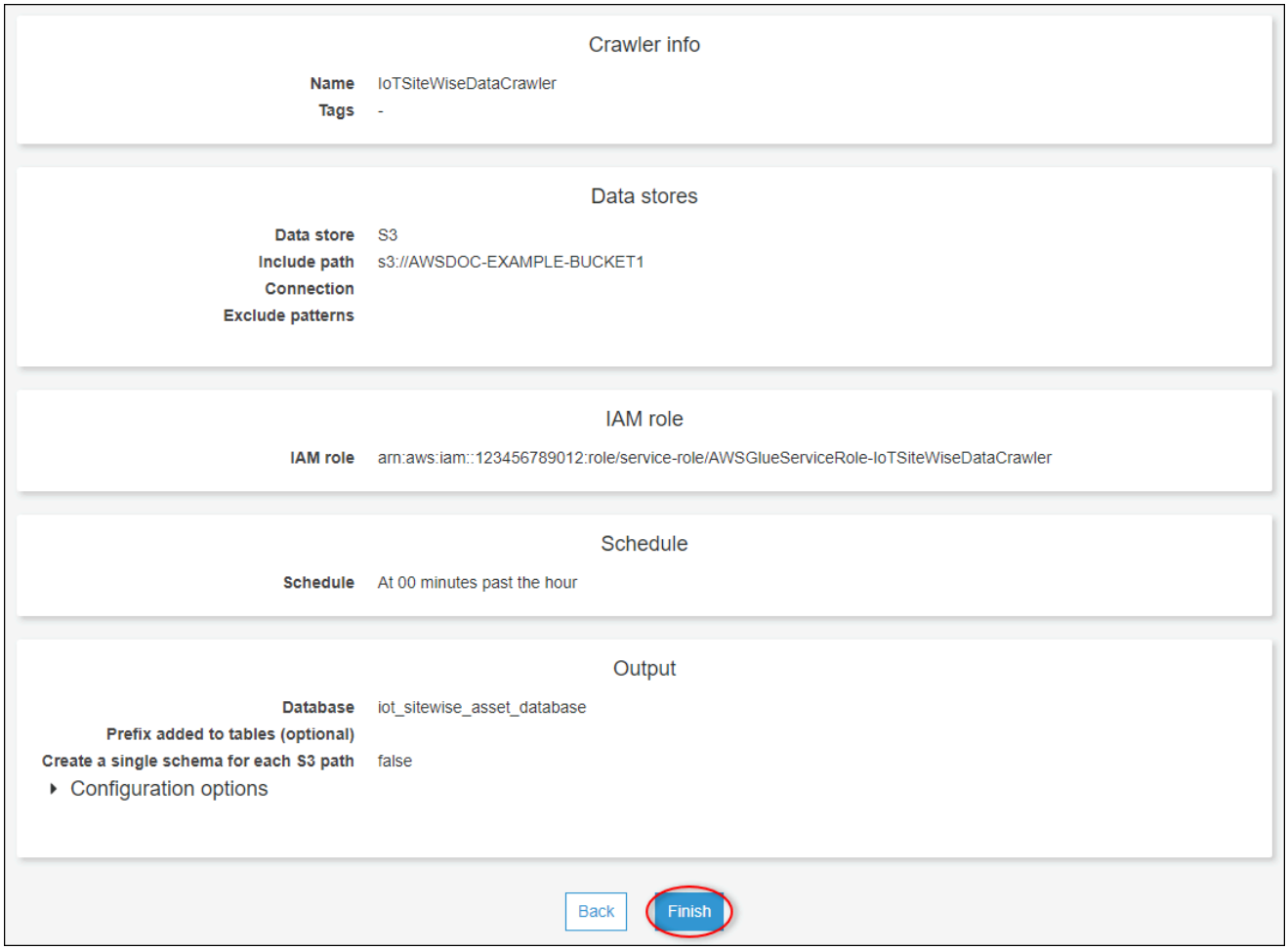
   i. Scegli Aggiungi database per creare un AWS Glue database per i dati degli asset.

   ii. Immettere un nome per il database, ad esempio **`iot_sitewise_asset_database`**.

   iii. Scegli Crea.

   iv. Seleziona Successivo.

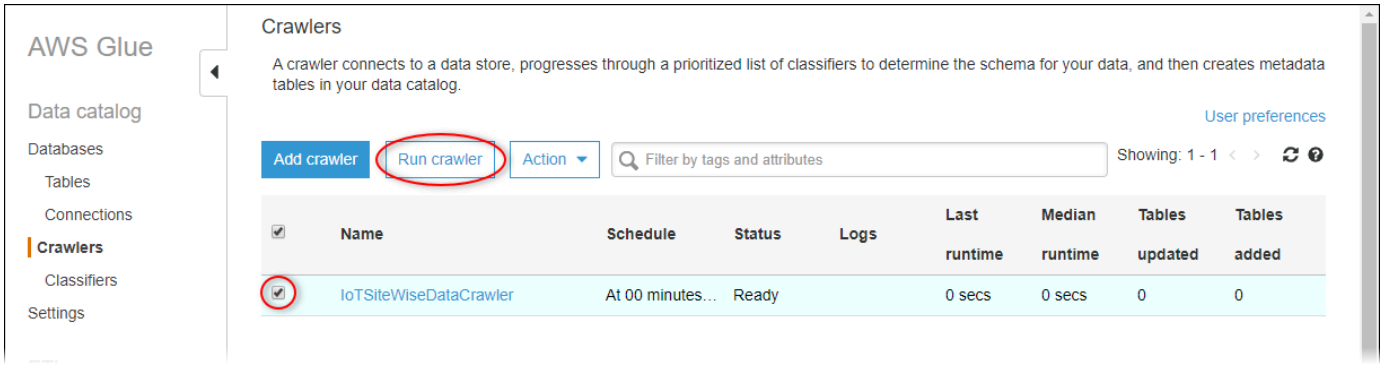
h. Esaminare i dettagli del crawler, quindi scegliere Fine.



Per impostazione predefinita, il nuovo crawler non viene eseguito immediatamente. È necessario eseguirlo manualmente o attendere che venga eseguito nella pianificazione configurata.

Per eseguire un crawler

1. Nella pagina Crawler, selezionare la casella di controllo relativa al nuovo crawler, quindi scegliere Esegui crawler.



2. Attendere finché il crawler non termina con stato Pronto.

   L'esecuzione del crawler può richiedere alcuni minuti e il suo stato si aggiorna automaticamente.

3. Nel pannello di navigazione, seleziona Tabelle.

   Vengono visualizzate due nuove tabelle: asset_metadata and asset_property_updates.

Interrogazione dei dati con Athena

Athena rileva automaticamente le tabelle dei dati degli asset in. AWS Glue Data Catalog Per eseguire query sull'intersezione di queste tabelle, è possibile creare una vista, che è una tabella dati logica. Per ulteriori informazioni, consulta Lavorare con le viste nella Guida per l'utente di Amazon Athena.

Dopo aver creato una visualizzazione che combina i dati delle proprietà degli asset e i metadati, è possibile eseguire query che generano i valori delle proprietà con i nomi degli asset e delle proprietà collegati. Per ulteriori informazioni, consulta Esecuzione di query SQL con Amazon Athena nella Amazon Athena User Guide.

Per interrogare i dati degli asset con Athena

1. Vai alla console Athena.

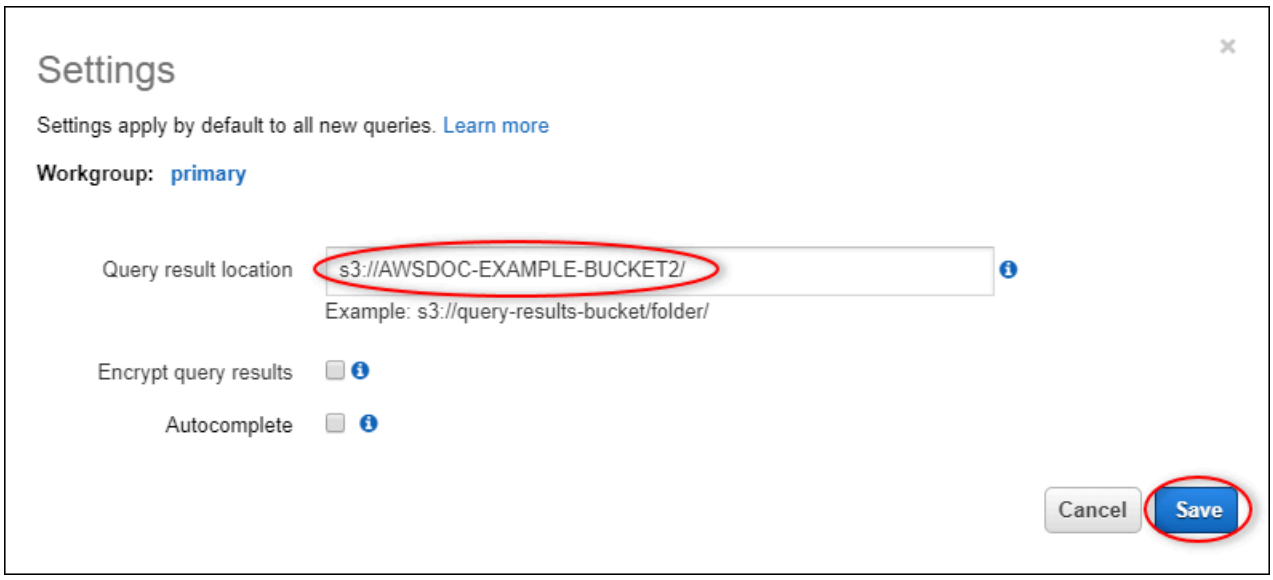
   Se viene visualizzata la pagina Nozioni di base, scegliere Inizia.

2. Se utilizzi Athena per la prima volta, completa i seguenti passaggi per configurare un bucket S3 per i risultati delle query. Athena memorizza i risultati delle tue ricerche in questo bucket.

   > **Important**
   >
   > Utilizzare un bucket diverso rispetto al bucket dei dati di asset, in modo che il crawler creato in precedenza non esegua il crawling dei risultati delle query. Ti consigliamo di creare un bucket da utilizzare solo per i risultati delle query Athena. Per ulteriori informazioni, vedi Come si crea un bucket S3? nella Guida per l'utente di Amazon Simple Storage Service.

   a. Seleziona Impostazioni.

   b. In Posizione dei risultati della query, inserisci il bucket S3 per i risultati della query Athena. Il bucket deve terminare con /.

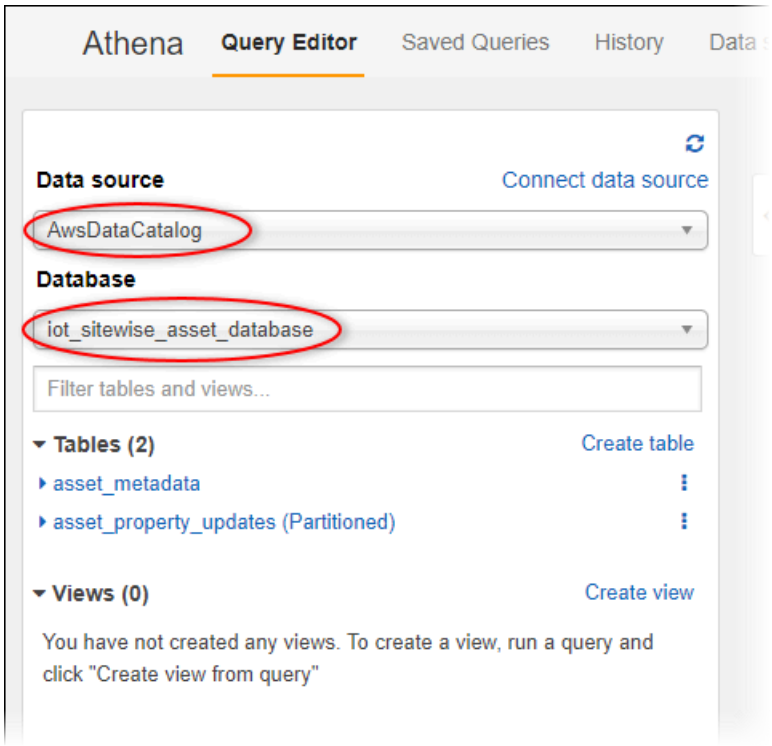


c. Selezionare Salva.

3. Il pannello a sinistra contiene l'origine dati su cui eseguire le query. Esegui questa operazione:

   a. Per Origine dati, scegli di AwsDataCatalogutilizzare il. AWS Glue Data Catalog

   b. Per Database, scegli il AWS Glue database che hai creato con il crawler.



Vengono visualizzate due tabelle: asset_metadata e asset_property_updates.

4. Per creare una visualizzazione a partire dalla combinazione di dati delle proprietà degli asset e metadati, immettere la query seguente e scegliere Esegui query.

```
CREATE
        OR REPLACE VIEW iot_sitewise_asset_data AS
SELECT "from_unixtime"("time_in_seconds" + ("offset_in_nanos" / 1000000000))
 "timestamp",
         "metadata"."asset_name",
         "metadata"."asset_property_name",
         "data"."asset_property_value",
         "metadata"."asset_property_unit",
         "metadata"."asset_property_alias"
FROM ( "iot_sitewise_asset_database".asset_property_updates data
INNER JOIN "iot_sitewise_asset_database".asset_metadata metadata
    ON ( ("data"."asset_id" = "metadata"."asset_id")
        AND ("data"."asset_property_id" = "metadata"."asset_property_id") ) );
```

   Questa query esegue il join dei dati delle proprietà degli asset e delle tabelle dei metadati sull'ID asset e l'ID proprietà per creare una visualizzazione. È possibile eseguire questa query più volte perché sostituisce la visualizzazione esistente, se esiste già.

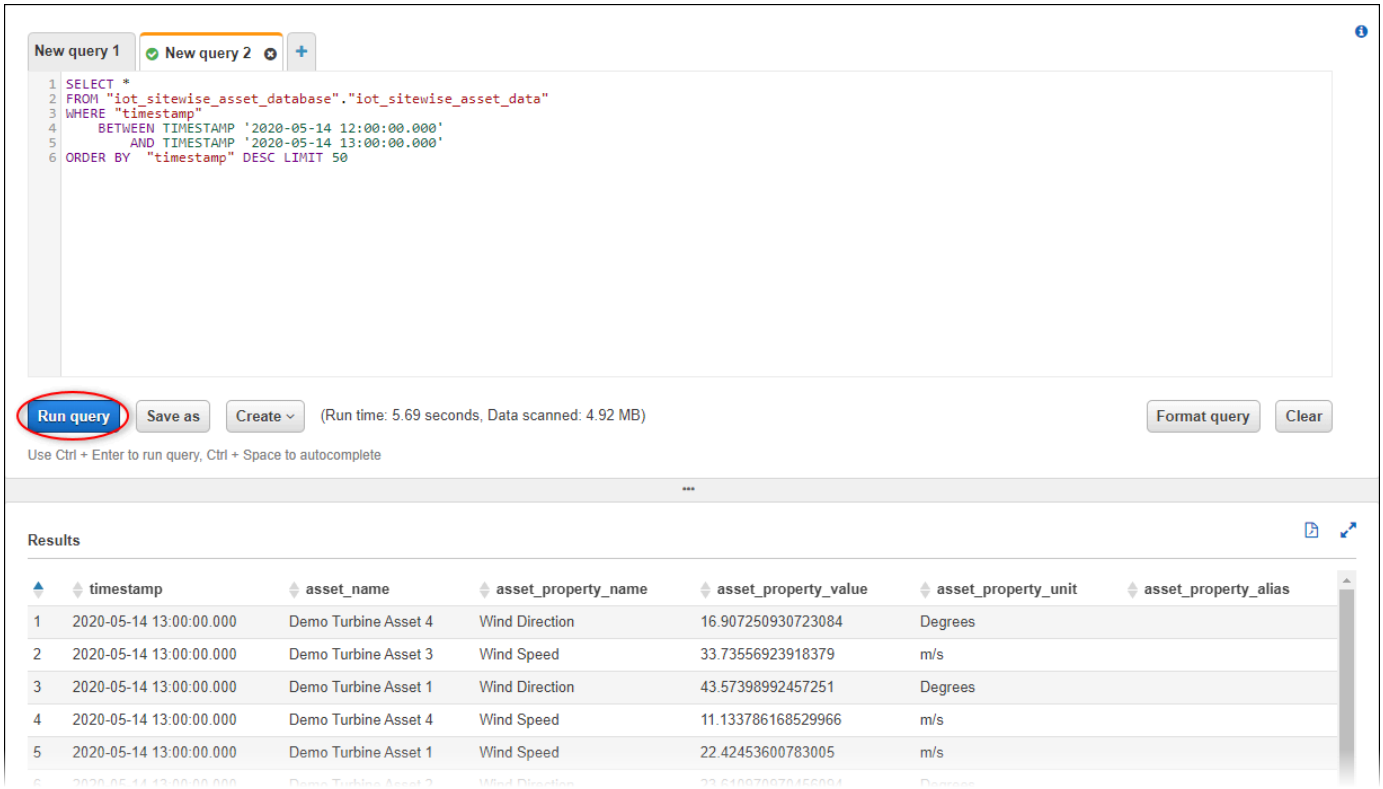
5. Per aggiungere una nuova query, scegli l'icona +.

6. Per visualizzare un esempio di dati degli asset, immettere la query seguente e scegliere Esegui query. Sostituire i timestamp con un intervallo per il quale il bucket contiene dati.

```
SELECT *
FROM "iot_sitewise_asset_database"."iot_sitewise_asset_data"
WHERE "timestamp"
    BETWEEN TIMESTAMP '2020-05-14 12:00:00.000'
        AND TIMESTAMP '2020-05-14 13:00:00.000'
ORDER BY  "timestamp" DESC LIMIT 50;
```

   Questa query genera fino a 50 punti dati tra due timestamp, con le voci più recenti visualizzate per prime.

   L'aspetto dell'output della query è simile ai risultati seguenti.



Ora puoi eseguire query utili alla tua applicazione. AWS IoT SiteWise Per ulteriori informazioni, consulta il riferimento SQL per Amazon Athena nella Amazon Athena User Guide.

Risorse create dal modello

Quando crei uno stack dal modello, AWS CloudFormation crea le seguenti risorse. I nomi della maggior parte delle risorse includono un prefisso che puoi personalizzare quando crei lo stack.

Parametri nome risorsa

- `BucketName`— Il nome del bucket S3 creato da questo modello che riceve i dati degli asset.
- `GlobalResourcePrefix`— Un prefisso per i nomi delle risorse globali create da questo modello. L'impostazione predefinita è `sitewise-export-to-s3`.
- `LocalResourcePrefix`— Un prefisso per i nomi delle risorse create da questo modello nella regione corrente. L'impostazione predefinita è `sitewise_export_to_s3`.

Risorse create dal modello AWS CloudFormation

Risorsa	Descrizione	Nome
Bucket S3 per i dati elaborati	Questo bucket contiene due cartelle. Una cartella riceve i dati appiattiti e formattati dal flusso di distribuzione di Firehose, mentre l'altra cartella riceve i metadati delle risorse.	`${BucketName}`
Database AWS Glue	Questo database contiene la AWS Glue tabella creata da questo stack.	`${LocalResourcePrefix}_firehose_glue_database`
AWS Glue tabella	Il flusso di distribuzione Firehose utilizza questa tabella per formattare i dati in formato Parquet.	`${LocalResourcePrefix}_firehose_glue_table`
Funzione AWS Lambda che trasforma i dati	Questa funzione appiattisce la matrice di valori nei messaggi di notifica dei valori delle proprietà inviati da. AWS IoT SiteWise	`${LocalResourcePrefix}_lambda_transform_function`
Ruolo IAM per la funzione Transform Lambda	Questo ruolo consente a Lambda di archiviare i log di runtime per la funzione di trasformazione.	`${GlobalResourcePrefix}-lambda-transform-role`
Politica IAM per il ruolo della funzione Transform Lambda	Questa politica consente a Lambda di archiviare i log di esecuzione per la funzione di trasformazione.	`${GlobalResourcePrefix}-lambda-transform-policy`
CloudWatch Registra il gruppo di log per la funzione di trasformazione	Questo gruppo di log contiene i log per la funzione di trasformazione.	`/aws/lambda/${LocalResourcePrefix}_l`

Risorsa	Descrizione	Nome
		`ambda_transform_function`
Funzione Lambda che raccoglie i metadati delle risorse	Questa funzione recupera i dettagli sugli asset contenuti AWS IoT SiteWise e li archivia in un bucket Amazon S3 creato da questo stack.	`${LocalResourcePrefix}_lambda_metadata_function`
Layer Lambda per la funzione metadati	Questo livello fornisce un AWS SDK che contiene AWS IoT SiteWise le operazioni utilizzate dalla funzione di metadati.	`${LocalResourcePrefix}_lambda_metadata_layer`
Ruolo IAM per la funzione Lambda dei metadati	Questo ruolo consente a Lambda di recuperare dettagli sugli asset in. AWS IoT SiteWise	`${GlobalResourcePrefix}-lambda-metadata-role`
Politica IAM per il ruolo della funzione Lambda dei metadati	Questa policy consente a Lambda di recuperare i dettagli sugli asset in. AWS IoT SiteWise	`${GlobalResourcePrefix}-lambda-metadata-policy`
EventBridgeevento pianificato per la funzione Lambda dei metadati	Questo evento pianificato esegue i metadati Lambda ogni 6 ore per aggiornare il bucket di metadati delle risorse.	`${LocalResourcePrefix}-metadata-event`
CloudWatch Registra il gruppo di log per la funzione dei metadati	Questo gruppo di log contiene i log per la funzione per metadati.	`/aws/lambda/${LocalResourcePrefix}_lambda_metadata_function`

Risorsa	Descrizione	Nome
Regola AWS IoT	Questa regola interroga i messaggi di notifica del valore delle proprietà e invia i dati degli asset a un flusso di distribuzione di Amazon Data Firehose.	`${LocalResourcePrefix}_iot_topic_rule`
Ruolo IAM per la regola AWS IoT	Questo ruolo consente di AWS IoT inviare dati al flusso di distribuzione di Firehose.	`${GlobalResourcePrefix}-core-firehose-role`
Politica IAM per il ruolo della AWS IoT regola	Questa politica consente di AWS IoT inviare dati al flusso di distribuzione di Firehose.	`${GlobalResourcePrefix}-core-firehose-policy`
Flusso di distribuzione Firehose	Questo flusso di distribuzione utilizza i dati della AWS IoT regola, li semplifica con una funzione Lambda e li consegna ad Amazon S3.	`${LocalResourcePrefix}_firehose_delivery_stream`
Ruolo IAM per il flusso di distribuzione	Questo ruolo consente a Firehose di eseguire operazioni sul bucket S3, sulla tabella AWS Glue , sulle funzioni Lambda e sul gruppo di log Logs. CloudWatch	`${GlobalResourcePrefix}-firehose-delivery-role`
CloudWatch Registra il gruppo di log per il flusso di consegna	Questo gruppo di log contiene un flusso di log che riceve i log relativi al flusso di distribuzione di Firehose. `S3 Delivery`	`/aws/kinesisfirehose/${LocalResourcePrefix}_firehose_delivery_stream`

Integrazione con Grafana

Grafana è una piattaforma di visualizzazione dei dati che puoi utilizzare per visualizzare e monitorare i dati nei dashboard. Nella versione 7.3.0 e successive di Grafana, puoi utilizzare il AWS IoT SiteWise plug-in per visualizzare i AWS IoT SiteWise dati delle tue risorse nelle dashboard Grafana. Puoi visualizzare i dati da più AWS fonti (come Amazon AWS IoT SiteWise Timestream CloudWatch e Amazon) e altre fonti di dati con un'unica dashboard Grafana.

Hai due opzioni per utilizzare il plugin: AWS IoT SiteWise

- Server Grafana locali

  Puoi configurare il AWS IoT SiteWise plugin su un server Grafana che gestisci. Per ulteriori informazioni su come aggiungere e utilizzare il plug-in, consulta il file README di AWS IoT SiteWise Datasource sul sito Web. GitHub

- AWSManaged Service for Grafana

  Puoi utilizzare il AWS IoT SiteWise plug-in nel AWS Managed Service for Grafana (AMG). AMG gestisce i server Grafana per te in modo che tu possa visualizzare i tuoi dati senza dover creare, impacchettare o implementare alcun hardware o altra infrastruttura Grafana. Per ulteriori informazioni, consulta i seguenti argomenti nella AWSManaged Service for Grafana User Guide:

  - Cos'è Amazon Managed Service for Grafana (AMG)?
  - Utilizzo della fonte di AWS IoT SiteWise dati

Example Esempio di dashboard Grafana

La seguente dashboard Grafana visualizza il parco eolico dimostrativo. Puoi accedere a questa dashboard demo sul sito web di Grafana Play.

Integrazione di AWS IoT SiteWise e AWS IoT TwinMaker

L'integrazione con AWS IoT TwinMaker garantisce l'accesso a funzionalità affidabiliAWS IoT SiteWise, come l'`ExecuteQuery`API per il recupero AWS IoT SiteWise dei dati e la ricerca avanzata degli asset nella console. AWS IoT SiteWise Per integrare i servizi e utilizzare queste funzionalità, devi prima abilitare l'integrazione.

Argomenti

- Abilitazione dell'integrazione
- Integrazione di AWS IoT SiteWise e AWS IoT TwinMaker

Abilitazione dell'integrazione

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni. L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Per ulteriori informazioni sulle azioni AWS IoT SiteWise supportate, vedere Azioni definite da AWS IoT SiteWise nel Service Authorization Reference.

Per ulteriori informazioni sul ruolo AWS IoT TwinMaker collegato al servizio, consulta la sezione Ruoli collegati ai servizi AWS IoT TwinMaker nella Guida per l'utente. AWS IoT TwinMaker

Prima di poter effettuare l'integrazione con AWS IoT SiteWise eAWS IoT TwinMaker, è necessario concedere le seguenti autorizzazioni che consentono l'integrazione con un'area di AWS IoT SiteWise lavoro collegata: AWS IoT TwinMaker

- `iotsitewise:EnableSiteWiseIntegration`— Consente AWS IoT SiteWise l'integrazione con uno spazio di lavoro collegatoAWS IoT TwinMaker. Questa integrazione consente di AWS IoT TwinMaker leggere tutte le informazioni di modellazione AWS IoT SiteWise tramite un ruolo collegato al AWS IoT TwinMaker servizio. Per abilitare questa autorizzazione, aggiungi la seguente policy al tuo ruolo IAM:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iotsitewise:EnableSiteWiseIntegration"
      ],
      "Resource": "*"
    }
  ]
}
```

Integrazione di AWS IoT SiteWise e AWS IoT TwinMaker

Per integrare AWS IoT SiteWise eAWS IoT TwinMaker, devi disporre di quanto segue:

- AWS IoT SiteWiseruolo collegato al servizio impostato nel tuo account

- AWS IoT TwinMakerruolo collegato al servizio impostato nel tuo account
- AWS IoT TwinMakerspazio di lavoro con ID `IoTSiteWiseDefaultWorkspace` nel tuo account nella regione.

Da integrare utilizzando la console AWS IoT SiteWise

Quando vedi il AWS IoT TwinMaker banner Integrazione con nella console, scegli Concedi l'autorizzazione. I prerequisiti vengono creati nel tuo account.

Da integrare utilizzando il AWS CLI

Per integrarlo AWS IoT SiteWise e AWS IoT TwinMaker utilizzarloAWS CLI, inserisci i seguenti comandi:

1. Chiama `CreateServiceLinkedRole` con un `AWSServiceName` di`iotsitewise.amazonaws.com`.

   ```
   aws iam create-service-linked-role --aws-service-name iotsitewise.amazonaws.com
   ```

2. Chiama `CreateServiceLinkedRole` con un `AWSServiceName` di `iottwinmaker.amazonaws.com`.

   ```
   aws iam create-service-linked-role --aws-service-name iottwinmaker.amazonaws.com
   ```

3. Chiama `CreateWorkspace` con un `ID` di`IoTSiteWiseDefaultWorkspace`.

   ```
   aws iottwinmaker create-workspace --workspace-id IoTSiteWiseDefaultWorkspace
   ```

Rilevamento di anomalie nelle apparecchiature con Amazon Lookout for Equipment

> **Note**
>
> Il rilevamento delle anomalie è disponibile solo nelle regioni in cui è disponibile Amazon Lookout for Equipment.

Puoi integrarti AWS IoT SiteWise con Amazon Lookout for Equipment per ottenere informazioni dettagliate sulle tue apparecchiature industriali attraverso il rilevamento delle anomalie e la manutenzione predittiva delle apparecchiature industriali. Lookout for Equipment è un servizio di machine learning (ML) per il monitoraggio delle apparecchiature industriali che rileva il comportamento anomalo delle apparecchiature e identifica potenziali guasti. Con Lookout for Equipment, è possibile implementare programmi di manutenzione predittiva e identificare i processi delle apparecchiature non ottimali. Per ulteriori informazioni su Lookout for Equipment, consulta Cos'è Amazon Lookout for Equipment? nella Guida per l'utente di Amazon Lookout for Equipment.

Quando crei una previsione per addestrare un modello ML a rilevare il comportamento anomalo delle apparecchiature, AWS IoT SiteWise invia i valori delle proprietà degli asset a Lookout for Equipment per addestrare un modello ML per rilevare il comportamento anomalo delle apparecchiature. Per definire una definizione di previsione su un modello di asset, specifichi i ruoli IAM necessari a Lookout for Equipment per accedere ai tuoi dati e alle proprietà da inviare a Lookout for Equipment e inviare i dati elaborati ad Amazon S3. Per ulteriori informazioni, consulta Creazione dei modelli di asset.

Per integrare AWS IoT SiteWise e Lookout for Equipment, dovrai eseguire i seguenti passaggi di alto livello:

- Aggiungi una definizione di previsione su un modello di asset che delinei le proprietà che desideri monitorare. La definizione di previsione è una raccolta riutilizzabile di misurazioni, trasformazioni e metriche utilizzata per creare previsioni sugli asset basati su quel modello di asset.
- Addestra la previsione in base ai dati storici che fornisci.
- Pianifica l'inferenza, che indica la AWS IoT SiteWise frequenza con cui eseguire una previsione specifica.

Una volta pianificata l'inferenza, il modello Lookout for Equipment monitora i dati ricevuti dalle apparecchiature e cerca anomalie nel comportamento delle apparecchiature. È possibile visualizzare e analizzare i risultati in SiteWise Monitor, utilizzando le operazioni dell'API AWS IoT SiteWise GET o la console Lookout for Equipment. Puoi anche creare allarmi utilizzando i rilevatori di allarme del modello Asset per avvisarti del comportamento anomalo delle apparecchiature.

Argomenti

- Addestramento di una previsione e inizio dell'inferenza (CLI)
- Addestramento di una previsione (CLI)
- Avvio o interruzione dell'inferenza su una previsione (CLI)

Aggiungere una definizione di previsione (console)

Per iniziare a inviare i dati raccolti da AWS IoT SiteWise a Lookout for Equipment, è necessario aggiungere AWS IoT SiteWise una definizione di previsione a un modello di asset.

Per aggiungere una definizione di previsione a un modello di asset AWS IoT SiteWise

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegliete Modelli e selezionate il modello di asset a cui desiderate aggiungere la definizione di previsione.
3. Scegliete Previsioni.
4. Scegli Aggiungi definizione di previsione.
5. Definisci i dettagli sulla definizione della previsione.

    a. Inserisci un nome e una descrizione univoci per la definizione della previsione. Scegli il nome con attenzione perché dopo aver creato la definizione di previsione, non puoi cambiarne il nome.

    b. Crea o seleziona un ruolo di autorizzazione IAM che AWS IoT SiteWise consenta di condividere i dati delle tue risorse con Amazon Lookout for Equipment. Il ruolo deve avere le seguenti politiche IAM e trust. Per informazioni sulla creazione del ruolo, consulta Creazione di un ruolo utilizzando politiche di fiducia personalizzate (console).

    Policy IAM

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "L4EPermissions",
            "Effect": "Allow",
            "Action": [
                "lookoutequipment:CreateDataset",
                "lookoutequipment:CreateModel",
                "lookoutequipment:CreateInferenceScheduler",
```

```
                "lookoutequipment:DescribeDataset",
                "lookoutequipment:DescribeDataIngestionJob",
                "lookoutequipment:DescribeModel",
                "lookoutequipment:DescribeInferenceScheduler",
                "lookoutequipment:ListInferenceExecutions",
                "lookoutequipment:StartDataIngestionJob",
                "lookoutequipment:StartInferenceScheduler",
                "lookoutequipment:UpdateInferenceScheduler",
                "lookoutequipment:StopInferenceScheduler"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:PutObject",
                "s3:GetObject"
            ],
            "Resource": ["arn:aws:s3:::iotsitewise-*"]
        },
        {
            "Sid": "IAMPermissions",
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam:::role/*"
        }
    ]
}
```

Policy di trust

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Principal": {
                "Service": "iotsitewise.amazonaws.com"
```

```
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "account_id"
                },
                "ArnEquals": {
                    "aws:SourceArn":
 "arn:aws:iotsitewise:region:account_id:asset/*"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "lookoutequipment.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "account_id"
                },
                "ArnEquals": {
                    "aws:SourceArn":
 "arn:aws:lookoutequipment:region:account_id:*"
                }
            }
        }
    ]
}
```

c. Seleziona Avanti.

6. Seleziona gli attributi dei dati (misurazioni, trasformazioni e metriche) che desideri inviare a Lookout for Equipment.

   a. (Facoltativo) Seleziona le misurazioni.

   b. (Facoltativo) Seleziona le trasformazioni.

   c. (Facoltativo) Seleziona le metriche.

   d. Seleziona Avanti.

7. Rivedi le tue selezioni. Per aggiungere la definizione di previsione al modello di asset, nella pagina di riepilogo, scegli Aggiungi definizione di previsione.

Puoi anche modificare o eliminare una definizione di previsione esistente a cui sono allegate previsioni attive.

Addestramento di una previsione (console)

Dopo aver aggiunto una definizione di previsione a un modello di asset, puoi addestrare le previsioni relative ai tuoi asset.

Per addestrare una previsione in AWS IoT SiteWise

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Risorse e seleziona la risorsa che desideri monitorare.
3. Scegliete Previsioni.
4. Seleziona i pronostici che desideri addestrare.
5. In Azioni, scegli Inizia allenamento ed esegui le seguenti operazioni:
    a. In Dettagli di previsione, seleziona un ruolo di autorizzazione IAM che AWS IoT SiteWise consenta di condividere i dati degli asset con Lookout for Equipment. Se devi creare un nuovo ruolo, scegli Crea un nuovo ruolo.
    b. Per le impostazioni dei dati di allenamento, inserisci un intervallo temporale dei dati di allenamento per selezionare quali dati utilizzare per addestrare la previsione.
    c. (Facoltativo) Per le etichette dati, fornisci un bucket Amazon S3 e un prefisso che contenga i dati di etichettatura. Per ulteriori informazioni sui dati di etichettatura, consulta Etichettatura dei dati nella Amazon Lookout for Equipment User Guide.
    d. Seleziona Avanti.
6. (Facoltativo) Se desideri che la previsione sia attiva non appena ha completato l'allenamento, in Impostazioni avanzate, seleziona Attiva automaticamente la previsione dopo l'allenamento, quindi procedi come segue:
    a. In Dati di input, per Frequenza di caricamento dei dati, definisci la frequenza di caricamento dei dati e per il tempo di ritardo di Offset, definisci la quantità di buffer da utilizzare.
    b. Seleziona Avanti.
7. Controlla i dettagli del pronostico e scegli Salva e inizia.

Avvio o interruzione dell'inferenza su una previsione (console)

> **Note**
>
> I costi di Lookout for Equipment si applicano alle inferenze programmate con i dati trasferiti AWS IoT SiteWise tra e Lookout for Equipment. Per ulteriori informazioni, consulta i prezzi di Amazon Lookout for Equipment.

Se hai aggiunto una previsione ma non hai scelto di attivarla dopo l'allenamento, devi attivarla per iniziare a monitorare le tue risorse.

Per avviare l'inferenza per una previsione

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Risorse e seleziona la risorsa a cui viene aggiunta la previsione.
3. Scegliete Previsioni.
4. Seleziona le previsioni che desideri attivare.
5. In Azioni, scegli Avvia inferenza ed esegui le seguenti operazioni:
   a. In Dati di input, per Frequenza di caricamento dei dati, definisci la frequenza di caricamento dei dati e per il tempo di ritardo di Offset, definisci la quantità di buffer da utilizzare.
   b. Scegli Salva e inizia.

Per interrompere l'inferenza per una previsione

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, scegli Risorse e seleziona la risorsa a cui viene aggiunta la previsione.
3. Scegliete Previsioni.
4. Seleziona i pronostici che desideri interrompere.
5. In Azioni, scegli Stop inference.

Aggiungere una definizione di previsione (CLI)

Per definire una definizione di previsione su un modello di asset nuovo o esistente, puoi utilizzare (). AWS Command Line Interface AWS CLI Dopo aver definito la definizione di previsione sul modello di asset, addestrate e pianificate l'inferenza per una previsione su un asset per eseguire il rilevamento delle anomalie con AWS IoT SiteWise Lookout for Equipment.

Prerequisiti

Per completare questi passaggi, è necessario disporre di un modello di asset e creare almeno una risorsa. Per ulteriori informazioni, consultare Creazione di un modello di asset (AWS CLI) e Creare una risorsa (AWS CLI).

Se non lo sapete AWS IoT SiteWise, dovete chiamare l'operazione `CreateBulkImportJob` API per importare i valori delle proprietà dell'asset AWS IoT SiteWise, che verranno utilizzati per addestrare il modello. Per ulteriori informazioni, consulta Crea un processo di importazione in blocco ()AWS CLI.

Per aggiungere una definizione di previsione

1. Crea un file denominato `asset-model-payload.json`. Segui i passaggi descritti in queste altre sezioni per aggiungere i dettagli del tuo modello di asset al file, ma non inviare la richiesta per creare o aggiornare il modello di asset.

   - Per ulteriori informazioni su come creare un modello di asset, consulta Creazione di un modello di asset (AWS CLI)
   - Per ulteriori informazioni su come aggiornare un modello di asset esistente, consulta Aggiornamento di un modello di asset o componente ()AWS CLI

2. Aggiungete un modello composito Lookout for Equipment `assetModelCompositeModels` () al modello di asset aggiungendo il codice seguente.

   - Sostituitelo *`Property`* con l'ID delle proprietà che desiderate includere. Per ottenere quegli ID, chiama `DescribeAssetModel`.
   - Sostituiscilo *`RoleARN`* con l'ARN di un ruolo IAM che consente a Lookout for Equipment di accedere ai tuoi dati. AWS IoT SiteWise

```
{
  ...
  "assetModelCompositeModels": [
    {
```

```
        "name": "L4Epredictiondefinition",
        "type": "AWS/L4E_ANOMALY",
        "properties": [
            {
              "name": "AWS/L4E_ANOMALY_RESULT",
              "dataType": "STRUCT",
              "dataTypeSpec": "AWS/L4E_ANOMALY_RESULT",
              "unit": "none",
              "type": {
                "measurement": {}
              }
            },
            {
              "name": "AWS/L4E_ANOMALY_INPUT",
              "dataType": "STRUCT",
              "dataTypeSpec": "AWS/L4E_ANOMALY_INPUT",
              "type": {
                 "attribute": {
                   "defaultValue": "{\"properties\": [\"Property1\", \"Property2\"]}"
                 }
              }
            },
            {
              "name": "AWS/L4E_ANOMALY_PERMISSIONS",
              "dataType": "STRUCT",
              "dataTypeSpec": "AWS/L4E_ANOMALY_PERMISSIONS",
              "type": {
                "attribute": {
                  "defaultValue": "{\"roleArn\": \"RoleARN\"}"
                }
              }
            },
            {
              "name": "AWS/L4E_ANOMALY_DATASET",
              "dataType": "STRUCT",
              "dataTypeSpec": "AWS/L4E_ANOMALY_DATASET",
              "type": {
                  "attribute": {}
              }
            },
            {
              "name": "AWS/L4E_ANOMALY_MODEL",
              "dataType": "STRUCT",
              "dataTypeSpec": "AWS/L4E_ANOMALY_MODEL",
```

```
            "type": {
              "attribute": {}
            }
          },
          {
            "name": "AWS/L4E_ANOMALY_INFERENCE",
            "dataType": "STRUCT",
            "dataTypeSpec": "AWS/L4E_ANOMALY_INFERENCE",
            "type": {
              "attribute": {}
            }
          },
          {
            "name": "AWS/L4E_ANOMALY_TRAINING_STATUS",
            "dataType": "STRUCT",
            "dataTypeSpec": "AWS/L4E_ANOMALY_TRAINING_STATUS",
            "type": {
              "attribute": {
                "defaultValue": "{}"
              }
            }
          },
          {
            "name": "AWS/L4E_ANOMALY_INFERENCE_STATUS",
            "dataType": "STRUCT",
            "dataTypeSpec": "AWS/L4E_ANOMALY_INFERENCE_STATUS",
            "type": {
              "attribute": {
                "defaultValue": "{}"
              }
            }
          }
    ]
}
```

3. Crea il modello di asset o aggiorna il modello di asset esistente. Esegui una di queste operazioni:

   - Per creare il modello di asset, esegui il seguente comando:

     ```
     aws iotsitewise create-asset-model --cli-input-json file://asset-model-
     payload.json
     ```

- Per aggiornare il modello di asset esistente, esegui il comando seguente. Sostituitelo *asset-model-id* con l'ID del modello di asset che desiderate aggiornare.

```
aws iotsitewise update-asset-model \
  --asset-model-id asset-model-id \
  --cli-input-json file://asset-model-payload.json
```

Dopo aver eseguito il comando, `assetModelId` annotatelo nella risposta.

Addestramento di una previsione e inizio dell'inferenza (CLI)

Ora che la definizione di previsione è stata definita, potete addestrare gli asset in base ad essa e avviare l'inferenza. Se vuoi addestrare la tua previsione ma non iniziare l'inferenza, passa a. Addestramento di una previsione (CLI) Per addestrare la previsione e iniziare l'inferenza sulla risorsa, avrai bisogno della `assetId` risorsa di destinazione.

Per addestrare e avviare l'inferenza della previsione

1. Esegui il seguente comando per trovare quanto segue`assetModelCompositeModelId`. `assetModelCompositeModelSummaries` *asset-model-id*Sostituitelo con l'ID del modello di asset in cui avete creatoAggiornamento di un modello di asset o componente ()AWS CLI.

```
aws iotsitewise describe-asset-model \
  --asset-model-id asset-model-id \
```

2. Eseguite il comando seguente per trovare `actionDefinitionId` l'`TrainingWithInferenceazione`. Sostituisci *asset-model-id*con l'ID utilizzato nel passaggio precedente e sostituisci *asset-model-composite-model-id*con l'ID restituito nel passaggio precedente.

```
aws iotsitewise describe-asset-model-composite-model \
  --asset-model-id asset-model-id \
  --asset-model-composite-model-id asset-model-composite-model-id \
```

3. Create un file chiamato `train-start-inference-prediction.json` e aggiungete il codice seguente, sostituendo il seguente:

   - *asset-id*con l'ID della risorsa di destinazione
   - *action-definition-id*con l'ID dell' TrainingWithInference azione

- *StartTime*con l'inizio dei dati di allenamento, forniti in secondi d'epoca
- *EndTime*con i dati di fine addestramento, forniti in secondi d'epoca

```
{
  "targetResource": {
    "assetId": "asset-id"
  },
  "actionDefinitionId": "action-definition-Id",
  "actionPayload":{
    "stringValue": "{\"l4ETrainingWithInference\":{\"trainingWithInferenceMode
\":\"START\",\"trainingPayload\":{\"exportDataStartTime\":StartTime,
\"exportDataEndTime\":EndTime},\"inferencePayload\":{\"dataDelayOffsetInMinutes
\":0,\"dataUploadFrequency\":\"PT5M\"}}}"
  }
}
```

4. Esegui il seguente comando per avviare l'addestramento e l'inferenza:

```
aws iotsitewise execute-action --cli-input-json file://train-start-inference-
prediction.json
```

Addestramento di una previsione (CLI)

Ora che la definizione di previsione è stata definita, puoi addestrare gli asset in base ad essa. Per addestrare la previsione sull'asset, avrai bisogno della risorsa `assetId` di destinazione.

Per addestrare la previsione

1. Esegui il seguente comando per trovare quanto segue`assetModelCompositeModelId`. `assetModelCompositeModelSummaries` *asset-model-id*Sostituitelo con l'ID del modello di asset in cui avete creatoAggiornamento di un modello di asset o componente ()AWS CLI.

```
aws iotsitewise describe-asset-model \
  --asset-model-id asset-model-id \
```

2. Eseguite il comando seguente per trovare `actionDefinitionId` l'`Training`azione. Sostituisci *asset-model-id*con l'ID utilizzato nel passaggio precedente e sostituisci *asset-model-composite-model-id*con l'ID restituito nel passaggio precedente.

```
aws iotsitewise describe-asset-model-composite-model \
  --asset-model-id asset-model-id \
  --asset-model-composite-model-id asset-model-composite-model-id \
```

3. Create un file chiamato `train-prediction.json` e aggiungete il codice seguente, sostituendo il seguente:

   - *asset-id*con l'ID della risorsa di destinazione
   - *action-definition-id*con l'ID dell'azione formativa
   - *StartTime*con i dati di inizio dell'allenamento, forniti in secondi epocali
   - *EndTime*con i dati di fine addestramento, forniti in secondi d'epoca
   - (Facoltativo) *BucketName* con il nome del bucket Amazon S3 che contiene i dati dell'etichetta
   - (Facoltativo) *Prefix* con il prefisso associato al bucket Amazon S3.

   > **Note**
   >
   > Includi sia il nome che il prefisso del bucket o nessuno dei due.

```
{
  "targetResource": {
    "assetId": "asset-id"
  },
  "actionDefinitionId": "action-definition-Id",
  "actionPayload":{ "stringValue": "{\"l4ETraining\": {\"trainingMode\":
\"START\",\"exportDataStartTime\": StartTime, \"exportDataEndTime\": EndTime,
 \"labelInputConfiguration\": {\"bucketName\": \"BucketName\", \"prefix\":
 \"Prefix\"}}}"
}
}
```

4. Esegui il seguente comando per iniziare l'allenamento:

```
aws iotsitewise execute-action --cli-input-json file://train-prediction.json
```

Prima di iniziare l'inferenza, è necessario completare l'addestramento. Per verificare lo stato della formazione, effettuate una delle seguenti operazioni:

- Dalla console, accedi alla risorsa su cui si basa la previsione.
- Da AWS CLI, chiama `BatchGetAssetPropertyValue` utilizzando l'indirizzo `propertyId` della `trainingStatus` proprietà.

Avvio o interruzione dell'inferenza su una previsione (CLI)

Una volta addestrata la previsione, puoi avviare l'inferenza per dire a Lookout for Equipment di iniziare a monitorare le tue risorse. Per avviare o interrompere l'inferenza, avrai bisogno della risorsa `assetId` di destinazione.

Per iniziare l'inferenza

1. Esegui il seguente comando per trovare il `assetModelCompositeModelId` sotto`assetModelCompositeModelSummaries`. *`asset-model-id`*Sostituitelo con l'ID del modello di asset in cui avete creatoAggiornamento di un modello di asset o componente ()AWS CLI.

   ```
   aws iotsitewise describe-asset-model \
     --asset-model-id asset-model-id \
   ```

2. Eseguite il comando seguente per trovare `actionDefinitionId` l'`Inference`azione. Sostituisci *`asset-model-id`*con l'ID utilizzato nel passaggio precedente e sostituisci *`asset-model-composite-model-id`*con l'ID restituito nel passaggio precedente.

   ```
   aws iotsitewise describe-asset-model-composite-model \
     --asset-model-id asset-model-id \
     --asset-model-composite-model-id asset-model-composite-model-id \
   ```

3. Create un file chiamato `start-inference.json` e aggiungete il codice seguente, sostituendo il seguente:

   - *`asset-id`*con l'ID della risorsa di destinazione
   - *`action-definition-id`*con l'ID dell'azione di inferenza iniziale
   - *`Offset`*con la quantità di buffer da usare
   - *`Frequency`*con la frequenza con cui vengono caricati i dati

   ```
   {
   ```

```
  "targetResource": {
    "assetId": "asset-id"
  },
  "actionDefinitionId": "action-definition-Id",
  "actionPayload":{ "stringValue": "{\"l4EInference\": {\"inferenceMode\":\"START
\",\"dataDelayOffsetInMinutes\": Offset, \"dataUploadFrequency\": \"Frequency\"}}"
}}
```

4. Esegui il seguente comando per avviare l'inferenza:

```
aws iotsitewise execute-action --cli-input-json file://start-inference.json
```

Per interrompere l'inferenza

1. Esegui il seguente comando per trovare il `assetModelCompositeModelId` sotto`assetModelCompositeModelSummaries`. *`asset-model-id`*Sostituitelo con l'ID del modello di asset in cui avete creatoAggiornamento di un modello di asset o componente ()AWS CLI.

```
aws iotsitewise describe-asset-model \
  --asset-model-id asset-model-id \
```

2. Eseguite il comando seguente per trovare `actionDefinitionId` l'`Inference`azione. Sostituisci *`asset-model-id`*con l'ID utilizzato nel passaggio precedente e sostituisci *`asset-model-composite-model-id`*con l'ID restituito nel passaggio precedente.

```
aws iotsitewise describe-asset-model-composite-model \
  --asset-model-id asset-model-id \
  --asset-model-composite-model-id asset-model-composite-model-id \
```

3. Create un file chiamato `stop-inference.json` e aggiungete il codice seguente, sostituendo il seguente:

   - *`asset-id`*con l'ID della risorsa di destinazione
   - *`action-definition-id`*con l'ID dell'azione di inferenza iniziale

```
{
  "targetResource": {
    "assetId": "asset-id"
```

```
  },
  "actionDefinitionId": "action-definition-Id",
  "actionPayload":{ "stringValue": "{\"l4EInference\":{\"inferenceMode\":\"STOP
\"}}"
}}
```

4. Esegui il comando seguente per interrompere l'inferenza:

```
aws iotsitewise execute-action --cli-input-json file://stop-inference.json
```

Gestione dell'archiviazione dei dati

È possibile AWS IoT SiteWise configurare il salvataggio dei dati nei seguenti livelli di storage:

Livello più elevato

L'hot storage tier è uno storage AWS IoT SiteWise gestito in serie temporali. Hot tier è più efficace per i dati a cui si accede di frequente, con bassa write-to-read latenza. I dati archiviati nell'hot tier vengono utilizzati dalle applicazioni industriali che richiedono un accesso rapido ai valori più recenti delle misurazioni delle apparecchiature. Ciò include applicazioni che visualizzano metriche in tempo reale con una dashboard interattiva o applicazioni che monitorano le operazioni e lanciano allarmi per identificare problemi di prestazioni.

Per impostazione predefinita, i dati inseriti vengono archiviati nel livello più AWS IoT SiteWise elevato. È possibile definire un periodo di conservazione per il livello caldo, dopodiché AWS IoT SiteWise spostare i dati nel livello più elevato su uno storage di livello caldo o freddo, in base alla configurazione. Per ottimizzare le prestazioni e l'efficienza in termini di costi, imposta il periodo di conservazione dei livelli più elevati in modo che sia più lungo del tempo necessario per recuperare spesso i dati. Viene utilizzato per metriche, allarmi e scenari di monitoraggio in tempo reale. Se non è impostato un periodo di conservazione, i dati vengono archiviati a tempo indeterminato nel livello più elevato.

Livello caldo

Il warm storage tier è un livello AWS IoT SiteWise gestito efficace per l'archiviazione economica dei dati storici. È ideale per recuperare grandi volumi di dati con caratteristiche di latenza media write-to-read . Utilizza il livello «warm» per archiviare i dati storici necessari per carichi di lavoro di grandi dimensioni. Ad esempio, viene utilizzato per il recupero dei dati per analisi, applicazioni di business intelligence (BI), strumenti di reporting e formazione di modelli di machine learning (ML). Se si abilita il livello di conservazione a freddo, è possibile definire un periodo di conservazione del livello caldo. Al termine del periodo di conservazione, AWS IoT SiteWise elimina i dati dal livello caldo.

Livello freddo

Il livello di cold storage utilizza un bucket Amazon S3 per archiviare dati usati raramente. Con il cold tier abilitato, AWS IoT SiteWise replica le serie temporali, incluse misurazioni, metriche, trasformazioni e aggregazioni e le definizioni dei modelli di asset ogni 6 ore. Cold tier viene utilizzato per archiviare dati che tollerano un'elevata latenza di lettura per report cronologici e backup.

Argomenti

Configurare le impostazioni di archiviazione

È possibile configurare le impostazioni di archiviazione per attivare lo storage warm tier gestito dal servizio e anche per replicare i dati sul piano freddo. Per ulteriori informazioni sul periodo di conservazione per i livelli caldo e caldo, consultaImpatto sulla conservazione dei dati. Durante la configurazione delle impostazioni di archiviazione, procedi come segue:

- Conservazione a livello elevato: imposta un periodo di conservazione per quanto tempo i dati vengono archiviati nel livello più elevato prima che vengano eliminati e spostati nello storage a livello caldo o a livello freddo gestito dal servizio in base alle impostazioni di archiviazione. AWS IoT SiteWise eliminerà tutti i dati del livello più elevato che esistevano prima della fine del periodo di conservazione. Se non imposti un periodo di conservazione, i tuoi dati vengono archiviati a tempo indeterminato nel livello più elevato.
- Conservazione a livello caldo: imposta un periodo di conservazione per quanto tempo i dati vengono archiviati nel livello caldo prima che vengano eliminati dallo AWS IoT SiteWise storage e trasferiti nello storage cold tier gestito dal cliente. AWS IoT SiteWise elimina tutti i dati dal livello caldo che esisteva prima della fine del periodo di conservazione. Se non è impostato un periodo di conservazione, i dati vengono archiviati a tempo indeterminato nel livello caldo.

> **Note**
>
> Per migliorare le prestazioni delle query, imposta un periodo di conservazione di livello elevato con lo storage di livello caldo.

Impatto della conservazione dei dati nello storage di livello caldo e caldo

- Quando si riduce il periodo di conservazione dello storage hot tier, i dati vengono trasferiti in modo permanente dal livello caldo a quello caldo o freddo. Quando si riduce il periodo di conservazione

del livello caldo, i dati vengono spostati sul livello freddo ed eliminati definitivamente dal livello caldo.

- Quando si aumenta il periodo di conservazione dello storage di livello caldo o caldo, la modifica influisce sui dati inviati AWS IoT SiteWise da quel momento in poi. AWS IoT SiteWise non recupera i dati dallo storage a caldo o a freddo per inserirli nel livello più caldo. Ad esempio, se il periodo di conservazione dello storage hot tier è inizialmente impostato su 30 giorni e poi aumentato a 60 giorni, occorrono 30 giorni perché lo storage hot tier contenga 60 giorni di dati.

Argomenti

Configura le impostazioni di archiviazione per il livello caldo (console)

La procedura seguente mostra come configurare le impostazioni di archiviazione per replicare i dati sul livello warm della AWS IoT SiteWise console.

Per configurare le impostazioni di archiviazione nella console

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, in Impostazioni, scegli Archiviazione.
3. Nell'angolo in alto a destra, scegliere Edit (Modifica).
4. Nella pagina Modifica spazio di archiviazione, procedi come segue:
5. Per le impostazioni Hot tier, procedi come segue:

    - Se desideri impostare un periodo di conservazione per il periodo di archiviazione dei dati nel livello più elevato prima di essere eliminati e spostati nello storage di livello caldo gestito dal servizio, scegli Abilita periodo di conservazione.
    - Per configurare un periodo di conservazione, inserisci un numero intero e scegli un'unità. Il periodo di conservazione deve essere maggiore o uguale a 30 giorni.

AWS IoT SiteWise elimina tutti i dati del livello più importante che sono più vecchi del periodo di conservazione. Se non imposti un periodo di conservazione, i dati vengono archiviati a tempo indeterminato.

6. (Consigliato) Per le impostazioni del livello Warm, procedi come segue:

   - Per attivare l'archiviazione di livello caldo, seleziona Confermo e attiva l'opzione di archiviazione di livello caldo per attivare l'archiviazione di livello caldo.
   - (Facoltativo) Per configurare un periodo di conservazione, inserisci un numero intero e scegli un'unità. Il periodo di conservazione deve essere maggiore o uguale a 365 giorni.

   AWS IoT SiteWise elimina i dati del livello «warm» che esistevano prima del periodo di conservazione. Se non imposti un periodo di conservazione, i dati vengono archiviati a tempo indeterminato.

   > **Note**
   >
   > - Quando si opta per il livello caldo, la configurazione viene visualizzata una sola volta.
   > - Per impostare la conservazione a caldo, è necessario disporre di un livello di archiviazione a caldo o a freddo. Per l'efficienza in termini di costi e il recupero dei dati storici, AWS IoT SiteWise consiglia di archiviare i dati a lungo termine nel livello caldo.
   > - Per impostare la conservazione del livello caldo, è necessario disporre di un livello di conservazione a freddo.

7. Scegli Salva per salvare le impostazioni di archiviazione.

Nella sezione AWS IoT SiteWise Archiviazione, lo storage Warm tier si trova in uno di questi stati:

- Abilitato: se i dati esistevano prima del periodo di conservazione del livello più elevato, li AWS IoT SiteWise sposta nel livello caldo».
- Disabilitato: lo storage warm tier è disabilitato.

Configura le impostazioni di archiviazione per warm tier (AWS CLI)

È possibile configurare le impostazioni di archiviazione per spostare i dati al livello caldo utilizzando AWS CLI i comandi seguenti.

Per evitare di sovrascrivere la configurazione esistente, recupera le informazioni sulla configurazione di archiviazione corrente eseguendo il comando seguente:

```
aws iotsitewise describe-storage-configuration
```

Example risposta senza una configurazione di livello freddo esistente

```
{
          "storageType": "SITEWISE_DEFAULT_STORAGE",
          "disassociatedDataStorage": "ENABLED",
          "configurationStatus": {
              "state": "ACTIVE"
          },
          "lastUpdateDate": "2021-10-14T15:53:35-07:00",
          "warmTier": "DISABLED"
}
```

Example risposta con la configurazione Cold Tier esistente

```
{
      "storageType": "MULTI_LAYER_STORAGE",
          "multiLayerStorage": {
            "customerManagedS3Storage": {
            "s3ResourceArn": "arn:aws:s3:::bucket-name/prefix/",
            "roleArn": "arn:aws:iam::aws-account-id:role/role-name"
            }
          },
      "disassociatedDataStorage": "ENABLED",
      "retentionPeriod": {
      "numberOfDays": retention-in-days
      },
       "configurationStatus": {
       "state": "ACTIVE"
      },
      "lastUpdateDate": "2023-10-25T15:59:46-07:00",
      "warmTier": "DISABLED"
}
```

Configura le impostazioni di archiviazione per il piano caldo con AWS CLI

Esegui il comando seguente per configurare le impostazioni di archiviazione. Sostituisci `file-name` con il nome del file che contiene la configurazione AWS IoT SiteWise di archiviazione.

```
aws iotsitewise put-storage-configuration --cli-input-json file://file-name.json
```

Example AWS IoT SiteWise configurazione con livello caldo e caldo

```
{
            "storageType": "SITEWISE_DEFAULT_STORAGE",
            "disassociatedDataStorage": "ENABLED",
            "warmTier": "ENABLED",
            "retentionPeriod": {
               "numberOfDays": hot-tier-retention-in-days
             }

}
```

`hot-tier-retention-in-days`deve essere un numero intero maggiore o uguale a 30 giorni.

Example response

```
{
            "storageType": "SITEWISE_DEFAULT_STORAGE",
            "configurationStatus": {
            "state": "UPDATE_IN_PROGRESS"
            }
}
```

Se hai abilitato lo storage a livello freddo, vediConfigura le impostazioni di archiviazione con AWS CLI un piano freddo esistente.

Configura le impostazioni di archiviazione con AWS CLI un piano freddo esistente

Configura le impostazioni di archiviazione utilizzando AWS CLI lo storage a livello freddo esistente

- Esegui il comando seguente per configurare le impostazioni di archiviazione. Sostituisci *`file-name`* con il nome del file che contiene la configurazione AWS IoT SiteWise di archiviazione.

  ```
  aws iotsitewise put-storage-configuration --cli-input-json file://file-name.json
  ```

Example AWS IoT SiteWise configurazione dello storage

- Sostituisci *bucket-name con il nome del* tuo bucket Amazon S3.
- Sostituisci il *prefisso* con il tuo prefisso Amazon S3.
- Sostituiscilo *aws-account-id*con l'ID del tuo account. AWS
- Sostituisci *role-name* con il nome del ruolo di accesso Amazon S3 che AWS IoT SiteWise consente di inviare dati ad Amazon S3.
- Sostituisci *hot-tier-retention-in-days* con un numero intero maggiore o uguale a 30 giorni.
- Sostituisci *warm-tier-retention-in-days* con un numero intero maggiore o uguale a 365 giorni.

> **Note**
>
> AWS IoT SiteWise eliminerà tutti i dati del livello caldo più vecchi del periodo di conservazione del livello freddo. Se non imposti un periodo di conservazione, i dati vengono archiviati a tempo indeterminato.

```
{
      "storageType": "MULTI_LAYER_STORAGE",
        "multiLayerStorage": {
          "customerManagedS3Storage": {
              "s3ResourceArn": "arn:aws:s3:::bucket-name/prefix/",
              "roleArn": "arn:aws:iam::aws-account-id:role/role-name"
              }
          },
    "disassociatedDataStorage": "ENABLED",
    "retentionPeriod": {
      "numberOfDays": hot-tier-retention-in-days
    },
    "warmTier": "ENABLED",
    "warmTierRetentionPeriod": {
      "numberOfDays": warm-tier-retention-in-days
    }
}
```

Example response

```
{
      "storageType": "MULTI_LAYER_STORAGE",
      "configurationStatus": {
        "state": "UPDATE_IN_PROGRESS"
       }
}
```

Configura le impostazioni di archiviazione per il livello freddo (console)

La procedura seguente mostra come configurare le impostazioni di archiviazione per replicare i dati nel livello freddo della AWS IoT SiteWise console.

Per configurare le impostazioni di archiviazione nella console

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione, in Impostazioni, scegli Archiviazione.
3. Nell'angolo in alto a destra, scegliere Edit (Modifica).
4. Nella pagina Modifica spazio di archiviazione, procedi come segue:

   a. Per le impostazioni di archiviazione, scegli Abilita archiviazione a freddo. La memorizzazione a livello freddo è disabilitata per impostazione predefinita.

   b. Per la posizione del bucket S3, inserisci il nome di un bucket Amazon S3 esistente e un prefisso.

   > **Note**
   >
   > - Amazon S3 utilizza il prefisso come nome di cartella nel bucket Amazon S3. Il prefisso deve contenere da 1 a 255 caratteri e terminare con una barra (/). AWS IoT SiteWise I dati vengono salvati in questa cartella.
   > - Se non disponi di un bucket Amazon S3, scegli Visualizza, quindi creane uno nella console Amazon S3. Per ulteriori informazioni, consulta Crea il tuo primo bucket S3 nella Amazon S3 User Guide.

   c. Per il ruolo di accesso S3, esegui una delle seguenti operazioni:

- Scegli Crea un ruolo da un modello AWS gestito, crea AWS automaticamente un ruolo IAM che consente di AWS IoT SiteWise inviare dati ad Amazon S3.
- Scegli Usa un ruolo esistente, quindi scegli il ruolo che hai creato dall'elenco.

> **Note**
>
> - È necessario utilizzare lo stesso nome di bucket Amazon S3 per la posizione del bucket S3 utilizzato nel passaggio precedente e nella policy IAM.
> - Assicurati che il tuo ruolo disponga delle autorizzazioni mostrate nell'esempio seguente.
>
>   Example politica delle autorizzazioni:
>
> ```
> {
>       "Version": "2012-10-17",
>       "Statement": [
>           {
>               "Effect": "Allow",
>               "Action": [
>                   "s3:PutObject",
>                   "s3:GetObject",
>                   "s3:DeleteObject",
>                   "s3:GetBucketLocation",
>                   "s3:ListBucket"
>               ],
>               "Resource": [
>                   "arn:aws:s3:::bucket-name",
>                   "arn:aws:s3:::bucket-name/*"
>               ]
>           }
>       ]
>   }
> ```
>
>   Sostituisci *bucket-name* con il nome del tuo bucket Amazon S3.

d. Per configurare l'hot tier, consulta la Fase 5 del Configura le impostazioni di archiviazione per il livello caldo (console)

e. (Facoltativo) Per AWS IoT Analytics l'integrazione, procedi come segue.

i. Se desideri utilizzarli AWS IoT Analytics per interrogare i tuoi dati, scegli Archivio AWS IoT Analytics dati abilitato.

ii. AWS IoT SiteWise genera un nome per il tuo data store oppure puoi inserire un nome diverso.

AWS IoT SiteWise crea automaticamente un data store in AWS IoT Analytics cui salvare i dati. Per interrogare i dati, puoi usarli AWS IoT Analytics per creare set di dati. Per ulteriori informazioni, consulta Lavorare con AWS IoT SiteWise i dati nella Guida per l'AWS IoT Analytics utente.

f. Selezionare Salva.

Nella sezione AWS IoT SiteWise Archiviazione, lo storage Cold tier può avere uno dei seguenti valori:

- Abilitato: AWS IoT SiteWise replica i dati nel bucket Amazon S3 specificato.
- Abilitazione: AWS IoT SiteWise sta elaborando la richiesta per abilitare lo storage a freddo. Il completamento di questo processo può richiedere diversi minuti.
- Enable_Failed: AWS IoT SiteWise impossibile elaborare la tua richiesta di abilitare lo storage a freddo. Se hai abilitato AWS IoT SiteWise l'invio di log ad Amazon CloudWatch Logs, puoi utilizzare questi log per risolvere i problemi. Per ulteriori informazioni, consulta Monitoraggio con Amazon CloudWatch Logs.
- Disabilitato: lo storage a livello freddo è disabilitato.

Configura le impostazioni di archiviazione per il livello freddo (AWS CLI)

La procedura seguente mostra come configurare le impostazioni di archiviazione per replicare i dati nel livello freddo utilizzando AWS CLI.

Per configurare le impostazioni di archiviazione utilizzando AWS CLI

1. Per esportare i dati in un bucket Amazon S3 nel tuo account, esegui il seguente comando per configurare le impostazioni di archiviazione. Sostituisci *file-name* con il nome del file che contiene la configurazione di storage. AWS IoT SiteWise

```
aws iotsitewise put-storage-configuration --cli-input-json file://file-name.json
```

Example AWS IoT SiteWise configurazione dello storage

- Sostituisci *bucket-name con il nome del* tuo bucket Amazon S3.
- Sostituisci il *prefisso* con il tuo prefisso Amazon S3.
- Sostituiscilo *aws-account-id*con l'ID del tuo account. AWS
- Sostituisci *role-name* con il nome del ruolo di accesso Amazon S3 che AWS IoT SiteWise consente di inviare dati ad Amazon S3.
- Sostituisci *retention-in-days*con un numero intero maggiore o uguale a 30 giorni.

```
{
      "storageType": "MULTI_LAYER_STORAGE",
      "multiLayerStorage": {
          "customerManagedS3Storage": {
              "s3ResourceArn": "arn:aws:s3:::bucket-name/prefix/",
              "roleArn": "arn:aws:iam::aws-account-id:role/role-name"
          }
      },
      "retentionPeriod": {
          "numberOfDays": retention-in-days,
          "unlimited": false
      }
  }
```

Note

- È necessario utilizzare lo stesso nome di bucket Amazon S3 nella configurazione AWS IoT SiteWise dello storage e nella policy IAM.
- Assicurati che il tuo ruolo disponga delle autorizzazioni mostrate nell'esempio seguente.

  Example politica delle autorizzazioni:

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

```
                "Action": [
                    "s3:PutObject",
                    "s3:GetObject",
                    "s3:DeleteObject",
                    "s3:GetBucketLocation",
                    "s3:ListBucket"
                ],
                "Resource": [
                    "arn:aws:s3:::bucket-name",
                    "arn:aws:s3:::bucket-name/*"
                ]
            }
        ]
    }
```

Sostituisci *bucket-name* con il nome del tuo bucket Amazon S3.

Example response

```
{
    "storageType": "MULTI_LAYER_STORAGE",
    "retentionPeriod": {
        "numberOfDays": 100,
        "unlimited": false
    },
    "configurationStatus": {
        "state": "UPDATE_IN_PROGRESS"
    }
}
```

Note

L'aggiornamento della configurazione di storage può richiedere alcuni minuti. AWS IoT SiteWise

2. Per recuperare le informazioni sulla configurazione dello storage, esegui il comando seguente.

```
aws iotsitewise describe-storage-configuration
```

Example response

```
{
      "storageType": "MULTI_LAYER_STORAGE",
      "multiLayerStorage": {
          "customerManagedS3Storage": {
              "s3ResourceArn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/torque/",
              "roleArn": "arn:aws:iam::123456789012:role/SWAccessS3Role"
          }
      },
      "retentionPeriod": {
          "numberOfDays": 100,
          "unlimited": false
      },
      "configurationStatus": {
          "state": "ACTIVE"
      },
      "lastUpdateDate": "2021-03-30T15:54:14-07:00"
  }
```

3. Per interrompere l'esportazione dei dati nel bucket Amazon S3, esegui il seguente comando per configurare le impostazioni di archiviazione.

```
aws iotsitewise put-storage-configuration --storage-type SITEWISE_DEFAULT_STORAGE
```

> **Note**
>
> Per impostazione predefinita, i tuoi dati vengono archiviati solo nel livello più elevato di. AWS IoT SiteWise

Example response

```
{
      "storageType": "SITEWISE_DEFAULT_STORAGE",
      "configurationStatus": {
          "state": "UPDATE_IN_PROGRESS"
      }
  }
```

4. Per recuperare le informazioni sulla configurazione dello storage, esegui il comando seguente.

```
aws iotsitewise describe-storage-configuration
```

Example response

```
{
      "storageType": "SITEWISE_DEFAULT_STORAGE",
      "configurationStatus": {
          "state": "ACTIVE"
      },
      "lastUpdateDate": "2021-03-30T15:57:14-07:00"
  }
```

(Facoltativo) Creare un archivio AWS IoT Analytics dati ()AWS CLI

Un AWS IoT Analytics data store è un repository scalabile e interrogabile che riceve e archivia dati. Puoi utilizzare la AWS IoT SiteWise console o le AWS IoT Analytics API per creare un archivio dati per salvare AWS IoT Analytics i tuoi dati. AWS IoT SiteWise Per interrogare i dati, crei set di dati utilizzando. AWS IoT Analytics Per ulteriori informazioni, consulta Lavorare con AWS IoT SiteWise i dati nella Guida per l'AWS IoT Analytics utente.

I passaggi seguenti consentono AWS CLI di creare un archivio dati in AWS IoT Analytics.

Per creare un archivio dati, esegui il comando seguente. Sostituisci *file-name* con il nome del file che contiene la configurazione del data store.

```
aws iotanalytics create-datastore --cli-input-json file://file-name.json
```

> **Note**
>
> - È necessario specificare il nome di un bucket Amazon S3 esistente. Se non disponi di un bucket Amazon S3, creane prima uno. Per ulteriori informazioni, consulta Crea il tuo primo bucket S3 nella Guida per l'utente di Amazon S3.
> - È necessario utilizzare lo stesso nome di bucket Amazon S3 nella configurazione AWS IoT SiteWise dello storage, nella policy IAM e nella configurazione del AWS IoT Analytics data store.

Example AWS IoT Analytics configurazione del data store

Sostituisci *s3-bucket-name con il nome del* tuo AWS IoT Analytics data store *data-store-name*e il nome del bucket Amazon S3.

```
{
      "datastoreName": "data-store-name",
      "datastoreStorage": {
          "iotSiteWiseMultiLayerStorage": {
              "customerManagedS3Storage": {
                  "bucket": "s3-bucket-name"
              }
          }
      },
      "retentionPeriod": {
          "numberOfDays": 90
      }
  }
```

Example response

```
{
      "datastoreName": "datastore_IoTSiteWise_demo",
      "datastoreArn": "arn:aws:iotanalytics:us-west-2:123456789012:datastore/
datastore_IoTSiteWise_demo",
      "retentionPeriod": {
          "numberOfDays": 90,
          "unlimited": false
      }
  }
```

Risoluzione dei problemi relativi alle impostazioni di archiviazione

Utilizza le seguenti informazioni per individuare e risolvere i problemi relativi alla configurazione dello storage.

Problemi

- Errore: il bucket non esiste
- Errore: accesso negato al percorso Amazon S3
- Errore: non è possibile assumere il ruolo ARN

- Errore: accesso al bucket Amazon S3 interregionale non riuscito

Errore: il bucket non esiste

Soluzione: AWS IoT SiteWise non è stato possibile trovare il bucket Amazon S3. Assicurati di inserire il nome di un bucket Amazon S3 esistente nella regione corrente.

Errore: accesso negato al percorso Amazon S3

Soluzione: AWS IoT SiteWise impossibile accedere al tuo bucket Amazon S3. Esegui questa operazione:

- Assicurati di utilizzare lo stesso bucket Amazon S3 specificato nella policy IAM.
- Assicurati che il tuo ruolo disponga delle autorizzazioni mostrate nell'esempio seguente.

  Example policy di autorizzazioni

```
{
      "Version": "2012-10-17",
      "Statement": [
          {
              "Effect": "Allow",
              "Action": [
                  "s3:PutObject",
                  "s3:GetObject",
                  "s3:DeleteObject",
                  "s3:GetBucketLocation",
                  "s3:ListBucket"
              ],
              "Resource": [
                  "arn:aws:s3:::bucket-name",
                  "arn:aws:s3:::bucket-name/*"
              ]
          }
      ]
  }
```

  Sostituisci *bucket-name* con il nome del tuo bucket Amazon S3.

Errore: non è possibile assumere il ruolo ARN

Soluzione: non AWS IoT SiteWise potrei assumere il ruolo IAM per tuo conto. Assicurati che il tuo ruolo si affidi al seguente servizio:`iotsitewise.amazonaws.com`. Per ulteriori informazioni, consulta Non posso assumere un ruolo, consulta la Guida per l'utente IAM.

Errore: accesso al bucket Amazon S3 interregionale non riuscito

Soluzione: il bucket Amazon S3 che hai specificato si trova in una regione diversa. AWS Assicurati che il bucket e gli AWS IoT SiteWise asset Amazon S3 si trovino nella stessa regione.

Percorsi dei file e schemi di dati salvati nella fase fredda

AWS IoT SiteWise archivia i dati nella fase fredda replicando serie temporali, tra cui misurazioni, metriche, trasformazioni e aggregazioni, nonché definizioni di asset e modelli di asset. Di seguito vengono descritti i percorsi dei file e gli schemi dei dati inviati al livello freddo.

Argomenti

- Dati dell'attrezzatura (misurazioni)
- Metriche, trasformazioni e aggregazioni
- Metadati delle risorse
- metadati della gerarchia degli asset
- File di indice dei dati di archiviazione

Dati dell'attrezzatura (misurazioni)

AWS IoT SiteWise esporta i dati dell'apparecchiatura (misurazioni) nella zona fredda una volta ogni sei ore. I dati grezzi vengono salvati nel livello freddo nel formato Apache AVRO (`.avro`).

Percorso del file

AWS IoT SiteWise memorizza i dati dell'apparecchiatura (misurazioni) nel livello freddo utilizzando il seguente modello.

```
{keyPrefix}/raw/startYear={startYear}/startMonth={startMonth}/startDay={startDay}/
seriesBucket={seriesBucket}/raw_{timeseriesId}_{startTimestamp}_{quality}.avro
```

Ogni percorso di file verso i dati grezzi in Amazon S3 contiene i seguenti componenti.

Componente del percorso	Descrizione
`keyPrefix`	Il prefisso Amazon S3 che hai specificato nella configurazione dello AWS IoT SiteWise storage. Amazon S3 utilizza il prefisso come nome di cartella nel bucket.
`raw`	La cartella che memorizza i dati delle serie temporali provenienti dall'apparecchiatura (misurazioni). La `raw` cartella viene salvata nella cartella dei prefissi.
`seriesBucket`	Un numero esadecimale compreso tra 00 e ff. Questo numero è derivato da. `timeSeriesId` Questa partizione viene utilizzata per aumentare la velocità effettiva durante le operazioni di AWS IoT SiteWise scrittura sul livello freddo. Quando usi Amazon Athena per eseguire query, puoi utilizzare la partizione per il partizionamento fine per migliorare le prestazioni delle query. `seriesBucket` e `timeSeriesBucket` nei metadati degli asset c'è lo stesso numero.
`startYear`	L'anno dell'ora di inizio esclusiva associata ai dati delle serie temporali.
`startMonth`	Il mese dell'ora di inizio esclusiva associata ai dati delle serie temporali.
`startDay`	Il giorno del mese dell'ora di inizio esclusiva associata ai dati delle serie temporali.
`fileName`	Il nome del file utilizza il carattere di sottoline atura (_) come delimitatore per separare quanto segue: • Il prefisso. `raw`

Componente del percorso	Descrizione
	• Il `timeSeriesId` valore. • Il timestamp dell'epoca dell'ora di inizio esclusiva associata ai dati delle serie temporali. • La qualità dei dati. Valori validi: `GOODBAD`, e`UNCERTAIN` . Per ulteriori informazioni, AssetPropertyValueconsulta l'AWS IoT SiteWise API Reference. Il file viene salvato nel `.avro` formato utilizzan do la compressione Snappy.

Example percorso del file verso i dati grezzi nella fase fredda

```
keyPrefix/raw/startYear=2021/startMonth=1/startDay=2/seriesBucket=a2/
raw_7020c8e2-e6db-40fa-9845-ed0dddd4c77d_95e63da7-d34e-43e1-
bc6f-1b490154b07a_1609577700_GOOD.avro
```

Campi

Lo schema dei dati grezzi esportati nel livello freddo contiene i seguenti campi.

Nome del campo	Tipi supportati	Tipo di predefinito	Descrizione
`seriesId`	`string`	N/D	L'ID che identific a i dati delle serie temporali provenien ti dall'apparecchiatu ra (misurazioni). È possibile utilizzare questo campo per unire dati grezzi e metadati delle risorse nelle query.

Nome del campo	Tipi supportati	Tipo di predefinito	Descrizione
`timeInSeconds`	`long`	N/D	La data e l'ora, in secondi, nel formato Unix epoch. I dati frazionari in nanosecondi sono forniti da. `offsetInNanos`
`offsetInNanos`	`long`	N/D	L'offset in nanosecondi da. `timeInSeconds`
`quality`	`string`	N/D	La qualità del valore delle serie temporali.
`doubleValue`	`double` o `null`	`null`	Dati di serie temporali di tipo double (numero in virgola mobile).
`stringValue`	`string` o `null`	`null`	Dati di serie temporali di tipo string (sequenza di caratteri).
`integerValue`	`int` o `null`	`null`	Dati di serie temporali di tipo intero (numero intero).
`booleanValue`	`boolean` o `null`	`null`	Dati di serie temporali di tipo booleano (vero o falso).

Nome del campo	Tipi supportati	Tipo di predefinito	Descrizione
`jsonValue`	`string` o `null`	`null`	Dati di serie temporali di tipo JSON (tipi di dati complessi memorizzati come stringa).
`recordVersion`	`long` o `null`	`null`	Il numero di versione del record. È possibile utilizzare il numero di versione per selezionare il record più recente. I record più recenti hanno numeri di versione più grandi.

Example dati grezzi nella fase fredda


```
{"seriesId":"e9687d2a-0dbe-4f65-9ed6-6f443cba41f7_95e63da7-d34e-43e1-
bc6f-1b490154b07a","timeInSeconds":1625675887,"offsetInNanos":0,"quality":"GOOD","doubleValue":
{"double":0.75},"stringValue":null,"integerValue":null,"booleanValue":null,"jsonValue":null,"re
  {"seriesId":"e9687d2a-0dbe-4f65-9ed6-6f443cba41f7_95e63da7-d34e-43e1-
bc6f-1b490154b07a","timeInSeconds":1625675889,"offsetInNanos":0,"quality":"GOOD","doubleValue":
{"double":0.69},"stringValue":null,"integerValue":null,"booleanValue":null,"jsonValue":null,"re
  {"seriesId":"e9687d2a-0dbe-4f65-9ed6-6f443cba41f7_95e63da7-d34e-43e1-
bc6f-1b490154b07a","timeInSeconds":1625675890,"offsetInNanos":0,"quality":"GOOD","doubleValue":
{"double":0.66},"stringValue":null,"integerValue":null,"booleanValue":null,"jsonValue":null,"re
  {"seriesId":"e9687d2a-0dbe-4f65-9ed6-6f443cba41f7_95e63da7-d34e-43e1-
bc6f-1b490154b07a","timeInSeconds":1625675891,"offsetInNanos":0,"quality":"GOOD","doubleValue":
{"double":0.92},"stringValue":null,"integerValue":null,"booleanValue":null,"jsonValue":null,"re
  {"seriesId":"e9687d2a-0dbe-4f65-9ed6-6f443cba41f7_95e63da7-d34e-43e1-
bc6f-1b490154b07a","timeInSeconds":1625675892,"offsetInNanos":0,"quality":"GOOD","doubleValue":
{"double":0.73},"stringValue":null,"integerValue":null,"booleanValue":null,"jsonValue":null,"re
```

Metriche, trasformazioni e aggregazioni

AWS IoT SiteWise esporta metriche, trasforma e aggrega nel livello freddo una volta ogni sei ore. Le metriche, le trasformazioni e gli aggregati vengono salvati nel livello freddo nel formato Apache AVRO (). `.avro`

Percorso del file

AWS IoT SiteWise archivia metriche, trasformazioni e aggregazioni nel livello freddo utilizzando il seguente modello.

```
{keyPrefix}/agg/startYear={startYear}/startMonth={startMonth}/startDay={startDay}/
seriesBucket={seriesBucket}/agg_{timeseriesId}_{startTimestamp}_{quality}.avro
```

Ogni percorso di file verso metriche, trasformazioni e aggregazioni in Amazon S3 contiene i seguenti componenti.

Componente del percorso	Descrizione
`keyPrefix`	Il prefisso Amazon S3 che hai specificato nella configurazione dello AWS IoT SiteWise storage. Amazon S3 utilizza il prefisso come nome di cartella nel bucket.
`agg`	La cartella che memorizza i dati delle serie temporali provenienti dalle metriche. La `agg` cartella viene salvata nella cartella dei prefissi.
`seriesBucket`	Un numero esadecimale compreso tra 00 e ff. Questo numero è derivato da. `timeSeriesId` Questa partizione viene utilizzata per aumentare la velocità effettiva durante le operazioni di AWS IoT SiteWise scrittura sul livello freddo. Quando usi Amazon Athena per eseguire query, puoi utilizzare la partizione per il partizionamento fine per migliorare le prestazioni delle query.

Componente del percorso	Descrizione
	`seriesBucket` e `timeSeriesBucket` nei metadati degli asset c'è lo stesso numero.
`startYear`	L'anno dell'ora di inizio esclusiva associata ai dati delle serie temporali.
`startMonth`	Il mese dell'ora di inizio esclusiva associata ai dati delle serie temporali.
`startDay`	Il giorno del mese dell'ora di inizio esclusiva associata ai dati delle serie temporali.
`fileName`	Il nome del file utilizza il carattere di sottoline atura (_) come delimitatore per separare quanto segue: • Il prefisso. `raw` • Il `timeSeriesId` valore. • Il timestamp dell'epoca dell'ora di inizio esclusiva associata ai dati delle serie temporali. • La qualità dei dati. Valori validi: `GOODBAD`, e`UNCERTAIN` . Per ulteriori informazioni, AssetPropertyValueconsulta l'AWS IoT SiteWise API Reference. Il file viene salvato nel `.avro` formato utilizzan do la compressione Snappy.

Example percorso del file verso le metriche nella fase fredda

```
keyPrefix/agg/startYear=2021/startMonth=1/startDay=2/seriesBucket=a2/
agg_7020c8e2-e6db-40fa-9845-ed0dddd4c77d_95e63da7-d34e-43e1-
bc6f-1b490154b07a_1609577700_GOOD.avro
```

Campi

Lo schema di metriche, trasformazioni e aggregati esportati nel livello freddo contiene i seguenti campi.

Nome del campo	Tipi supportati	Tipo di predefinito	Descrizione
`seriesId`	`string`	N/D	L'ID che identifica i dati delle serie temporali provenienti da apparecchiature, metriche o trasformazioni. È possibile utilizzare questo campo per unire dati non elaborati e metadati delle risorse nelle query.
`timeInSeconds`	`long`	N/D	La data e l'ora, in secondi, nel formato Unix epoch. I dati frazionari in nanosecondi sono forniti da. `offsetInNanos`
`offsetInNanos`	`long`	N/D	L'offset in nanosecondi da. `timeInSeconds`
`quality`	`string`	N/D	La qualità con cui filtrare i dati degli asset.
`resolution`	`string`	N/D	L'intervallo di tempo in cui aggregare i dati.

Nome del campo	Tipi supportati	Tipo di predefinito	Descrizione
`count`	`double` o `null`	`null`	Il numero totale di punti dati per le variabili specificate nell'intervallo di tempo corrente.
`average`	`double` o `null`	`null`	La media dei valori delle variabili specificate nell'intervallo di tempo corrente.
`min`	`double` o `null`	`null`	Il minimo dei valori delle variabili specificate nell'intervallo di tempo corrente.
`max`	`boolean` o `null`	`null`	Il massimo dei valori delle variabili specificate nell'intervallo di tempo corrente.
`sum`	`string` o `null`	`null`	La somma dei valori delle variabili specificate nell'intervallo di tempo corrente.
`recordVersion`	`long` o `null`	`null`	Il numero di versione del record. È possibile utilizzare il numero di versione per selezionare il record più recente. I record più recenti hanno numeri di versione più grandi.

Example Dati metrici nella fase fredda


```
{"seriesId":"f74c2828-5317-4df3-
ba16-6d41b5bcb531","timeInSeconds":1637334060,"offsetInNanos":0,"quality":"GOOD","resolution":"
{"double":16.0},"min":{"double":1.0},"max":{"double":31.0},"sum":
{"double":496.0},"recordVersion":null}
  {"seriesId":"f74c2828-5317-4df3-
ba16-6d41b5bcb531","timeInSeconds":1637334120,"offsetInNanos":0,"quality":"GOOD","resolution":"
{"double":46.0},"min":{"double":32.0},"max":{"double":60.0},"sum":
{"double":1334.0},"recordVersion":null}
  {"seriesId":"f74c2828-5317-4df3-
ba16-6d41b5bcb531","timeInSeconds":1637334540,"offsetInNanos":0,"quality":"GOOD","resolution":"
{"double":16.0},"min":{"double":1.0},"max":{"double":31.0},"sum":
{"double":496.0},"recordVersion":null}
  {"seriesId":"f74c2828-5317-4df3-
ba16-6d41b5bcb531","timeInSeconds":1637334600,"offsetInNanos":0,"quality":"GOOD","resolution":"
{"double":46.0},"min":{"double":32.0},"max":{"double":60.0},"sum":
{"double":1334.0},"recordVersion":null}
  {"seriesId":"f74c2828-5317-4df3-
ba16-6d41b5bcb531","timeInSeconds":1637335020,"offsetInNanos":0,"quality":"GOOD","resolution":"
{"double":16.0},"min":{"double":1.0},"max":{"double":31.0},"sum":
{"double":496.0},"recordVersion":null}
```


Metadati delle risorse

Quando abiliti AWS IoT SiteWise l'esportazione dei dati nel livello freddo per la prima volta, i metadati degli asset vengono esportati nel livello freddo. Dopo la configurazione iniziale, AWS IoT SiteWise esporta i metadati degli asset nel livello solo quando modificate le definizioni dei modelli di asset o le definizioni degli asset. I metadati delle risorse vengono salvati nel livello freddo nel formato JSON () delimitato da nuova riga. `.ndjson`

Percorso del file

AWS IoT SiteWise archivia i metadati delle risorse nel livello freddo utilizzando il seguente modello.

```
{keyPrefix}/asset_metadata/asset_{assetId}.ndjson
```

Ogni percorso di file verso i metadati delle risorse nel livello freddo contiene i seguenti componenti.

Componente del percorso	Descrizione
`keyPrefix`	Il prefisso Amazon S3 che hai specificato nella configurazione di storage AWS IoT SiteWise s. Amazon S3 utilizza il prefisso come nome di cartella nel bucket.
`asset_metadata`	La cartella in cui sono archiviati i metadati delle risorse. La `asset_metadata` cartella viene salvata nella cartella dei prefissi.
`fileName`	Il nome del file utilizza il carattere di sottoline atura (_) come delimitatore per separare quanto segue: • Il prefisso. `asset` • Il `assetId` valore. Il file viene salvato nel `.ndjson` formato.

Example percorso del file ai metadati delle risorse nel livello più freddo

```
keyPrefix/asset_metadata/asset_35901915-d476-4dca-8637-d9ed4df939ed.ndjson
```

Campi

Lo schema dei metadati delle risorse che viene esportato nel livello freddo contiene i seguenti campi.

Nome campo	Descrizione
`assetId`	L'ID dell'asset .
`assetName`	Il nome della risorsa.
`assetExternalId`	L'ID esterno della risorsa.
`assetModelId`	L'ID del modello di asset utilizzato per creare questa risorsa.

Nome campo	Descrizione
`assetModelName`	Il nome del modello di asset.
`assetModelExternalId`	L'ID esterno del modello di asset.
`assetPropertyId`	L'ID della proprietà dell'asset.
`assetPropertyName`	Il nome della proprietà dell'asset.
`assetPropertyExternalId`	L'ID esterno della proprietà dell'asset.
`assetPropertyDataType`	Il tipo di dati della proprietà dell'asset.
`assetPropertyUnit`	L'unità della proprietà dell'asset (ad esempio, `Newtons` e`RPM`).
`assetPropertyAlias`	L'alias che identifica la proprietà dell'asset, ad esempio il percorso del flusso di dati del server OPC-UA (ad esempio,). `/company/windfarm/3/turbine/7/temperature`
`timeSeriesId`	L'ID che identifica i dati delle serie temporali provenienti da apparecchiature, metriche o trasformazioni. È possibile utilizzare questo campo per unire dati non elaborati e metadati delle risorse nelle query.

Nome campo	Descrizione
`timeSeriesBucket`	Un numero esadecimale compreso tra 00 e ff. Questo numero è derivato da. `timeSeriesId` Questa partizione viene utilizzata per aumentare la velocità effettiva durante le operazioni di AWS IoT SiteWise scrittura sul livello freddo. Quando usi Amazon Athena per eseguire query, puoi utilizzare la partizione per il partizionamento fine per migliorare le prestazioni delle query. `timeSeriesBucket` e `seriesBucket` nel percorso del file i dati grezzi sono presenti gli stessi numeri.
`assetCompositeModelId`	L'ID del modello composito.
`assetCompositeModelExternalId`	L'ID esterno del modello composito.
`assetCompositeModelDescription`	La descrizione del modello composito.
`assetCompositeModelName`	Il nome del modello composito.
`assetCompositeModelType`	Il tipo del modello composito. Per i modelli compositi di allarme, questo tipo è `AWS/ALARM` .
`assetCreationDate`	La data di creazione della risorsa, nell'epoca di Unix.
`assetLastUpdateDate`	La data dell'ultimo aggiornamento della risorsa, espressa in Unix Epoch Time.
`assetStatusErrorCode`	Il codice di errore.
`assetStatusErrorMessage`	Messaggio di errore.
`assetStatusState`	Lo stato attuale della risorsa.

Example metadati degli asset nella fase fredda


```
  {"assetId":"7020c8e2-e6db-40fa-9845-
ed0dddd4c77d","assetExternalId":null,"assetName":"Wind Turbine Asset
 2","assetModelId":"ec1d924f-f07d-444f-b072-
e2994c165d35","assetModelExternalId":null,"assetModelName":"Wind
 Turbine Asset Model","assetPropertyId":"95e63da7-d34e-43e1-
bc6f-1b490154b07a","assetPropertyExternalId":null,"assetPropertyName":"Temperature","assetPrope
Washington/Seattle/WT2/temp","timeSeriesId":"7020c8e2-e6db-40fa-9845-
ed0dddd4c77d_95e63da7-d34e-43e1-
bc6f-1b490154b07a","timeSeriesBucket":"f6","assetArn":null,"assetCompositeModelDescription":nul
  {"assetId":"7020c8e2-e6db-40fa-9845-
ed0dddd4c77d","assetExternalId":null,"assetName":"Wind Turbine Asset
 2","assetModelId":"ec1d924f-f07d-444f-b072-
e2994c165d35","assetModelExternalId":null,"assetModelName":"Wind Turbine Asset
 Model","assetPropertyId":"c706d54d-4c11-42dc-9a01-63662fc697b4","assetPropertyExternalId":null
Washington/Seattle/WT2/pressure","timeSeriesId":"7020c8e2-e6db-40fa-9845-
ed0dddd4c77d_c706d54d-4c11-42dc-9a01-63662fc697b4","timeSeriesBucket":"1e","assetArn":null,"ass
  {"assetId":"7020c8e2-e6db-40fa-9845-
ed0dddd4c77d","assetExternalId":null,"assetName":"Wind Turbine Asset
 2","assetModelId":"ec1d924f-f07d-444f-b072-
e2994c165d35","assetModelExternalId":null,"assetModelName":"Wind
 Turbine Asset Model","assetPropertyId":"8cf1162f-dead-4fbe-b468-
c8e24cde9f50","assetPropertyExternalId":null,"assetPropertyName":"Max
 Temperature","assetPropertyDataType":"DOUBLE","assetPropertyUnit":null,"assetPropertyAlias":nu
e6db-40fa-9845-ed0dddd4c77d_8cf1162f-dead-4fbe-b468-
c8e24cde9f50","timeSeriesBucket":"d7","assetArn":null,"assetCompositeModelDescription":null,"as

 {"assetId":"3a5f2a22-3b37-4332-9c1c-404ea1d73fab","assetExternalId":null,"assetName":"BatchAss
ebc75e75e827","assetModelExternalId":null,"assetModelName":"FlashTestAssetModelDouble","assetPr
b410-
ab401a9176ed","assetPropertyExternalId":null,"assetPropertyName":"measurementProperty","assetPr
ae89-
ff316f5ff8aa","timeSeriesBucket":"af","assetArn":null,"assetCompositeModelDescription":null,"as
```


metadati della gerarchia degli asset

Quando AWS IoT SiteWise abiliti il salvataggio dei dati nel livello freddo per la prima volta, i metadati della gerarchia degli asset vengono esportati nel livello freddo. Dopo la configurazione iniziale, AWS IoT SiteWise esporta i metadati della gerarchia degli asset nel livello freddo solo quando si apportano

modifiche al modello degli asset o alle definizioni degli asset. I metadati della gerarchia degli asset vengono salvati nel livello freddo nel formato JSON () delimitato da nuova riga. `.ndjson`

Un identificatore esterno per la gerarchia, la risorsa di destinazione o la risorsa di origine viene recuperato chiamando l'API. DescribeAsset

Percorso del file

AWS IoT SiteWise archivia i metadati della gerarchia degli asset nel livello freddo utilizzando il seguente modello.

```
{keyPrefix}/asset_hierarchy_metadata/{parentAssetId}_{hierarchyId}.ndjson
```

Ogni percorso di file verso i metadati della gerarchia degli asset nel livello freddo contiene i seguenti componenti.

Componente del percorso	Descrizione
`keyPrefix`	Il prefisso Amazon S3 che hai specificato nella configurazione dello AWS IoT SiteWise storage. Amazon S3 utilizza il prefisso come nome di cartella nel bucket.
`asset_hierarchy_metadata`	La cartella che memorizza i metadati della gerarchia degli asset. La `asset_hierarchy_metadata` cartella viene salvata nella cartella dei prefissi.
`fileName`	Il nome del file utilizza il carattere di sottolineatura (_) come delimitatore per separare quanto segue: • Il valore. `parentAssetId` • Il `hierarchyId` valore. Il file viene salvato nel `.ndjson` formato.

Example percorso del file ai metadati della gerarchia degli asset nel livello freddo

```
keyPrefix/asset_hierarchy_metadata/35901915-d476-4dca-8637-
d9ed4df939ed_c5b3ced8-589a-48c7-9998-cdccfc9747a0.ndjson
```

Campi

Lo schema dei metadati della gerarchia degli asset che viene esportato nel livello freddo contiene i seguenti campi.

Nome campo	Descrizione
`sourceAssetId`	L'ID della risorsa di origine in questa relazione tra asset.
`targetAssetId`	L'ID della risorsa di destinazione in questa relazione tra asset.
`hierarchyId`	L'ID della gerarchia.
`associationType`	Il tipo di associazione di questa relazione tra asset. Il valore deve essere`CHILD`. La risorsa di destinazione è una risorsa secondaria della risorsa di origine.

Example metadati della gerarchia degli asset nel livello freddo

```
{"sourceAssetId":"80388e72-2284-44fb-9c89-
bfbaf0dfedd2","targetAssetId":"2b866c25-0c74-4750-bdf5-
b73683c8a2a2","hierarchyId":"bbed9f59-0412-4585-
a61d-6044db526aee","associationType":"CHILD"}
  {"sourceAssetId":"80388e72-2284-44fb-9c89-
bfbaf0dfedd2","targetAssetId":"6b51246e-984d-460d-
bc0b-470ea47d1e31","hierarchyId":"bbed9f59-0412-4585-
a61d-6044db526aee","associationType":"CHILD"}
```

Per visualizzare i dati nella fase fredda

1. Accedi alla console Amazon S3.
2. Nel pannello di navigazione, scegli Bucket, quindi scegli il tuo bucket Amazon S3.
3. Passa alla cartella che contiene i dati grezzi, i metadati degli asset o i metadati della gerarchia degli asset.
4. Seleziona i file, quindi da Azioni scegli Scarica.

File di indice dei dati di archiviazione

AWS IoT SiteWise utilizza questi file per ottimizzare le prestazioni delle query di dati. Vengono visualizzati nel bucket Amazon S3, ma non è necessario utilizzarli.

Percorso del file

AWS IoT SiteWise archivia i file di indice dei dati nella fase fredda utilizzando il seguente modello.

```
keyPrefix/index/series=timeseriesId/startYear=startYear/startMonth=startMonth/
startDay=startDay/index_timeseriesId_startTimestamp_quality
```

Example percorso del file del file di indice di archiviazione dei dati

```
keyPrefix/index/series=7020c8e2-e6db-40fa-9845-ed0dddd4c77d_95e63da7-
d34e-43e1-bc6f-1b490154b07a/startYear=2022/startMonth=02/startDay=03/
index_7020c8e2-e6db-40fa-9845-ed0dddd4c77d_95e63da7-d34e-43e1-
bc6f-1b490154b07a_1643846400_GOOD
```

Sicurezza in AWS IoT SiteWise

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. Per maggiori informazioni sui programmi di conformità applicabili a AWS IoT SiteWise, consulta la sezione AWS Servizi rientranti nell'ambito dei programmi di conformità, .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo AWS IoT SiteWise. I seguenti argomenti mostrano come eseguire la configurazione AWS IoT SiteWise per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche a utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere AWS IoT SiteWise le tue risorse.

Argomenti

Protezione dei dati in AWS IoT SiteWise

Il modello di responsabilità AWS condivisa modello di di si applica alla protezione dei dati in AWS IoT SiteWise. 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. Questi contenuti includono la configurazione della protezione e le attività di gestione per i servizi 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 o Servizi AWS utilizzi la console, l'API AWS IoT SiteWise 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.

Argomenti

Riservatezza del traffico Internet

Le connessioni tra AWS IoT SiteWise applicazioni locali, come i gateway SiteWise Edge, sono protette tramite connessioni Transport Layer Security (TLS). Per ulteriori informazioni, consulta Crittografia in transito.

AWS IoT SiteWise non supporta connessioni tra zone di disponibilità all'interno di una AWS regione o connessioni tra account. AWS

Puoi configurare IAM Identity Center in una sola regione alla volta. SiteWise Monitor si connette alla regione che hai configurato per IAM Identity Center. Ciò significa che utilizzi una regione per l'accesso a IAM Identity Center, ma puoi creare portali in qualsiasi regione.

Crittografia dei dati

La crittografia dei dati si riferisce alla protezione dei dati durante il transito (mentre viaggiano da AWS IoT SiteWise e verso e tra gateway SiteWise Edge e server) e quando sono inattivi (mentre sono archiviati su dispositivi locali o in AWS servizi). Puoi proteggere i dati in transito utilizzando Transport Layer Security (TLS) o i dati inattivi utilizzando la crittografia lato client.

> **Note**
>
> AWS IoT SiteWise L'elaborazione edge espone le API ospitate all'interno dei gateway SiteWise Edge e accessibili tramite la rete locale. Queste API sono esposte tramite una connessione TLS supportata da un certificato server di proprietà del connettore Edge. AWS IoT SiteWise Per l'autenticazione del client, queste API utilizzano una password di controllo degli accessi. La chiave privata del certificato del server e la password di controllo degli accessi sono entrambe archiviate su disco. AWS IoT SiteWise l'elaborazione perimetrale si basa sulla crittografia del file system per la sicurezza di queste credenziali archiviate.

Per ulteriori informazioni sulla crittografia lato server e la crittografia lato client, esamina gli argomenti elencati di seguito.

Argomenti

Crittografia a riposo

AWS IoT SiteWise archivia i tuoi dati nel AWS cloud e sui gateway AWS IoT SiteWise Edge.

Dati inattivi nel cloud AWS

AWS IoT SiteWise archivia i dati in altri AWS servizi che crittografano i dati inattivi per impostazione predefinita. Encryption at rest si integra con AWS Key Management Service (AWS KMS) per la gestione della chiave di crittografia utilizzata per crittografare i valori delle proprietà degli asset e i valori aggregati. AWS IoT SiteWise Puoi scegliere di utilizzare una chiave gestita dal cliente per crittografare i valori delle proprietà degli asset e aggregarli. AWS IoT SiteWise Puoi creare, gestire e visualizzare la tua chiave di crittografia tramite. AWS KMS

Puoi scegliere di Chiave di proprietà di AWS crittografare i tuoi dati o scegliere una chiave gestita dal cliente per crittografare i valori delle proprietà degli asset e i valori aggregati:

Come funziona

Encryption at rest si integra con la gestione della chiave di crittografia utilizzata AWS KMS per crittografare i dati.

- Chiave di proprietà di AWS — Chiave di crittografia predefinita. AWS IoT SiteWise possiede questa chiave. Non puoi visualizzare questa chiave nel tuo AWS account. Inoltre, non puoi visualizzare le operazioni sulla chiave nei AWS CloudTrail registri. È possibile utilizzare questa chiave senza costi aggiuntivi.
- Chiave gestita dal cliente: la chiave viene memorizzata nel tuo account, che crei, possiedi e gestisci. Hai il pieno controllo sulla chiave KMS. AWS KMS Si applicano costi aggiuntivi.

Chiavi di proprietà di AWS

Chiavi di proprietà di AWS non sono archiviate nel tuo account. Fanno parte di una raccolta di chiavi KMS che AWS possiede e gestisce per l'utilizzo in più AWS account. AWS i servizi possono essere utilizzati Chiavi di proprietà di AWS per proteggere i tuoi dati.

Non puoi visualizzarne, gestirne Chiavi di proprietà di AWS, utilizzarne o controllarne l'utilizzo. Tuttavia, non è necessario eseguire alcuna operazione o modificare alcun programma per proteggere le chiavi che crittografano i dati.

Se li utilizzi, non ti viene addebitato alcun canone mensile o un canone di utilizzo Chiavi di proprietà di AWS e non vengono conteggiati nelle AWS KMS quote per il tuo account.

Chiavi gestite dal cliente

Le chiavi gestite dal cliente sono chiavi KMS nel tuo account create da te, di tua proprietà e gestite da te. Hai il pieno controllo su queste chiavi KMS, come le seguenti:

- Stabilire e mantenere le proprie politiche chiave, le politiche IAM e le sovvenzioni
- Abilitarli e disabilitarli
- Ruotando il loro materiale crittografico
- Aggiungere tag
- Creazione di alias che si riferiscono ad essi
- Pianificazione della loro eliminazione

Puoi anche utilizzare CloudTrail Amazon CloudWatch Logs per tenere traccia delle richieste AWS IoT SiteWise inviate a per tuo AWS KMS conto.

Se utilizzi chiavi gestite dai clienti, devi concedere AWS IoT SiteWise l'accesso alla chiave KMS memorizzata nel tuo account. AWS IoT SiteWise utilizza la crittografia a busta e la gerarchia delle chiavi per crittografare i dati. La chiave di AWS KMS crittografia viene utilizzata per crittografare la chiave principale di questa gerarchia di chiavi. Per ulteriori informazioni, consulta Crittografia envelope nella Guida per gli sviluppatori di AWS Key Management Service .

La seguente politica di esempio concede AWS IoT SiteWise le autorizzazioni per creare una chiave gestita dal cliente per conto dell'utente. Quando crei la tua chiave, devi consentire le azioni `kms:CreateGrant` e `kms:DescribeKey`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1603902045292",
      "Action": [
```

```
        "kms:CreateGrant",
        "kms:DescribeKey"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Il contesto di crittografia per la concessione creata utilizza il tuo ID `aws:iotsitewise:subscriberId` e quello dell'account.

Dati inattivi sui gateway SiteWise Edge

AWS IoT SiteWise i gateway archiviano i seguenti dati nel file system locale:

- Informazioni sulla configurazione dell'origine OPC-UA
- Il set di percorsi dei flussi di dati OPC-UA da origini OPC-UA collegate
- Dati industriali memorizzati nella cache quando il gateway SiteWise Edge perde la connessione a Internet

SiteWise I gateway Edge funzionano su. AWS IoT Greengrass AWS IoT Greengrass si affida alle autorizzazioni di file Unix e alla crittografia dell'intero disco (se abilitata) per proteggere i dati archiviati sul core. È tua responsabilità proteggere il file system e il dispositivo.

Tuttavia, AWS IoT Greengrass crittografa le copie locali dei segreti del server OPC-UA recuperati da Secrets Manager. Per ulteriori informazioni, consulta Secrets encryption nella Developer Guide.AWS IoT Greengrass Version 1

Per ulteriori informazioni sulla crittografia a riposo sui AWS IoT Greengrass core, consulta Encryption at rest nella AWS IoT Greengrass Version 1 Developer Guide.

Crittografia in transito

AWS IoT SiteWise dispone di tre modalità di comunicazione in cui i dati sono in transito:

- Tramite Internet: la comunicazione tra dispositivi locali (compresi i gateway SiteWise Edge) AWS IoT SiteWise è crittografata.
- Tramite la rete locale: la comunicazione tra OpsHub for SiteWise application e i gateway SiteWise Edge è sempre crittografata. La comunicazione tra l'applicazione di SiteWise monitoraggio in

esecuzione nel browser e i gateway SiteWise Edge è sempre crittografata. La comunicazione tra i gateway SiteWise Edge e le sorgenti OPC-UA può essere crittografata.

- Tra i componenti sui gateway SiteWise Edge: la comunicazione tra AWS IoT Greengrass i componenti sui gateway SiteWise Edge non è crittografata.

Argomenti

Dati in transito su Internet

AWS IoT SiteWise utilizza Transport Layer Security (TLS) per crittografare tutte le comunicazioni su Internet. Tutti i dati inviati al AWS Cloud vengono inviati tramite una connessione TLS utilizzando i protocolli MQTT o HTTPS, quindi sono sicuri per impostazione predefinita. SiteWise I gateway edge, che funzionano su AWS IoT Greengrass, e le notifiche sui valori delle proprietà utilizzano il modello di sicurezza del AWS IoT trasporto. Per ulteriori informazioni, consulta l'argomento relativo alla sicurezza del trasporto nella Guida per gli sviluppatori AWS IoT .

Dati in transito sulla rete locale

SiteWise Gli edge gateway seguono le specifiche OPC-UA per la comunicazione con le sorgenti OPC-UA locali. È tua responsabilità configurare le origini in modo da utilizzare una modalità di sicurezza dei messaggi che esegue la crittografia dei dati in transito.

Se si sceglie una modalità di sicurezza dei messaggi di firma, i dati in transito tra i gateway SiteWise Edge e le sorgenti vengono firmati ma non crittografati. Se si sceglie una modalità di sicurezza per la firma e la crittografia dei messaggi, i dati in transito tra i gateway SiteWise Edge e le fonti vengono firmati e crittografati. Per ulteriori informazioni sulla configurazione delle origini, consulta Configurazione delle origini dati.

La comunicazione tra l'applicazione della console Edge e i gateway SiteWise Edge è sempre crittografata tramite TLS. Il connettore SiteWise Edge sul gateway SiteWise Edge genera e archivia un certificato autofirmato per poter stabilire una connessione TLS con la console edge per l'applicazione. AWS IoT SiteWise È necessario copiare questo certificato dal gateway SiteWise Edge alla console edge per l' AWS IoT SiteWise applicazione prima di connettere l'applicazione al gateway

SiteWise Edge. Ciò garantisce che la console perimetrale AWS IoT SiteWise dell'applicazione sia in grado di verificare che sia connessa al gateway SiteWise Edge affidabile.

Oltre a TLS per la segretezza e l'autenticità del server, SiteWise Edge utilizza il protocollo SigV4 per stabilire l'autenticità dell'applicazione della console perimetrale. Il connettore SiteWise Edge sul gateway SiteWise Edge accetta e archivia una password per poter verificare le connessioni in entrata dall'applicazione della console edge, dall'applicazione SiteWise Monitor in esecuzione nei browser e da altri client basati sull'SDK. AWS IoT SiteWise

Per ulteriori informazioni sulla generazione della password e del certificato del server, consulta. the section called “Gestione dei gateway SiteWise Edge”

Dati in transito tra componenti locali sui gateway SiteWise Edge

SiteWise I gateway Edge funzionano su AWS IoT Greengrass, il che non crittografa i dati scambiati localmente sul AWS IoT Greengrass core perché i dati non escono dal dispositivo. Ciò include la comunicazione tra AWS IoT Greengrass componenti come il connettore. AWS IoT SiteWise Per ulteriori informazioni, consulta Data on the core device nella AWS IoT Greengrass Version 1 Developer Guide.

Gestione delle chiavi

AWS IoT SiteWise gestione delle chiavi nel cloud

Per impostazione predefinita, AWS IoT SiteWise vengono utilizzati Chiavi gestite da AWS per proteggere i dati nel AWS cloud. Puoi aggiornare le impostazioni per utilizzare una chiave gestita dal cliente per crittografare alcuni dati. AWS IoT SiteWiseÈ possibile creare, gestire e visualizzare la chiave di crittografia tramite AWS Key Management Service (AWS KMS).

AWS IoT SiteWise supporta la crittografia lato server con chiavi gestite dal cliente archiviate AWS KMS per crittografare i seguenti dati:

- valori delle proprietà degli asset
- Valori aggregati

> **Note**
>
> Altri dati e risorse vengono crittografati utilizzando la crittografia predefinita con chiavi gestite da AWS IoT SiteWise. Questa chiave è memorizzata nell' AWS IoT SiteWise account.

Per ulteriori informazioni, vedi Cos'è AWS Key Management Service? nella Guida per gli AWS Key Management Service sviluppatori.

Abilita la crittografia utilizzando chiavi gestite dal cliente

Per utilizzare le chiavi gestite dal cliente con AWS IoT SiteWise, devi aggiornare AWS IoT SiteWise le impostazioni.

Per abilitare la crittografia utilizzando le chiavi KMS

1. Passare alla console AWS IoT SiteWise.
2. Scegli Impostazioni account e scegli Modifica per aprire la pagina Modifica impostazioni account.
3. Per Tipo di chiave di crittografia, scegli Scegli una AWS KMS chiave diversa. Ciò consente la crittografia con chiavi gestite dal cliente archiviate in AWS KMS.

   > **Note**
   >
   > Attualmente, è possibile utilizzare la crittografia a chiave gestita dal cliente solo per i valori delle proprietà degli asset e i valori aggregati.

4. Scegli la tua chiave KMS con una delle seguenti opzioni:

   - Per utilizzare una chiave KMS esistente: scegli l'alias della tua chiave KMS dall'elenco.
   - Per creare una nuova chiave KMS, scegli Crea una chiave. AWS KMS

   > **Note**
   >
   > In questo modo si apre AWS KMS Pannello di controllo. Per ulteriori informazioni sulla creazione di una chiave KMS, consulta Creating keys nella AWS Key Management Service Developer Guide.

5. Scegli Salva per aggiornare le impostazioni.

SiteWise Gestione delle chiavi del gateway Edge

SiteWise I gateway edge funzionano su AWS IoT Greengrass e i dispositivi AWS IoT Greengrass principali utilizzano chiavi pubbliche e private per autenticarsi con il AWS cloud e crittografare i

segreti locali, come i segreti di autenticazione OPC-UA. Per ulteriori informazioni, consulta Gestione delle chiavi nella Guida per gli sviluppatori.AWS IoT Greengrass Version 1

Gestione delle identità e degli accessi per AWS IoT SiteWise

AWS Identity and Access Management (IAM) è un software Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse. AWS IoT SiteWise IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro che AWS IoT SiteWise svolgi.

Utente del servizio: se utilizzi il AWS IoT SiteWise servizio per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più AWS IoT SiteWise funzionalità per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di AWS IoT SiteWise, consulta Risoluzione dei problemi relativi AWS IoT SiteWise all'identità e all'accesso.

Amministratore del servizio: se sei responsabile delle AWS IoT SiteWise risorse della tua azienda, probabilmente hai pieno accesso a AWS IoT SiteWise. È tuo compito determinare a quali AWS

IoT SiteWise funzionalità e risorse devono accedere gli utenti del servizio. 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 saperne di più su come la tua azienda può utilizzare IAM con AWS IoT SiteWise, consultaCome AWS IoT SiteWise funziona con IAM.

Amministratore IAM: un amministratore IAM potrebbe essere interessato a ottenere dei dettagli su come scrivere policy per gestire l'accesso a AWS IoT SiteWise. Per visualizzare esempi di policy AWS IoT SiteWise basate sull'identità che puoi utilizzare in IAM, consulta. AWS IoT SiteWise esempi di politiche basate sull'identità

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.

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'operazione 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.

Come AWS IoT SiteWise funziona con IAM

Prima di utilizzare AWS Identity and Access Management (IAM) per gestire l'accesso a AWS IoT SiteWise, è necessario comprendere con quali funzionalità IAM è possibile utilizzare AWS IoT SiteWise.

Funzionalità IAM	Supporto da AWS IoT SiteWis
Policy basate sull'identità con autorizzazioni a livello di risorse	Sì

Funzionalità IAM	Supporto da AWS IoT SiteWise
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì
Policy basate su risorse	No
Liste di controllo degli accessi (ACL)	No
Autorizzazione basata su tag (ABAC)	Sì
Credenziali temporanee	Sì
Sessioni di accesso diretto (FAS)	Sì
Ruoli collegati al servizio	Sì
Ruoli di servizio	Sì

Per avere una visione di alto livello di come AWS IoT SiteWise e altri AWS servizi funzionano con IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Indice

- Autorizzazione basata su tag AWS IoT SiteWise
- AWS IoT SiteWise politiche basate sull'identità
  - Operazioni di policy
    - BatchPutAssetPropertyValue autorizzazione
  - Risorse relative alle policy
  - Chiavi di condizione delle policy
  - Esempi
- AWS IoT SiteWise esempi di politiche basate sull'identità
  - Best practice delle policy
  - Utilizzo della console di AWS IoT SiteWise
  - Consentire agli utenti di visualizzare le loro autorizzazioni
  - Consentire agli utenti di inserire i dati negli asset in un'unica gerarchia
  - Visualizzazione di asset AWS IoT SiteWise in base ai tag
- Gestione dell'accesso con policy
  - Policy basate su identità
  - Policy basate su risorse
  - Liste di controllo degli accessi (ACL)
  - Altri tipi di policy
  - Più tipi di policy

AWS IoT SiteWise Ruoli IAM

Un ruolo IAM è un'entità all'interno dell' Account AWS che dispone di autorizzazioni specifiche.

Utilizzo di credenziali temporanee con AWS IoT SiteWise

È possibile utilizzare credenziali temporanee per effettuare l'accesso con la federazione, assumere un ruolo IAM o un ruolo multi-account. È possibile ottenere credenziali di sicurezza temporanee chiamando operazioni AWS STS API come AssumeRoleo. GetFederationToken

AWS IoT SiteWise supporta l'utilizzo di credenziali temporanee.

SiteWise Monitor supporta gli utenti federati per accedere ai portali. Gli utenti del portale si autenticano con le proprie credenziali IAM Identity Center o IAM.

> **Important**
>
> Gli utenti o i ruoli devono disporre dell'`iotsitewise:DescribePortal`autorizzazione per accedere al portale.

Quando un utente accede a un portale, SiteWise Monitor genera una politica di sessione che fornisce le seguenti autorizzazioni:

- Accesso in sola lettura alle risorse e ai dati delle risorse presenti AWS IoT SiteWise nel tuo account a cui il ruolo del portale fornisce l'accesso.
- Accesso ai progetti in tale portale per il quale l'utente dispone dell'accesso amministratore (proprietario del progetto) o di sola lettura (visualizzatore progetto).

Per ulteriori informazioni sulle autorizzazioni utente del portale federato, consulta Utilizzo dei ruoli di servizio per AWS IoT SiteWise Monitor.

Sessioni di accesso diretto (FAS) per AWS IoT SiteWise

Supporta sessioni di accesso diretto (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'operazione 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 collegati ai servizi

I ruoli collegati ai AWS servizi consentono ai servizi di accedere alle risorse di altri servizi per completare un'azione per conto dell'utente. I ruoli collegati ai servizi sono visualizzati nell'account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non può modificarle.

AWS IoT SiteWise supporta ruoli collegati ai servizi. Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi AWS IoT SiteWise , consulta Utilizzo di ruoli collegati ai servizi per AWS IoT SiteWise.

Ruoli dei servizi

Questa caratteristica consente a un servizio di assumere un ruolo di servizio per conto dell'utente. Questo ruolo consente al servizio di accedere alle risorse in altri servizi per completare un'azione per conto dell'utente. I ruoli di servizio vengono visualizzati nell'utente Account AWS e sono di proprietà dell'account. Ciò significa che un amministratore IAM può modificare le autorizzazioni per questo ruolo. Tuttavia, questo potrebbe pregiudicare la funzionalità del servizio.

AWS IoT SiteWise utilizza un ruolo di servizio per consentire agli utenti del portale SiteWise Monitor di accedere ad alcune AWS IoT SiteWise risorse per conto dell'utente. Per ulteriori informazioni, consulta Utilizzo dei ruoli di servizio per AWS IoT SiteWise Monitor.

È necessario disporre delle autorizzazioni necessarie prima di poter creare modelli di AWS IoT Events allarme in AWS IoT SiteWise. Per ulteriori informazioni, consulta Configurazione delle autorizzazioni per gli AWS IoT Events allarmi.

Scelta di un ruolo IAM in AWS IoT SiteWise

Quando crei una `portal` risorsa in AWS IoT SiteWise, devi scegliere un ruolo per consentire agli utenti federati del tuo portale SiteWise Monitor di accedere per tuo AWS IoT SiteWise conto. Se in precedenza hai creato un ruolo di servizio, ti AWS IoT SiteWise fornisce un elenco di ruoli tra cui scegliere. In caso contrario, puoi creare un ruolo con le autorizzazioni richieste quando crei un portale. È importante scegliere un ruolo che consenta l'accesso agli asset e ai dati degli asset. Per ulteriori informazioni, consulta Utilizzo dei ruoli di servizio per AWS IoT SiteWise Monitor.

Autorizzazione basata su tag AWS IoT SiteWise

È possibile allegare tag alle AWS IoT SiteWise risorse o passarli in una richiesta a AWS IoT SiteWise. 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`. Per ulteriori informazioni sul tagging delle risorse di AWS IoT SiteWise , consulta Taggare le tue risorse AWS IoT SiteWise.

Per visualizzare una policy basata sulle identità di esempio per limitare l'accesso a una risorsa basata su tag su tale risorsa, consulta Visualizzazione di asset AWS IoT SiteWise in base ai tag.

AWS IoT SiteWise politiche basate sull'identità

Le policy IAM ti consentono di controllare chi può fare cosa. AWS IoT SiteWise Puoi decidere quali azioni sono consentite o meno e impostare condizioni specifiche per tali azioni. Ad esempio, puoi stabilire delle regole su chi può visualizzare o modificare le informazioni AWS IoT SiteWise. AWS IoT SiteWise supporta azioni, risorse e chiavi di condizione specifiche. Per informazioni su tutti gli elementi utilizzati in una policy JSON, consulta Documentazione di riferimento degli elementi delle policy JSON IAM nella Guida per l'utente IAM.

Operazioni di policy

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.

Le azioni politiche AWS IoT SiteWise utilizzano il seguente prefisso prima dell'azione:`iotsitewise:`. Ad esempio, per concedere a qualcuno il permesso di caricare i dati delle proprietà degli asset AWS IoT SiteWise con l'operazione `BatchPutAssetPropertyValue` API, includi l'`iotsitewise:BatchPutAssetPropertyValue`azione nella sua politica. Le dichiarazioni politiche devono includere un `NotAction` elemento `Action` or. AWS IoT SiteWise definisce il proprio set di azioni che descrivono le attività che è possibile eseguire con questo servizio.

Per specificare più operazioni in una singola istruzione, separarle con una virgola come mostrato di seguito.

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

Puoi specificare più operazioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le operazioni che iniziano con la parola `Describe`, includi la seguente operazione.

```
"Action": "iotsitewise:Describe*"
```

Per visualizzare un elenco di AWS IoT SiteWise azioni, consulta Actions Defined by AWS IoT SiteWise nella IAM User Guide.

BatchPutAssetPropertyValue autorizzazione

AWS IoT SiteWise autorizza l'accesso all'BatchPutAssetPropertyValueazione in un modo insolito. Per la maggior parte delle azioni, quando consenti o neghi l'accesso, tale azione restituisce un errore se le autorizzazioni non vengono concesse. Con`BatchPutAssetPropertyValue`, puoi inviare più immissioni di dati a diverse risorse e proprietà delle risorse in un'unica richiesta API. AWS IoT SiteWise autorizza ogni immissione di dati in modo indipendente. Per ogni singola immissione non autorizzata nella richiesta, AWS IoT SiteWise include un errore `AccessDeniedException` nell'elenco restituito. AWS IoT SiteWise riceve i dati relativi a qualsiasi immissione autorizzata e che ha esito positivo, anche se un'altra immissione nella stessa richiesta ha esito negativo.

> **Important**
>
> Prima di importare dati in un flusso di dati, procedi come segue:
>
> - Autorizzate la `time-series` risorsa se utilizzate un alias di proprietà per identificare il flusso di dati.
> - Autorizzate la `asset` risorsa se utilizzate un ID di risorsa per identificare la risorsa che contiene la proprietà della risorsa associata.

Risorse relative alle policy

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": "*"
```

Ogni dichiarazione di policy IAM si applica alle risorse specificate utilizzando i relativi ARN. Di seguito è riportata la sintassi generale di un ARN.

```
arn:${Partition}:${Service}:${Region}:${Account}:${ResourceType}/${ResourcePath}
```

Per ulteriori informazioni sul formato degli ARN, consulta Amazon Resource Names (ARNs) e AWS service namespace.

Ad esempio, per specificare l'asset con ID `a1b2c3d4-5678-90ab-cdef-22222EXAMPLE` nell'istruzione, utilizza il seguente ARN.

```
"Resource": "arn:aws:iotsitewise:region:123456789012:asset/a1b2c3d4-5678-90ab-
cdef-22222EXAMPLE"
```

Per specificare tutti i flussi di dati che appartengono a un account specifico, usa il carattere jolly (*):

```
"Resource": "arn:aws:iotsitewise:region:123456789012:time-series/*"
```

Per specificare tutti gli asset che appartengono a un account specifico, utilizza il carattere jolly (*):

```
"Resource": "arn:aws:iotsitewise:region:123456789012:asset/*"
```

Alcune AWS IoT SiteWise azioni, come quelle per la creazione di risorse, non possono essere eseguite su una risorsa specifica. In questi casi, è necessario utilizzare il carattere jolly (*).

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

Per specificare più risorse in una singola istruzione, separa gli ARN con le virgole.

```
"Resource": [
  "resource1",
  "resource2"
]
```

Per visualizzare un elenco dei tipi di AWS IoT SiteWise risorse e dei relativi ARN, consulta Resources Defined by AWS IoT SiteWise nella IAM User Guide. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta Operazioni definite da AWS IoT SiteWise.

Chiavi di condizione delle policy

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.

> **Important**
>
> Molte chiavi di condizione sono specifiche di una risorsa e alcune operazioni API utilizzano più risorse. Se scrivi una dichiarazione di policy con una chiave di condizione, utilizza l'elemento `Resource` della dichiarazione per specificare la risorsa a cui viene applicata la chiave di condizione. In caso contrario, la policy potrebbe impedire agli utenti di eseguire operazioni perché il controllo della condizione ha esito negativo per le risorse alle quali non viene applicata la chiave di condizione. Se non desideri specificare una risorsa oppure se hai scritto l'elemento `Action` della policy in modo da includere più operazioni API, devi utilizzare il tipo di condizione `...IfExists` per assicurarti che la chiave di condizione venga ignorata

per le risorse che non la utilizzano. Per ulteriori informazioni, consulta... IfExists condizioni nella Guida per l'utente IAM.

AWS IoT SiteWise definisce il proprio set di chiavi di condizione e supporta anche l'utilizzo di alcune chiavi di condizione globali. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

AWS IoT SiteWise chiavi di condizione

Chiave di condizione	Descrizione	Tipi
`iotsitewise:isAssociatedWithAssetProperty`	Se i flussi di dati sono associati a una proprietà dell'asset. Utilizzate questa chiave di condizione per definire le autorizzazioni in base all'esistenza di una proprietà di asset associata per i flussi di dati. Valore di esempio: `true`	Stringa
`iotsitewise:assetHierarchyPath`	Il percorso della gerarchia dell'asset, ovvero una stringa di ID asset separati da una barra. Utilizzare questa chiave di condizione per definire le autorizzazioni in base a un sottoinsieme della gerarchia di tutti gli asset nell'account. Valore di esempio: `/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE/a1b2c3d4-5678-90ab-cdef-66666EXAMPLE`	Stringa

Chiave di condizione	Descrizione	Tipi
`iotsitewise:propertyId`	L'ID di una proprietà di asset. Utilizza questa chiave di condizione per definire le autorizzazioni in base a una proprietà specificata di un modello di asset. Questa chiave di condizione si applica a tutti gli asset di tale modello. Valore di esempio: `a1b2c3d4-5678-90ab-cdef-33333EXAMPLE`	Stringa
`iotsitewise:childAssetId`	L'ID di un asset associato come un figlio a un altro asset. Utilizza questa chiave di condizione per definire le autorizzazioni in base agli asset figlio. Per definire le autorizzazioni in base agli asset padre, utilizza la sezione delle risorse di un'istruzione policy. Valore di esempio: `a1b2c3d4-5678-90ab-cdef-66666EXAMPLE`	Stringa

Chiave di condizione	Descrizione	Tipi
`iotsitewise:iam`	L'ARN di un'identità IAM quando si elencano le politiche di accesso. Utilizza questa chiave di condizione per definire le autorizzazioni delle politiche di accesso per un'identità IAM. Valore di esempio: `arn:aws:iam::123456789012:user/JohnDoe`	Stringa, Null
`iotsitewise:propertyAlias`	L'alias che identifica una proprietà o un flusso di dati di una risorsa. Utilizzate questa chiave di condizione per definire le autorizzazioni in base all'alias.	Stringa
`iotsitewise:user`	L'ID di un utente di IAM Identity Center quando elenca le politiche di accesso. Utilizza questa chiave di condizione per definire le autorizzazioni delle policy di accesso per un utente IAM Identity Center. Valore di esempio: `a1b2c3d4e5-a1b2c3d4-5678-90ab-cdef-aaaaEXAMPLE`	Stringa, Null

Chiave di condizione	Descrizione	Tipi
`iotsitewise:group`	L'ID di un gruppo IAM Identity Center quando si elencano le politiche di accesso. Utilizza questa chiave di condizione per definire le autorizzazioni delle policy di accesso per un gruppo IAM Identity Center. Valore di esempio: `a1b2c3d4e5-a1b2c3d4-5678-90ab-cdef-bbbbbEXAMPLE`	Stringa, Null
`iotsitewise:portal`	ID di un portale in una policy di accesso. Utilizza questa chiave di condizione per definire le autorizzazioni delle policy di accesso in base a un portale. Valore di esempio: `a1b2c3d4-5678-90ab-cdef-77777EXAMPLE`	Stringa, Null

Chiave di condizione	Descrizione	Tipi
`iotsitewise:project`	L'ID di un progetto in una policy di accesso o l'ID di un progetto per un pannello di controllo. Utilizza questa chiave di condizione per definire il pannello di controllo o le autorizzazioni delle policy di accesso in base a un progetto. Valore di esempio: `a1b2c3d4-5678-90ab-cdef-88888EXAMPLE`	Stringa, Null

Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, consulta Azioni definite da AWS IoT SiteWise.

Esempi

Per visualizzare esempi di politiche AWS IoT SiteWise basate sull'identità, vedere. AWS IoT SiteWise esempi di politiche basate sull'identità

AWS IoT SiteWise esempi di politiche basate sull'identità

Per impostazione predefinita, le entità (utenti e ruoli) non sono autorizzate a creare o modificare AWS IoT SiteWise risorse. Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS l'API. Per modificare le autorizzazioni, un amministratore AWS Identity and Access Management (IAM) deve effettuare le seguenti operazioni:

1. Crea policy IAM che concedano a utenti e ruoli il permesso di eseguire operazioni API specifiche sulle risorse di cui hanno bisogno.
2. Allega tali policy agli utenti o ai gruppi che richiedono tali autorizzazioni.

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

Argomenti

- Best practice delle policy
- Utilizzo della console di AWS IoT SiteWise
- Consentire agli utenti di visualizzare le loro autorizzazioni
- Consentire agli utenti di inserire i dati negli asset in un'unica gerarchia
- Visualizzazione di asset AWS IoT SiteWise in base ai tag

Best practice delle policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare AWS IoT SiteWise risorse nel tuo 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 politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS 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 funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso 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 di AWS IoT SiteWise

Per accedere alla AWS IoT SiteWise console, è necessario un set di autorizzazioni di base. Queste autorizzazioni consentono di visualizzare e gestire i dettagli sulle AWS IoT SiteWise risorse di. Account AWS

Se stabilisci una politica troppo restrittiva, la console potrebbe non funzionare come previsto per gli utenti o i ruoli (entità) con quella politica. Per garantire che tali entità possano ancora utilizzare la AWS IoT SiteWise console, allega loro la policy AWSIoTSiteWiseConsoleFullAccessgestita o definisci autorizzazioni equivalenti per tali entità. Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente IAM.

Se le entità utilizzano solo la AWS Command Line Interface (CLI) o l' AWS IoT SiteWise API e non la console, non necessitano di queste autorizzazioni minime. In tal caso, è sufficiente consentire loro di accedere alle azioni specifiche di cui hanno bisogno per le loro attività API.

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 l'API o a livello di codice. AWS CLI 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": "*"
        }
    ]
}
```

Consentire agli utenti di inserire i dati negli asset in un'unica gerarchia

In questo esempio, volete concedere a un utente del vostro account l' Account AWS accesso per scrivere dati su tutte le proprietà delle risorse in una gerarchia specifica di risorse, a partire dalla risorsa principale. `a1b2c3d4-5678-90ab-cdef-22222EXAMPLE` La policy concede l'autorizzazione `iotsitewise:BatchPutAssetPropertyValue` all'utente. Questa policy utilizza la chiave di condizione `iotsitewise:assetHierarchyPath` per limitare l'accesso agli asset il cui percorso della gerarchia corrisponde all'asset o ai relativi discendenti.

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

```
  "Statement": [
    {
      "Sid": "PutAssetPropertyValuesForHierarchy",
      "Effect": "Allow",
      "Action": "iotsitewise:BatchPutAssetPropertyValue",
      "Resource": "arn:aws:iotsitewise:*:*:asset/*",
      "Condition": {
        "StringLike": {
          "iotsitewise:assetHierarchyPath": [
            "/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
            "/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE/*"
          ]
        }
      }
    }
  ]
}
```

Visualizzazione di asset AWS IoT SiteWise in base ai tag

Utilizzate le condizioni nella vostra politica basata sull'identità per controllare l'accesso alle AWS IoT SiteWise risorse in base ai tag. Questo esempio mostra come creare una politica che consenta la visualizzazione delle risorse. Tuttavia, l'autorizzazione viene concessa solo se il valore del tag di asset `0wner` corrisponde al nome utente dell'utente. Questo criterio concede inoltre l'autorizzazione a completare questa azione sulla console.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAllAssets",
      "Effect": "Allow",
      "Action": [
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DescribeAssetIfOwner",
      "Effect": "Allow",
      "Action": "iotsitewise:DescribeAsset",
      "Resource": "arn:aws:iotsitewise:*:*:asset/*",
```

```
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Owner": "${aws:username}"
        }
      }
    }
  ]
}
```

Allega questa politica agli utenti del tuo account. Se un utente denominato `richard-roe` tenta di visualizzare una AWS IoT SiteWise risorsa, la risorsa deve essere contrassegnata con `0wner=richard-roe` o`owner=richard-roe`. In caso contrario, a Richard viene negato l'accesso. I nomi delle chiavi dei tag di condizione non fanno distinzione tra maiuscole e minuscole. Quindi, `0wner` corrisponde a entrambi `0wner` e. `owner` Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando politiche e allegandole 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.

AWS politiche gestite per AWS IoT SiteWise

Semplifica l'aggiunta di autorizzazioni a utenti, gruppi e ruoli utilizzando policy AWS gestite anziché scrivere policy da soli. Ci vogliono tempo ed esperienza per creare policy gestite dai clienti IAM che forniscano autorizzazioni precise al tuo team. Per una configurazione più rapida, prendi in considerazione l'utilizzo delle nostre policy AWS gestite per casi d'uso comuni. Trova le politiche

AWS gestite nel tuo Account AWS. Per ulteriori informazioni sulle policy gestite da AWS , consulta Policy gestite da AWS nella Guida per l'utente di IAM.

AWS i servizi si occupano dell'aggiornamento e della manutenzione delle politiche AWS gestite, il che significa che non è possibile modificare le autorizzazioni di queste politiche. Occasionalmente, AWS IoT SiteWise può aggiungere autorizzazioni per integrare nuove funzionalità, con un impatto su tutte le identità con la politica allegata. Tali aggiornamenti sono comuni con l'introduzione di nuovi servizi o funzionalità. Tuttavia, le autorizzazioni non vengono mai rimosse, garantendo che le impostazioni rimangano intatte.

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 un elenco con le descrizioni delle politiche relative alle funzioni lavorative, consulta le politiche AWS gestite per le funzioni lavorative nella Guida per l'utente IAM.

AWS politica gestita: AWSIoTSiteWiseReadOnlyAccess

Utilizza la policy `AWSIoTSiteWiseReadOnlyAccess` AWS gestita per consentire l'accesso in sola lettura a. AWS IoT SiteWise

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

Autorizzazioni a livello di servizio

Questa politica fornisce l'accesso in sola lettura a. AWS IoT SiteWise In questa policy non sono incluse altre autorizzazioni di servizio.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iotsitewise:Describe*",
                "iotsitewise:List*",
                "iotsitewise:BatchGet*",
                "iotsitewise:Get*"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

AWS politica gestita: AWSServiceRoleForIoTSiteWise

Il `AWSServiceRoleForIoTSiteWise` ruolo utilizza la `AWSServiceRoleForIoTSiteWise` politica con le seguenti autorizzazioni. Questa politica:

- Consente di AWS IoT SiteWise implementare gateway SiteWise Edge (che funzionano su`AWS IoT Greengrass`).
- Consente di eseguire AWS IoT SiteWise la registrazione.
- Consente di AWS IoT SiteWise eseguire una query di ricerca di metadati nel AWS IoT TwinMaker database.

Se utilizzi AWS IoT SiteWise un solo account utente, il `AWSServiceRoleForIoTSiteWise` ruolo crea la `AWSServiceRoleForIoTSiteWise` policy nel tuo account IAM e la associa ai ruoli collegati al `AWSServiceRoleForIoTSiteWise` servizio per. AWS IoT SiteWise

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AllowSiteWiseReadGreenGrass",
   "Effect": "Allow",
   "Action": [
    "greengrass:GetAssociatedRole",
    "greengrass:GetCoreDefinition",
    "greengrass:GetCoreDefinitionVersion",
    "greengrass:GetGroup",
    "greengrass:GetGroupVersion"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowSiteWiseAccessLogGroup",
   "Effect": "Allow",
   "Action": [
```

```
    "logs:CreateLogGroup",
    "logs:DescribeLogGroups"
   ],
   "Resource": "arn:aws:logs:*:*:log-group:/aws/iotsitewise*"
  },
  {
   "Sid": "AllowSiteWiseAccessLog",
   "Effect": "Allow",
   "Action": [
    "logs:CreateLogStream",
    "logs:DescribeLogStreams",
    "logs:PutLogEvents"
   ],
   "Resource": "arn:aws:logs:*:*:log-group:/aws/iotsitewise*:log-stream:*"
  },
  {
   "Sid": "AllowSiteWiseAccessSiteWiseManagedWorkspaceInTwinMaker",
   "Effect": "Allow",
   "Action": [
    "iottwinmaker:GetWorkspace",
    "iottwinmaker:ExecuteQuery"
   ],
   "Resource": "arn:aws:iottwinmaker:*:*:workspace/*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "iottwinmaker:linkedServices": [
      "IOTSITEWISE"
     ]
    }
   }
  }
 ]
}
```

AWS IoT SiteWise aggiornamenti alle politiche gestite AWS

È possibile visualizzare i dettagli sugli aggiornamenti delle politiche AWS gestite per AWS IoT SiteWise, a partire da quando questo servizio ha iniziato a tenere traccia delle modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei AWS IoT SiteWise documenti.

Modifica	Descrizione	Data
AWSServiceRoleForIoTSiteWise: aggiornamento a una policy esistente	AWS IoT SiteWise ora puoi eseguire una query di ricerca di metadati sul database. AWS IoT TwinMaker	6 novembre 2023
AWSIoTSiteWiseReadOnlyAccess: aggiornamento a una policy esistente	AWS IoT SiteWise ha aggiunto un nuovo prefisso di policy`BatchGet*` , che consente di eseguire operazioni di lettura in batch.	16 settembre 2022
AWSIoTSiteWiseReadOnlyAccess: nuova policy	AWS IoT SiteWise ha aggiunto una nuova politica a cui concedere l'accesso in sola lettura. AWS IoT SiteWise	24 novembre 2021
AWS IoT SiteWise ha iniziato a tenere traccia delle modifiche	AWS IoT SiteWise ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	24 novembre 2021

Utilizzo di ruoli collegati ai servizi per AWS IoT SiteWise

AWS IoT SiteWise utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM a cui è collegato direttamente. AWS IoT SiteWise I ruoli collegati ai servizi sono predefiniti AWS IoT SiteWise e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

I ruoli collegati ai servizi semplificano la configurazione AWS IoT SiteWise includendo automaticamente tutte le autorizzazioni necessarie. AWS IoT SiteWise definisce le autorizzazioni dei suoi ruoli collegati ai servizi e, se non diversamente definito, solo può assumerne i ruoli. AWS IoT SiteWise Le autorizzazioni definite includono policy di attendibilità e di autorizzazioni. E quella politica di autorizzazione non può essere associata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. Questo protegge AWS IoT SiteWise le tue risorse perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta Servizi AWS che funzionano con IAM e cerca i servizi che riportano Sì nella colonna Ruolo associato ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Argomenti

- Autorizzazioni del ruolo collegato ai servizi per AWS IoT SiteWise
- Creazione di un ruolo collegato ai servizi per AWS IoT SiteWise
- Modifica di un ruolo collegato ai servizi per AWS IoT SiteWise
- Eliminazione di un ruolo collegato ai servizi per AWS IoT SiteWise
- Regioni supportate per i ruoli collegati ai servizi AWS IoT SiteWise
- Utilizzo dei ruoli di servizio per AWS IoT SiteWise Monitor

Autorizzazioni del ruolo collegato ai servizi per AWS IoT SiteWise

AWS IoT SiteWise utilizza il ruolo collegato al servizio denominato. AWSServiceRoleForIoTSiteWise AWS IoT SiteWise utilizza questo ruolo collegato al servizio per distribuire i gateway SiteWise Edge (che vengono eseguiti) ed eseguire la registrazione. AWS IoT Greengrass

Il ruolo `AWSServiceRoleForIoTSiteWise` collegato al servizio utilizza la policy con le seguenti autorizzazioni. `AWSServiceRoleForIoTSiteWise` Questa politica:

- Consente di AWS IoT SiteWise implementare gateway SiteWise Edge (che funzionano su`AWS IoT Greengrass`).
- Consente di eseguire AWS IoT SiteWise la registrazione.
- Consente di AWS IoT SiteWise eseguire una query di ricerca di metadati nel AWS IoT TwinMaker database.

Per ulteriori informazioni sulle azioni consentite in`AWSServiceRoleForIoTSiteWise`, consulta le politiche AWS gestite per AWS IoT SiteWise.

```
{
```

```
"Version": "2012-10-17",
"Statement": [
 {
  "Sid": "AllowSiteWiseReadGreenGrass",
  "Effect": "Allow",
  "Action": [
   "greengrass:GetAssociatedRole",
   "greengrass:GetCoreDefinition",
   "greengrass:GetCoreDefinitionVersion",
   "greengrass:GetGroup",
   "greengrass:GetGroupVersion"
  ],
  "Resource": "*"
 },
 {
  "Sid": "AllowSiteWiseAccessLogGroup",
  "Effect": "Allow",
  "Action": [
   "logs:CreateLogGroup",
   "logs:DescribeLogGroups"
  ],
  "Resource": "arn:aws:logs:*:*:log-group:/aws/iotsitewise*"
 },
 {
  "Sid": "AllowSiteWiseAccessLog",
  "Effect": "Allow",
  "Action": [
   "logs:CreateLogStream",
   "logs:DescribeLogStreams",
   "logs:PutLogEvents"
  ],
  "Resource": "arn:aws:logs:*:*:log-group:/aws/iotsitewise*:log-stream:*"
 },
 {
  "Sid": "AllowSiteWiseAccessSiteWiseManagedWorkspaceInTwinMaker",
  "Effect": "Allow",
  "Action": [
   "iottwinmaker:GetWorkspace",
   "iottwinmaker:ExecuteQuery"
  ],
  "Resource": "arn:aws:iottwinmaker:*:*:workspace/*",
  "Condition": {
   "ForAnyValue:StringEquals": {
    "iottwinmaker:linkedServices": [
```

```
      "IOTSITEWISE"
     ]
    }
   }
  }
 ]
}
```

È possibile utilizzare i log per monitorare e risolvere i problemi dei gateway Edge. SiteWise Per ulteriori informazioni, consulta Monitoraggio dei log del gateway SiteWise Edge.

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato al servizio, configura innanzitutto le autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per AWS IoT SiteWise

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando esegui le seguenti operazioni nella AWS IoT SiteWise console, AWS IoT SiteWise crea automaticamente il ruolo collegato al servizio.

- Crea un gateway Greengrass V1.
- Configura l'opzione di registrazione.
- Scegliendo il pulsante di attivazione nel banner di esecuzione della query.

Se elimini questo ruolo collegato ai servizi, puoi ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando esegui un'operazione nella AWS IoT SiteWise console, AWS IoT SiteWise crea nuovamente il ruolo collegato al servizio.

Puoi anche utilizzare la console o l'API IAM per creare un ruolo collegato al servizio per. AWS IoT SiteWise

- Per farlo nella console IAM, crea un ruolo con la AWSServiceRoleForIoTSiteWisepolicy e instaura una relazione di fiducia con. `iotsitewise.amazonaws.com`
- Per farlo utilizzando la AWS CLI nostra API IAM, crea un ruolo con la `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise` policy e instaura una relazione di fiducia con`iotsitewise.amazonaws.com`.

Per ulteriori informazioni, consulta Creazione di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Se elimini il ruolo collegato ai servizi, puoi utilizzare lo stesso processo per crearlo nuovamente.

Modifica di un ruolo collegato ai servizi per AWS IoT SiteWise

AWS IoT SiteWise non consente di modificare il ruolo AWSServiceRoleForIoTSiteWise collegato al servizio. Dopo aver creato un ruolo collegato al servizio, non puoi modificarne il nome, perché potrebbero farvi riferimento diverse entità. Puoi tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per AWS IoT SiteWise

Se una funzionalità o un servizio che richiede un ruolo collegato al servizio non è più in uso, è consigliabile eliminare il ruolo associato. Questo per evitare di avere un'entità inattiva che non viene monitorata o gestita. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato al servizio prima di poterlo eliminare manualmente.

> **Note**
>
> Se il AWS IoT SiteWise servizio utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e riprova.

Per eliminare AWS IoT SiteWise le risorse utilizzate da AWSServiceRoleForIoTSiteWise

1. Disabilita la registrazione per AWS IoT SiteWise. Per ulteriori informazioni, consulta Modifica del livello di registrazione
2. Eliminare tutti i gateway SiteWise Edge attivi.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo collegato al AWSServiceRoleForIoTSiteWise servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi AWS IoT SiteWise

AWS IoT SiteWise supporta l'utilizzo di ruoli collegati al servizio in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta Endpoint e quote per AWS IoT SiteWise.

Utilizzo dei ruoli di servizio per AWS IoT SiteWise Monitor

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.

Per consentire agli utenti federati del portale SiteWise Monitor di accedere AWS IoT SiteWisealle AWS IAM Identity Center proprie risorse, è necessario assegnare un ruolo di servizio a ciascun portale creato. Il ruolo di servizio deve specificare SiteWise Monitor come entità attendibile e includere la policy AWSIoTSiteWiseMonitorPortalAccessgestita o definire autorizzazioni equivalenti. Questa policy è gestita AWS e definisce il set di autorizzazioni che SiteWise Monitor utilizza per accedere alle tue risorse AWS IoT SiteWise e a quelle di IAM Identity Center.

Quando crei un portale SiteWise Monitor, devi scegliere un ruolo che consenta agli utenti di quel portale di accedere alle tue risorse AWS IoT SiteWisee a quelle di IAM Identity Center. La AWS IoT SiteWise console può creare e configurare il ruolo per te. Puoi modificare il ruolo in IAM in un secondo momento. Gli utenti del portale avranno problemi a utilizzare i loro portali SiteWise Monitor se rimuovi le autorizzazioni richieste dal ruolo o elimini il ruolo.

> **Note**
>
> I portali creati prima del 29 aprile 2020 non richiedevano ruoli del servizio. Se hai creato portali prima di tale data, devi collegare ruoli del servizio per continuare a utilizzarli. Per farlo, vai alla pagina Portali nella AWS IoT SiteWise console, quindi scegli Migra tutti i portali per utilizzare i ruoli IAM.

Le sezioni seguenti descrivono come creare e gestire il ruolo del servizio SiteWise Monitor in o in. AWS Management Console AWS Command Line Interface

Indice

- Individuazione del ruolo del servizio di un portale (console)
- Creazione di un ruolo del servizio SiteWise Monitor (AWS IoT SiteWise console)
- Creazione di un ruolo del servizio SiteWise Monitor (console IAM)
- Modifica del ruolo del servizio di un portale (console)
- Gestione del ruolo del servizio SiteWise Monitor (CLI)
  - Individuazione del ruolo del servizio di un portale (CLI)
  - Creazione del ruolo del servizio SiteWise Monitor (CLI)
- SiteWise Monitora gli aggiornamenti a AWSIoTSiteWiseMonitorServiceRole

Autorizzazioni del ruolo di servizio per Monitor SiteWise

Quando si crea un portale, AWS IoT SiteWise consente di creare un ruolo il cui nome inizia con AWSIoTSiteWiseMonitorServiceRole. Questo ruolo consente agli utenti federati di SiteWise Monitor di accedere alla configurazione del portale, agli asset, ai dati degli asset e ai dati di configurazione di IAM Identity Center.

Ai fini dell'assunzione del ruolo, il ruolo considera attendibile il seguente servizio:

- `monitor.iotsitewise.amazonaws.com`

Il ruolo utilizza la seguente politica di autorizzazioni, il cui nome inizia con AWSIoTSiteWiseMonitorServicePortalPolicy, per consentire agli utenti di SiteWise Monitor di completare azioni sulle risorse del proprio account. La politica AWSIoTSiteWiseMonitorPortalAccessgestita definisce autorizzazioni equivalenti.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iotsitewise:DescribePortal",
                "iotsitewise:CreateProject",
                "iotsitewise:DescribeProject",
                "iotsitewise:UpdateProject",
                "iotsitewise:DeleteProject",
                "iotsitewise:ListProjects",
                "iotsitewise:BatchAssociateProjectAssets",
```

```
                "iotsitewise:BatchDisassociateProjectAssets",
                "iotsitewise:ListProjectAssets",
                "iotsitewise:CreateDashboard",
                "iotsitewise:DescribeDashboard",
                "iotsitewise:UpdateDashboard",
                "iotsitewise:DeleteDashboard",
                "iotsitewise:ListDashboards",
                "iotsitewise:CreateAccessPolicy",
                "iotsitewise:DescribeAccessPolicy",
                "iotsitewise:UpdateAccessPolicy",
                "iotsitewise:DeleteAccessPolicy",
                "iotsitewise:ListAccessPolicies",
                "iotsitewise:DescribeAsset",
                "iotsitewise:ListAssets",
                "iotsitewise:ListAssociatedAssets",
                "iotsitewise:DescribeAssetProperty",
                "iotsitewise:GetAssetPropertyValue",
                "iotsitewise:GetAssetPropertyValueHistory",
                "iotsitewise:GetAssetPropertyAggregates",
                "iotsitewise:BatchPutAssetPropertyValue",
                "iotsitewise:ListAssetRelationships",
                "iotsitewise:DescribeAssetModel",
                "iotsitewise:ListAssetModels",
                "iotsitewise:UpdateAssetModel",
                "iotsitewise:UpdateAssetModelPropertyRouting",
                "sso-directory:DescribeUsers",
                "sso-directory:DescribeUser",
                "iotevents:DescribeAlarmModel",
                "iotevents:ListTagsForResource"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iotevents:BatchAcknowledgeAlarm",
                "iotevents:BatchSnoozeAlarm",
                "iotevents:BatchEnableAlarm",
                "iotevents:BatchDisableAlarm"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "iotevents:keyValue": "false"
```

```
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iotevents:CreateAlarmModel",
                "iotevents:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/iotsitewisemonitor": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iotevents:UpdateAlarmModel",
                "iotevents:DeleteAlarmModel"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/iotsitewisemonitor": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "iotevents.amazonaws.com"
                    ]
                }
            }
        }
    ]
```

```
}
```

Per ulteriori informazioni sulle autorizzazioni richieste per gli allarmi, consulta. Configurazione delle autorizzazioni per gli AWS IoT Events allarmi

Quando un utente del portale accede, SiteWise Monitor crea una politica di sessione basata sull'intersezione tra il ruolo del servizio e le politiche di accesso dell'utente. Le policy di accesso definiscono il livello di accesso delle identità ai portali e ai progetti. Per ulteriori informazioni sulle autorizzazioni del portale e sulle politiche di accesso, consulta Amministrazione dei portali SiteWise Monitor e. CreateAccessPolicy

Gestione del ruolo del servizio SiteWise Monitor (console)

Console AWS IoT SiteWise Facilita la gestione del ruolo del servizio SiteWise Monitor per i portali. Al momento della creazione di un portale, la console verifica la presenza di ruoli esistenti adatti all'allegato. Se non ce ne sono disponibili, la console può creare e configurare automaticamente un ruolo di servizio. Per ulteriori informazioni, consulta Creazione di un portale.

Argomenti

- Individuazione del ruolo del servizio di un portale (console)
- Creazione di un ruolo del servizio SiteWise Monitor (AWS IoT SiteWise console)
- Creazione di un ruolo del servizio SiteWise Monitor (console IAM)
- Modifica del ruolo del servizio di un portale (console)

Individuazione del ruolo del servizio di un portale (console)

Utilizza i passaggi seguenti per trovare il ruolo di servizio associato a un portale di SiteWise monitoraggio.

Per individuare il ruolo del servizio di un portale

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione a sinistra scegliere Portals (Portali).
3. Scegliere il portale per il quale si desidera individuare il ruolo del servizio.

   Il ruolo collegato al portale viene visualizzato in Permissions (Autorizzazioni), Service role (Ruolo del servizio).

Creazione di un ruolo del servizio SiteWise Monitor (AWS IoT SiteWise console)

Quando crei un portale SiteWise Monitor, puoi creare un ruolo di servizio per il tuo portale. Per ulteriori informazioni, consulta Creazione di un portale.

È inoltre possibile creare un ruolo di servizio per un portale esistente nella AWS IoT SiteWise console. Questo sostituisce il ruolo di servizio esistente del portale.

Per creare un ruolo del servizio per un portale esistente

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione scegli Portali.
3. Scegliere il portale per il quale si desidera creare un nuovo ruolo del servizio.
4. In Portal details (Dettagli portale), scegliere Edit (Modifica).
5. In Permissions (Autorizzazioni), scegliere Create and use a new service role (Crea e utilizza un nuovo ruolo del servizio) dall'elenco.
6. Immettere un nome per il nuovo ruolo.
7. Selezionare Salva.

Creazione di un ruolo del servizio SiteWise Monitor (console IAM)

Puoi creare un ruolo di servizio dal modello di ruolo di servizio nella console IAM. Questo modello di ruolo include la policy AWSIoTSiteWiseMonitorPortalAccessgestita e specifica SiteWise Monitor come entità affidabile.

Per creare un ruolo di servizio dal modello di ruolo di servizio del portale

1. Passare alla IAM console (Console IAM).
2. Nel pannello di navigazione, seleziona Roles (Ruoli).
3. Selezionare Create role (Crea ruolo).
4. In Scegli un caso d'uso, scegli IoT SiteWise.
5. In Seleziona il tuo caso d'uso, scegli IoT SiteWise Monitor - Portal.
6. Scegliere Next: Permissions (Successivo: Autorizzazioni).
7. Scegliere Next: Tags (Successivo: Tag).
8. Scegliere Next:Review (Successivo: Rivedi).

9. Immettete un nome di ruolo per il nuovo ruolo di servizio.
10. Scegli Crea ruolo.

Modifica del ruolo del servizio di un portale (console)

Utilizzare la procedura seguente per scegliere un ruolo del servizio di SiteWise monitoraggio diverso per un portale.

Per modificare il ruolo del servizio di un portale

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione scegli Portali.
3. Scegliere il portale per il quale si desidera modificare il ruolo del servizio.
4. In Portal details (Dettagli portale), scegliere Edit (Modifica).
5. In Permissions (Autorizzazioni), scegliere Use an existing role (Utilizza un ruolo esistente).
6. Scegliere un ruolo esistente da collegare al portale.
7. Selezionare Salva.

Gestione del ruolo del servizio SiteWise Monitor (CLI)

È possibile utilizzare il AWS CLI per le seguenti attività di gestione dei ruoli del servizio del portale:

Argomenti

- Individuazione del ruolo del servizio di un portale (CLI)
- Creazione del ruolo del servizio SiteWise Monitor (CLI)

Individuazione del ruolo del servizio di un portale (CLI)

Per trovare il ruolo di servizio associato a un portale di SiteWise monitoraggio, esegui il comando seguente per elencare tutti i portali nella regione corrente.

```
aws iotsitewise list-portals
```

L'operazione restituisce una risposta contenente i riepiloghi del portale nel formato seguente.

```
{
```

```
  "portalSummaries": [
    {
      "id": "a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE",
      "name": "WindFarmPortal",
      "description": "A portal that contains wind farm projects for Example Corp.",
      "roleArn": "arn:aws:iam::123456789012:role/service-role/role-name",
      "startUrl": "https://a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE.app.iotsitewise.aws",
      "creationDate": "2020-02-04T23:01:52.90248068Z",
      "lastUpdateDate": "2020-02-04T23:01:52.90248078Z"
    }
  ]
}
```

Puoi anche utilizzare l'DescribePortaloperazione per trovare il ruolo del tuo portale se conosci l'ID del tuo portale.

Creazione del ruolo del servizio SiteWise Monitor (CLI)

Utilizza la procedura seguente per creare un nuovo ruolo del servizio SiteWise Monitor.

Per creare un ruolo SiteWise del servizio Monitor

1. Crea un ruolo con una politica di fiducia che consenta a SiteWise Monitor di assumere il ruolo. In questo esempio viene creato un ruolo denominato **`MySiteWiseMonitorPortalRole`** da una policy di attendibilità archiviata in una stringa JSON.

   Linux, macOS, or Unix

   ```
   aws iam create-role --role-name MySiteWiseMonitorPortalRole --assume-role-
   policy-document '{
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Principal": {
           "Service": "monitor.iotsitewise.amazonaws.com"
         },
         "Action": "sts:AssumeRole"
       }
     ]
   }'
   ```

Windows command prompt

```
aws iam create-role --role-name MySiteWiseMonitorPortalRole --assume-role-
policy-document "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"Service\":\"monitor.iotsitewise.amazonaws.com\"},\"Action\":
\"sts:AssumeRole\"}]}"
```

2. Copiare il ruolo ARN dai metadati del ruolo nell'output. Quando si crea un portale, utilizzare questo ARN per associare il ruolo al portale. Per ulteriori informazioni sulla creazione di un portale, CreatePortalconsulta l'AWS IoT SiteWise API Reference.
3. Allega la `AWSIoTSiteWiseMonitorPortalAccess` policy al ruolo o allega una policy che definisca autorizzazioni equivalenti.

```
aws iam attach-role-policy --role-name MySiteWiseMonitorPortalRole --policy-arn
 arn:aws:iam::aws:policy/service-role/AWSIoTSiteWiseMonitorPortalAccess
```

Per collegare un ruolo del servizio a un portale esistente

1. Per recuperare i dettagli esistenti del portale, eseguire il comando seguente. Sostituire *portal-id* con l'ID del portale.

```
aws iotsitewise describe-portal --portal-id portal-id
```

L'operazione restituisce una risposta contenente i dettagli del portale nel formato seguente.

```
{
    "portalId": "a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE",
    "portalArn": "arn:aws:iotsitewise:region:account-id:portal/a1b2c3d4-5678-90ab-
cdef-aaaaaEXAMPLE",
    "portalName": "WindFarmPortal",
    "portalDescription": "A portal that contains wind farm projects for Example
 Corp.",
    "portalClientId": "E-1a2b3c4d5e6f_sn6tbqHVzLWVEXAMPLE",
    "portalStartUrl": "https://a1b2c3d4-5678-90ab-cdef-
aaaaaEXAMPLE.app.iotsitewise.aws",
    "portalContactEmail": "support@example.com",
    "portalStatus": {
        "state": "ACTIVE"
    },
```

```
    "portalCreationDate": "2020-04-29T23:01:52.90248068Z",
    "portalLastUpdateDate": "2020-04-29T00:28:26.103548287Z",
    "roleArn": "arn:aws:iam::123456789012:role/service-role/
AWSIoTSiteWiseMonitorServiceRole_1aEXAMPLE"
}
```

2. Per collegare un ruolo del servizio a un portale, eseguire il comando seguente. Sostituire il *ruolo arn* con l'ARN del ruolo del servizio e sostituire i parametri rimanenti con i valori esistenti del portale.

```
aws iotsitewise update-portal \
  --portal-id portal-id \
  --role-arn role-arn \
  --portal-name portal-name \
  --portal-description portal-description \
  --portal-contact-email portal-contact-email
```

SiteWise Monitora gli aggiornamenti a AWSIoTSiteWiseMonitorServiceRole

È possibile visualizzare i dettagli sugli aggiornamenti di AWSIoTSiteWiseMonitorServiceRolefor SiteWise Monitor, a partire da quando questo servizio ha iniziato a tenere traccia delle modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei AWS IoT SiteWise documenti.

Modifica	Descrizione	Data
AWSIoTSiteWiseMonitorPortalAccess— Politica aggiornata	AWS IoT SiteWise ha aggiornato la politica di AWSIoTSiteWiseMonitorPortalAccessgestione per la funzionalità degli allarmi.	27 maggio 2021
AWS IoT SiteWise ha iniziato a tenere traccia delle modifiche	AWS IoT SiteWise ha iniziato a tenere traccia delle modifiche relative al suo ruolo di servizio.	15 dicembre 2020

Configurazione delle autorizzazioni per gli AWS IoT Events allarmi

Quando utilizzi un modello di AWS IoT Events allarme per monitorare la proprietà di un AWS IoT SiteWise asset, devi disporre delle seguenti autorizzazioni IAM:

- Un ruolo AWS IoT Events di servizio che consente di AWS IoT Events inviare dati a AWS IoT SiteWise. Per ulteriori informazioni, consulta la sezione Gestione delle identità e degli accessi AWS IoT Events nella Guida per gli AWS IoT Events sviluppatori.
- È necessario disporre delle seguenti AWS IoT SiteWise autorizzazioni di azione: `iotsitewise:DescribeAssetModel` `eiotsitewise:UpdateAssetModelPropertyRouting`. Queste autorizzazioni consentono di AWS IoT SiteWise inviare i valori delle proprietà degli asset ai modelli di AWS IoT Events allarme.

Per ulteriori informazioni, consulta le politiche basate sulle risorse nella Guida per l'utente IAM.

Autorizzazioni di azione richieste

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.

Prima di definire un modello di AWS IoT Events allarme, è necessario concedere le seguenti autorizzazioni che consentono AWS IoT SiteWise di inviare i valori delle proprietà degli asset al modello di allarme.

- `iotsitewise:DescribeAssetModel`— Consente di AWS IoT Events verificare se esiste una proprietà dell'asset.
- `iotsitewise:UpdateAssetModelPropertyRouting`— Consente di AWS IoT SiteWise creare automaticamente abbonamenti che consentono AWS IoT SiteWise di inviare dati a AWS IoT Events.

Per ulteriori informazioni sulle azioni AWS IoT SiteWise supportate, vedere Azioni definite da AWS IoT SiteWise nel Service Authorization Reference.

Example Esempio di politica delle autorizzazioni 1

La seguente politica consente di AWS IoT SiteWise inviare i valori delle proprietà degli asset a qualsiasi modello di AWS IoT Events allarme.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iotevents:CreateAlarmModel",
                "iotevents:UpdateAlarmModel"
            ],
            "Resource": "arn:aws:iotevents:us-east-1:123456789012:alarmModel/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iotsitewise:DescribeAssetModel",
                "iotsitewise:UpdateAssetModelPropertyRouting"
            ],
            "Resource": "arn:aws:iotsitewise:us-east-1:123456789012:asset-model/*"
        }
    ]
}
```

Example Esempio di politica di autorizzazione 2

La seguente politica consente di AWS IoT SiteWise inviare i valori di una proprietà di asset specificata a un modello di AWS IoT Events allarme specificato.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iotevents:CreateAlarmModel",
                "iotevents:UpdateAlarmModel"
            ],
            "Resource": "arn:aws:iotevents:us-east-1:123456789012:alarmModel/*"
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "iotsitewise:DescribeAssetModel"
            ],
            "Resource": "arn:aws:iotsitewise:us-east-1:123456789012:asset-model/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iotsitewise:UpdateAssetModelPropertyRouting"
            ],
            "Resource": [
                "arn:aws:iotsitewise:us-east-1:123456789012:asset-model/12345678-90ab-
cdef-1234-567890abcdef"
            ],
            "Condition": {
                "StringLike": {
                    "iotsitewise:propertyId": "abcdef12-3456-7890-abcd-ef1234567890",
                    "iotevents:alarmModelArn": "arn:aws:iotevents:us-
east-1:123456789012:alarmModel/MyAlarmModel"
                }
            }
        }
    ]
}
```

ListInputRoutings Autorizzazione (Facoltativa)

Quando aggiorni o elimini un modello di asset, AWS IoT SiteWise puoi verificare se un modello di allarme in esecuzione AWS IoT Events sta monitorando una proprietà di asset associata a questo modello di asset. Ciò impedisce di eliminare una proprietà dell'asset attualmente utilizzata da un AWS IoT Events allarme. Per abilitare questa funzionalità AWS IoT SiteWise, è necessario disporre dell'`iotevents:ListInputRoutings`autorizzazione. Questa autorizzazione consente di AWS IoT SiteWise effettuare chiamate all'operazione ListInputRoutingsAPI supportata da AWS IoT Events.

> **Note**
>
> Ti consigliamo vivamente di aggiungere l'`ListInputRoutings`autorizzazione.

Example Esempio di politica sulle autorizzazioni

La seguente politica consente di aggiornare ed eliminare i modelli di asset e di utilizzare l'`ListInputRoutings`API in AWS IoT SiteWise.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iotsitewise:UpdateAssetModel",
                "iotsitewise:DeleteAssetModel",
                "iotevents:ListInputRoutings"
            ],
            "Resource": "arn:aws:iotsitewise:us-east-1:123456789012:asset-model/*"
        }
    ]
}
```

Autorizzazioni richieste per Monitor SiteWise

Se desideri utilizzare la funzionalità di allarme nei portali SiteWise Monitor, devi aggiornare il ruolo del servizio SiteWise Monitor con la seguente politica:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iotsitewise:DescribePortal",
                "iotsitewise:CreateProject",
                "iotsitewise:DescribeProject",
                "iotsitewise:UpdateProject",
                "iotsitewise:DeleteProject",
                "iotsitewise:ListProjects",
                "iotsitewise:BatchAssociateProjectAssets",
                "iotsitewise:BatchDisassociateProjectAssets",
                "iotsitewise:ListProjectAssets",
                "iotsitewise:CreateDashboard",
                "iotsitewise:DescribeDashboard",
                "iotsitewise:UpdateDashboard",
```

```
                "iotsitewise:DeleteDashboard",
                "iotsitewise:ListDashboards",
                "iotsitewise:CreateAccessPolicy",
                "iotsitewise:DescribeAccessPolicy",
                "iotsitewise:UpdateAccessPolicy",
                "iotsitewise:DeleteAccessPolicy",
                "iotsitewise:ListAccessPolicies",
                "iotsitewise:DescribeAsset",
                "iotsitewise:ListAssets",
                "iotsitewise:ListAssociatedAssets",
                "iotsitewise:DescribeAssetProperty",
                "iotsitewise:GetAssetPropertyValue",
                "iotsitewise:GetAssetPropertyValueHistory",
                "iotsitewise:GetAssetPropertyAggregates",
                "iotsitewise:BatchPutAssetPropertyValue",
                "iotsitewise:ListAssetRelationships",
                "iotsitewise:DescribeAssetModel",
                "iotsitewise:ListAssetModels",
                "iotsitewise:UpdateAssetModel",
                "iotsitewise:UpdateAssetModelPropertyRouting",
                "sso-directory:DescribeUsers",
                "sso-directory:DescribeUser",
                "iotevents:DescribeAlarmModel",
                "iotevents:ListTagsForResource"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iotevents:BatchAcknowledgeAlarm",
                "iotevents:BatchSnoozeAlarm",
                "iotevents:BatchEnableAlarm",
                "iotevents:BatchDisableAlarm"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "iotevents:keyValue": "false"
                }
            }
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "iotevents:CreateAlarmModel",
                "iotevents:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/iotsitewisemonitor": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iotevents:UpdateAlarmModel",
                "iotevents:DeleteAlarmModel"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/iotsitewisemonitor": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "iotevents.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

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 intersettoriale 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 `aws:SourceArn`le chiavi di contesto della condizione `aws:SourceAccount`globale nelle politiche delle risorse per limitare le autorizzazioni che AWS IoT SiteWise forniscono un altro servizio alla risorsa. Se il valore `aws:SourceArn` non contiene l'ID account, ad esempio il nome della risorsa Amazon (ARN) di un bucket Amazon S3, è necessario utilizzare entrambe le chiavi di contesto delle condizioni globali per limitare le autorizzazioni. Se si utilizzano entrambe le chiavi di contesto delle condizioni globali e il valore `aws:SourceArn` contiene l'ID account, il valore `aws:SourceAccount` e l'account nel valore `aws:SourceArn` deve utilizzare lo stesso ID account nella stessa dichiarazione di policy.

- Utilizzare `aws:SourceArn` se si desidera consentire l'associazione di una sola risorsa all'accesso tra servizi.
- Utilizza `aws:SourceAccount` se desideri consentire l'associazione di qualsiasi risorsa in tale account all'uso tra servizi.

Il valore di `aws:SourceArn` deve essere la risorsa AWS IoT SiteWise del cliente associata alla `sts:AssumeRole` richiesta.

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'ARN completo della risorsa. Se non si conosce l'ARN completo della risorsa o se si sta specificando più risorse, utilizzare la chiave di condizione del contesto globale `aws:SourceArn` con caratteri speciali (`*`) per le parti sconosciute dell'ARN. Ad esempio, `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`.

Example — Vice Prevenzione confusa

L'esempio seguente mostra come utilizzare le chiavi di contesto `aws:SourceArn` e `aws:SourceAccount` global condition AWS IoT SiteWise per prevenire il problema del confuso vice.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "iotsitewise.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Resource": [
      "arn:aws:iotsitewise:::ResourceName/*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:iotsitewise:*:123456789012:*"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

Risoluzione dei problemi relativi AWS IoT SiteWise all'identità e all'accesso

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con AWS IoT SiteWise and AWS Identity and Access Management (IAM).

Argomenti

- Non sono autorizzato a eseguire alcuna azione in AWS IoT SiteWise
- Non sono autorizzato a eseguire iam:PassRole
- Voglio consentire a persone esterne a me di accedere Account AWS alle mie AWS IoT SiteWise risorse

Non sono autorizzato a eseguire alcuna azione in AWS IoT SiteWise

Se ti AWS Management Console dice che non sei autorizzato a eseguire un'azione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è la persona da cui si sono ricevuti il nome utente e la password.

L'errore di esempio seguente si verifica quando l'utente `mateojackson` IAM tenta di utilizzare la console per visualizzare i dettagli su una risorsa ma non dispone `iotsitewise:DescribeAsset` delle autorizzazioni.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 iotsitewise:DescribeAsset on resource: a1b2c3d4-5678-90ab-cdef-22222EXAMPLE
```

In questo caso, Mateo chiede al suo amministratore di aggiornare le sue policy per poter accedere alla risorsa asset con ID `a1b2c3d4-5678-90ab-cdef-22222EXAMPLE` mediante l'operazione `iotsitewise:DescribeAsset`.

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 AWS IoT SiteWise.

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 in AWS IoT SiteWise. 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 a me di accedere Account AWS alle mie AWS IoT SiteWise risorse

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 sapere se AWS IoT SiteWise supporta queste funzionalità, consultaCome AWS IoT SiteWise 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 AWS IoT SiteWise

AWS IoT SiteWise non rientra nell'ambito di alcun programma di AWS conformità.

Per un elenco dei AWS servizi che rientrano nell'ambito di specifici programmi di conformità, vedere AWS Servizi compresi nell'ambito del programma di conformitàAWS . Per informazioni generali, vedere 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 AWS IoT SiteWise 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 rapide su sicurezza e conformità Guide introduttive implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla sicurezza e la conformità. AWS
- Whitepaper sull'architettura per la sicurezza e la conformità HIPAA: questo white paper descrive in che modo le aziende possono utilizzare per creare applicazioni conformi all'HIPAA. AWS
- AWS Risorse per la conformità Risorse per la conformità: questa raccolta di potrebbe riguardare il settore e la località in cui operate.
- Valutazione delle risorse in base alle regole contenute nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- AWS Security Hub— Questo AWS servizio offre una visione completa dello stato di sicurezza dell'utente, AWS che consente di verificare la conformità agli standard e alle best practice del settore della sicurezza.
- Dieci regole d'oro di sicurezza per le soluzioni IoT industriali: questo post sul blog introduce dieci regole d'oro che aiutano a proteggere i sistemi di controllo industriale (ICS), l'Internet of Things industriale (IIoT) e gli ambienti cloud.
- Best practice di sicurezza per la produzione OT: questo white paper descrive le migliori pratiche di sicurezza per progettare, implementare e progettare questi carichi di lavoro di produzione ibrida on-premise per il cloud. AWS

Resilienza in AWS IoT SiteWise

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.

AWS IoT SiteWise è completamente gestito e utilizza AWS servizi durevoli e ad alta disponibilità, come Amazon S3 e Amazon EC2. Per garantire la disponibilità in caso di interruzione della zona di disponibilità, AWS IoT SiteWise opera su più zone di disponibilità.

Per ulteriori informazioni su AWS regioni e zone di disponibilità, vedere AWS Global Infrastructure.

Oltre all'infrastruttura AWS globale, AWS IoT SiteWise offre diverse funzionalità per supportare le esigenze di resilienza e backup dei dati:

- È possibile pubblicare gli aggiornamenti dei valori delle proprietà AWS IoT Core tramite messaggi MQTT, quindi configurare le regole per agire su tali dati. Con questa funzionalità, puoi eseguire il backup dei dati in altri AWS servizi come Amazon S3 e Amazon DynamoDB. Per ulteriori informazioni, consulta Interazione con altri servizi AWS e Esporta i dati su Amazon S3 con notifiche sulle proprietà degli asset.
- Puoi utilizzare le AWS IoT SiteWise `Get*` API per recuperare e fare il backup dei dati storici sulle proprietà degli asset. Per ulteriori informazioni, consulta Esecuzione di query sui valori cronologici delle proprietà degli asset.
- Puoi utilizzare le AWS IoT SiteWise `Describe*` API per recuperare le definizioni delle tue risorse, come asset e modelli. È possibile eseguire il backup di queste definizioni e utilizzarle in seguito per ricreare le risorse. Per ulteriori informazioni, consulta la Documentazione di riferimento delle API di AWS IoT SiteWise .

Sicurezza dell'infrastruttura in AWS IoT SiteWise

In quanto servizio gestito, AWS IoT SiteWise è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzate chiamate API AWS pubblicate per accedere AWS IoT SiteWise attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), 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.

SiteWise I gateway edge, che funzionano su AWS IoT Greengrass, utilizzano certificati X.509 e chiavi crittografiche per connettersi e autenticarsi al cloud. AWS Per ulteriori informazioni,

consulta Autenticazione e autorizzazione del dispositivo nella Guida per gli AWS IoT Greengrass sviluppatori.AWS IoT Greengrass Version 1

Analisi della configurazione e delle vulnerabilità

I parchi istanze IoT possono essere costituiti da un numero elevato di dispositivi con funzionalità diverse, usati per lunghi periodi di tempo e distribuiti in varie aree geografiche. Queste caratteristiche rendono la configurazione di un parco istanze complessa e soggetta a errori. Poiché i dispositivi di solito hanno potenza di elaborazione, memoria e spazio di archiviazione limitati, non sempre possono supportare la crittografia e altre misure di sicurezza. I dispositivi, inoltre, usano spesso software con vulnerabilità note. La combinazione di questi fattori rende i parchi istanze IoT un facile bersaglio per gli hacker e rende difficile la protezione continuativa di un parco istanze di dispositivi.

AWS IoT Device Defender affronta queste sfide fornendo strumenti per identificare i problemi di sicurezza e le deviazioni dalle migliori pratiche. AWS IoT Device Defender Utilizzatelo per analizzare, controllare e monitorare i dispositivi connessi per rilevare comportamenti anomali e mitigare i rischi per la sicurezza. AWS IoT Device Defender può controllare le flotte di dispositivi per garantire che aderiscano alle migliori pratiche di sicurezza e rilevi comportamenti anomali sui dispositivi. In questo modo è possibile applicare politiche di sicurezza coerenti in tutto il parco AWS IoT dispositivi e rispondere rapidamente quando i dispositivi vengono compromessi. Per ulteriori informazioni, consulta la sezione AWS IoT Device Defender nella Guida per gli sviluppatori di AWS IoT .

Se utilizzi i gateway SiteWise Edge per importare dati nel servizio, è tua responsabilità configurare e gestire l'ambiente del gateway SiteWise Edge. Questa responsabilità include l'aggiornamento alle versioni più recenti del software di sistema, AWS IoT Greengrass del software e del connettore del gateway SiteWise Edge. AWS IoT SiteWise Per ulteriori informazioni, consulta Configurare il AWS IoT Greengrass core nella Guida per gli AWS IoT Greengrass Version 1 sviluppatori e. Aggiornamento di un connettore

Endpoint VPC

Un endpoint VPC di interfaccia stabilisce una connessione privata tra il tuo cloud privato virtuale (VPC) e. AWS IoT SiteWiseAWS PrivateLinkalimenta gli endpoint di interfaccia, abilitando l'accesso privato alle operazioni delle API. AWS IoT SiteWise È possibile ignorare la necessità di un gateway Internet, un dispositivo NAT, una connessione VPN o. AWS Direct Connect Le istanze nel tuo VPC non necessitano di indirizzi IP pubblici per comunicare AWS IoT SiteWise con le operazioni API. Il traffico tra il tuo VPC e AWS IoT SiteWise non esce dalla AWS rete.

Ogni endpoint di interfaccia è rappresentato da una o più interfacce di rete elastiche nelle sottoreti.

Prima di configurare un endpoint VPC di interfaccia per AWS IoT SiteWise, consulta le proprietà e le limitazioni dell'endpoint dell'interfaccia nella Amazon VPC User Guide.

Per ulteriori informazioni, consultare Endpoint VPC di interfaccia (AWS PrivateLink) nella Guida per l'utente di Amazon VPC.

Operazioni API supportate per endpoint VPC

AWS IoT SiteWise supporta l'effettuazione di chiamate alle seguenti operazioni AWS IoT SiteWise API dal tuo VPC:

- Per tutte le operazioni dell'API del piano dati, utilizza il seguente endpoint: Sostituisci *region* con Regione AWS

  ```
  data.iotsitewise.region.amazonaws.com
  ```

  Le operazioni dell'API del piano dati includono quanto segue:

  - BatchGetAssetPropertyValue
  - BatchGetAssetPropertyValueHistory
  - BatchPutAssetPropertyValue
  - GetAssetPropertyAggregates
  - GetAssetPropertyValue
  - GetAssetPropertyValueHistory
  - GetInterpolatedAssetPropertyValues
- Per le operazioni API del piano di controllo utilizzate per gestire i modelli di asset, gli asset, i gateway SiteWise Edge, i tag e le configurazioni degli account, utilizzate il seguente endpoint. Sostituisci *region* con il tuo Regione AWS.

  ```
  api.iotsitewise.region.amazonaws.com
  ```

  Le operazioni API del piano di controllo supportate includono quanto segue:

  - AssociateAssets
  - CreateAsset
  - CreateAssetModel

- DeleteAsset
- DeleteAssetModel
- DeleteDashboard
- DescribeAsset
- DescribeAssetModel
- DescribeAssetProperty
- DescribeDashboard
- DescribeLoggingOptions
- DisassociateAssets
- ListAssetModels
- ListAssetRelationships
- ListAssets
- ListAssociatedAssets
- PutLoggingOptions
- UpdateAsset
- UpdateAssetModel
- UpdateAssetProperty
- CreateGateway
- DeleteGateway
- DescribeDefaultEncryptionConfiguration
- DescribeGateway
- DescribeGatewayCapabilityConfiguration
- DescribeStorageConfiguration
- ListGateways
- ListTagsForResource
- UpdateGateway
- UpdateGatewayCapabilityConfiguration
- PutDefaultEncryptionConfiguration
- PutStorageConfiguration
- TagResource

- UntagResource

> **Note**
>
> L'endpoint VPC dell'interfaccia per le operazioni dell'API del piano di controllo attualmente non supporta l'effettuazione di chiamate alle seguenti operazioni dell'API SiteWise Monitor:
>
> - BatchAssociateProjectAssets
> - BatchDisassociateProjectAssets
> - CreateAccessPolicy
> - CreateDashboard
> - CreatePortal
> - CreateProject
> - DeleteAccessPolicy
> - DeletePortal
> - DeleteProject
> - DescribeAccessPolicy
> - DescribePortal
> - DescribeProject
> - ListAccessPolicies
> - ListDashboards
> - ListPortals
> - ListProjects
> - ListProjectAssets
> - UpdateAccessPolicy
> - UpdateDashboard
> - UpdatePortal
> - UpdateProject

Creazione di un endpoint VPC interfaccia per l' AWS IoT SiteWise

Per creare un endpoint VPC per il AWS IoT SiteWise servizio, usa la console Amazon VPC o (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consulta Creazione di un endpoint dell'interfaccia nella Guida per l'utente di Amazon VPC.

Crea un endpoint VPC per AWS IoT SiteWise utilizzando uno dei seguenti nomi di servizio:

- Per le operazioni dell'API del piano dati, utilizza il seguente nome di servizio:

```
com.amazonaws.region.iotsitewise.data
```

- Per le operazioni dell'API del piano di controllo, utilizzare il seguente nome di servizio:

```
com.amazonaws.region.iotsitewise.api
```

Accesso AWS IoT SiteWise tramite un endpoint VPC di interfaccia

Quando crei un endpoint di interfaccia, generiamo nomi host DNS specifici dell'endpoint con cui puoi comunicare. AWS IoT SiteWise L'opzione DNS privato è abilitata per impostazione predefinita. Per ulteriori informazioni, consulta Using private hosted zones nella Amazon VPC User Guide.

Se abiliti il DNS privato per l'endpoint, puoi effettuare richieste API AWS IoT SiteWise tramite uno dei seguenti endpoint VPC.

- *Per le operazioni dell'API del **piano dati**, utilizza il seguente endpoint: Sostituisci la regione con la tua.* Regione AWS

```
data.iotsitewise.region.amazonaws.com
```

- Per le operazioni dell'API del piano di controllo, utilizza il seguente endpoint: Sostituisci la *regione* con la tua. Regione AWS

```
api.iotsitewise.region.amazonaws.com
```

Se disabiliti il DNS privato per l'endpoint, devi fare quanto segue per accedere AWS IoT SiteWise tramite l'endpoint:

1. Specificare l'URL dell'endpoint VPC nelle richieste API.
   - Per le operazioni dell'API del piano dati, utilizza il seguente URL dell'endpoint. Sostituisci una *regione* con l'ID *vpc-endpoint-id*e la regione dell'endpoint VPC.

     ```
     vpc-endpoint-id.data.iotsitewise.region.vpce.amazonaws.com
     ```

   - Per le operazioni dell'API del piano di controllo, utilizza il seguente URL dell'endpoint. Sostituisci una *regione* con l'ID *vpc-endpoint-id*e la regione dell'endpoint VPC.

     ```
     vpc-endpoint-id.api.iotsitewise.region.vpce.amazonaws.com
     ```

2. Disabilita l'iniezione del prefisso dell'host. Gli AWS CLI e AWS SDK antepongono all'endpoint del servizio vari prefissi host quando si chiama ciascuna operazione API. Questa funzionalità fa sì che gli AWS CLI e AWS SDK producano URL non validi per AWS IoT SiteWise quando si specifica un endpoint VPC.

   > **Important**
   >
   > Non è possibile disabilitare l'iniezione del prefisso host in o in. AWS CLI AWS Tools for PowerShell Ciò significa che se disabiliti il DNS privato, non puoi utilizzare questi strumenti per accedere AWS IoT SiteWise tramite l'endpoint VPC. Abilita il DNS privato per utilizzare AWS CLI o per accedere tramite AWS IoT SiteWise l' AWS Tools for PowerShell endpoint.

   Per ulteriori informazioni su come disabilitare l'inserimento del prefisso dell'host negli AWS SDK, consulta le seguenti sezioni della documentazione per ciascun SDK:

   - AWS SDK for C++
   - AWS SDK for Go
   - AWS SDK for Go v2
   - AWS SDK for Java
   - AWS SDK for Java 2.x
   - AWS SDK for JavaScript
   - AWS SDK for .NET
   - AWS SDK for PHP
   - AWS SDK for Python (Boto3)
   - AWS SDK for Ruby

Per ulteriori informazioni, consulta Accesso a un servizio tramite un endpoint dell'interfaccia in Guida per l'utente di Amazon VPC.

Creazione di una policy per gli endpoint VPC per AWS IoT SiteWise

È possibile allegare un criterio all'endpoint VPC che controlla l'accesso all' AWS IoT SiteWise. Questa policy specifica le informazioni riportate di seguito:

- Il principale che può eseguire operazioni.
- Le operazioni che possono essere eseguite.
- Le risorse su cui è possibile eseguire le operazioni.

Per ulteriori informazioni, consulta Controllo degli accessi ai servizi con endpoint VPC nella Guida per l'utente di Amazon VPC.

Esempio: policy degli endpoint VPC per le azioni AWS IoT SiteWise

Di seguito è riportato un esempio di policy sugli endpoint per. AWS IoT SiteWise Se associata a un endpoint, questa policy concede l'accesso alle AWS IoT SiteWise azioni elencate per l'utente *iotsitewiseadmin* in Account AWS *123456789012* sulla risorsa specificata.

```
{
    "Statement": [
        {
            "Action": [
                "iotsitewise:CreateAsset",
                "iotsitewise:ListGateways",
                "iotsitewise:ListTagsForResource"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:iotsitewise:us-west-2:123456789012:asset/
a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
            "Principal": {
                "AWS": [
                    "123456789012:user/iotsitewiseadmin"
                ]
            }
        }
    ]
}
```

Le migliori pratiche di sicurezza per AWS IoT SiteWise

Questo argomento contiene le migliori pratiche di sicurezza per AWS IoT SiteWise.

Utilizzo delle credenziali di autenticazione sui server OPC-UA

Richiedi credenziali di autenticazione per connetterti ai server OPC-UA. A questo scopo, consulta la documentazione relativa ai server. Quindi, per consentire al gateway SiteWise Edge di connettersi ai server OPC-UA, aggiungi i segreti di autenticazione del server al gateway SiteWise Edge. Per ulteriori informazioni, consulta Configurazione dell'autenticazione dell'origine.

Utilizzo delle modalità di comunicazione crittografate per i server OPC-UA

Scegli una modalità di sicurezza dei messaggi crittografata e non obsoleta quando configuri le sorgenti OPC-UA per il tuo gateway Edge. SiteWise Questo aiuta a proteggere i dati industriali durante il trasferimento dai server OPC-UA al gateway Edge. SiteWise Per ulteriori informazioni, consulta Dati in transito sulla rete locale e Configurazione delle origini dati.

Mantieni aggiornati i tuoi componenti

Se utilizzi i gateway SiteWise Edge per importare dati nel servizio, è tua responsabilità configurare e mantenere l'ambiente del gateway Edge. SiteWise Questa responsabilità include l'aggiornamento alle versioni più recenti del software di sistema, del software e dei connettori del gateway. AWS IoT Greengrass

> **Note**
>
> Il connettore AWS IoT SiteWise Edge memorizza segreti sul file system. Questi segreti controllano chi può visualizzare i dati memorizzati nella cache all'interno del gateway SiteWise Edge. Si consiglia vivamente di attivare la crittografia del disco o del file system per il sistema su cui è in esecuzione il SiteWise gateway Edge.

Crittografa il file system SiteWise del gateway Edge

Crittografa e proteggi il tuo gateway SiteWise Edge, in modo che i tuoi dati industriali siano al sicuro mentre si spostano attraverso il gateway SiteWise Edge. Se il gateway SiteWise Edge dispone di un modulo di sicurezza hardware, è possibile configurarlo AWS IoT Greengrass per proteggere il

gateway SiteWise Edge. Per ulteriori informazioni, consulta Integrazione della sicurezza hardware nella Guida per gli AWS IoT Greengrass Version 1 sviluppatori. In caso contrario, consulta la documentazione del sistema operativo in uso per informazioni su come crittografare e proteggere il file system.

Accesso sicuro alla configurazione perimetrale

Non condividere la password dell'applicazione Edge Console o la password dell'applicazione SiteWise Monitor. Non inserire questa password in luoghi in cui chiunque possa vederla. Implementa una corretta politica di rotazione delle password configurando una scadenza appropriata per la password.

Concedi agli utenti di SiteWise Monitor le autorizzazioni minime possibili

Segui il principio del privilegio minimo utilizzando il set minimo di autorizzazioni relative ai criteri di accesso per gli utenti del portale.

- Quando si crea un portale, definire un ruolo che consenta il set minimo di asset necessario per tale portale. Per ulteriori informazioni, consulta Utilizzo dei ruoli di servizio per AWS IoT SiteWise Monitor.
- Quando l'utente e gli amministratori del portale creano e condividono progetti, utilizzare il set minimo di asset richiesto per tale progetto.
- Quando un'identità non ha più bisogno di accedere a un portale o a un progetto, rimuovila da quella risorsa. Se tale identità non è più applicabile alla tua organizzazione, eliminala dal tuo archivio di identità.

La best practice basata sul principio minimo si applica anche ai ruoli IAM. Per ulteriori informazioni, consulta Best practice delle policy.

Non esporre informazioni riservate

È necessario impedire la registrazione delle credenziali e di altre informazioni riservate, come le informazioni personali (PII). Ti consigliamo di implementare le seguenti misure di sicurezza anche se l'accesso ai log locali su un gateway SiteWise Edge richiede i privilegi di root e l'accesso ai CloudWatch log richiede le autorizzazioni IAM.

- Non utilizzare informazioni riservate in nomi, descrizioni o proprietà di asset o modelli.
- Non utilizzare informazioni sensibili nel gateway SiteWise Edge o nei nomi delle sorgenti.

- Non utilizzare informazioni riservate in nomi o descrizioni di portali, progetti o pannelli di controllo.

Segui le migliori pratiche di AWS IoT Greengrass sicurezza

Segui le best practice AWS IoT Greengrass di sicurezza per il tuo gateway SiteWise Edge. Per ulteriori informazioni, consulta le migliori pratiche di sicurezza nella Guida per gli AWS IoT Greengrass Version 1 sviluppatori.

Consulta anche

- Le migliori pratiche di sicurezza nella Guida per AWS IoT gli sviluppatori
- Dieci regole d'oro di sicurezza per le soluzioni Industrial IoT

Registrazione e monitoraggio AWS IoT SiteWise

Il monitoraggio è un elemento importante per mantenere l'affidabilità, la disponibilità e le prestazioni delle AWS IoT SiteWise altre AWS soluzioni. AWS IoT SiteWise supporta i seguenti strumenti di monitoraggio per monitorare il servizio, segnalare quando qualcosa non va e intraprendere azioni automatiche se necessario:

- Amazon CloudWatch monitora AWS le tue risorse e le applicazioni su cui esegui AWS in tempo reale. Raccogli e monitora i parametri, crea dashboard personalizzati e imposta allarmi che ti avvisano o intraprendono azioni quando una determinata metrica raggiunge una determinata soglia. Ad esempio, puoi tenere CloudWatch traccia dell'utilizzo della CPU o di altri parametri delle tue istanze Amazon EC2 e avviare automaticamente nuove istanze quando necessario. Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.
- Amazon CloudWatch Logs monitora, archivia e accede ai tuoi file di registro da gateway SiteWise Edge e altre fonti CloudTrail. CloudWatch I log possono monitorare le informazioni nei file di registro e avvisarti quando vengono raggiunte determinate soglie. Puoi inoltre archiviare i dati del log in storage estremamente durevole. Per ulteriori informazioni, consulta la Amazon CloudWatch Logs User Guide.
- AWS CloudTrailacquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo AWS account. Quindi CloudTrail invia i file di log a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno effettuato le chiamate AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Per ulteriori informazioni, consulta la Guida per l'utente AWS CloudTrail.

Argomenti

Monitoraggio con Amazon CloudWatch Logs

Configura AWS IoT SiteWise per registrare le informazioni in CloudWatch Logs per monitorare e risolvere i problemi del servizio.

Quando usi la AWS IoT SiteWise console, AWS IoT SiteWise crea un ruolo collegato al servizio che consente al servizio di registrare le informazioni per tuo conto. Se non utilizzi la AWS IoT SiteWise console, devi creare manualmente un ruolo collegato al servizio per ricevere i log. Per ulteriori informazioni, consulta Creazione di un ruolo collegato ai servizi per AWS IoT SiteWise.

È necessario disporre di una politica delle risorse che AWS IoT SiteWise consenta di inserire gli eventi di registro negli stream. CloudWatch Per creare e aggiornare una politica delle risorse per CloudWatch Logs, esegui il comando seguente. Sostituisci *logging-policy-name* con il nome della politica da creare.

```
aws logs put-resource-policy --policy-name logging-policy-name --policy-
document "{ \"Version\": \"2012-10-17\", \"Statement\": [ { \"Sid\":
 \"IoTSiteWiseToCloudWatchLogs\", \"Effect\": \"Allow\", \"Principal\": { \"Service\":
 [ \"iotsitewise.amazonaws.com\" ] }, \"Action\":\"logs:PutLogEvents\", \"Resource\":
 \"*\" } ] }"
```

CloudWatch Logs supporta anche le chiavi di contesto aws: SourceArn e aws: SourceAccount condition. Queste chiavi di contesto delle condizioni sono opzionali.

Per creare o aggiornare una politica delle risorse che AWS IoT SiteWise consenta di inserire solo i log associati alla AWS IoT SiteWise risorsa specificata negli CloudWatch stream, esegui il comando ed esegui quanto segue:

- Sostituisci *logging-policy-name* con il nome della politica da creare.
- Sostituisci *Source-ARN con* l'ARN della tua AWS IoT SiteWise risorsa, ad esempio un modello di asset o un asset. Per trovare l'ARN per ogni tipo di AWS IoT SiteWise risorsa, vedere Tipi di risorse definiti da AWS IoT SiteWise nel Service Authorization Reference.
- Sostituisci l'*Account-ID* con l'ID AWS dell'account associato alla risorsa specificata. AWS IoT SiteWise

```
aws logs put-resource-policy --policy-name logging-policy-name --policy-
document "{ \"Version\": \"2012-10-17\", \"Statement\": [ { \"Sid\":
 \"IoTSiteWiseToCloudWatchLogs\", \"Effect\": \"Allow\", \"Principal\": { \"Service
\": [ \"iotsitewise.amazonaws.com\" ] }, \"Action\":\"logs:PutLogEvents\", \"Resource
\": \"*\", \"Condition\":{\"StringLike\":{\"aws:SourceArn\":[\"source-ARN\"],
\"aws:SourceAccount\":[\"account-ID\"]}}}]}"
```

Per impostazione predefinita, AWS IoT SiteWise non registra le informazioni nei registri. CloudWatch Per attivare la registrazione, scegliete un livello di registrazione diverso da Disabilitato (). `OFF` AWS IoT SiteWise supporta i seguenti livelli di registrazione:

- `OFF`— La registrazione è disattivata.
- `ERROR`— Gli errori vengono registrati.
- `INFO`— Gli errori e i messaggi informativi vengono registrati.

È possibile configurare i gateway SiteWise Edge per registrare le informazioni su Logs through. CloudWatch AWS IoT Greengrass Per ulteriori informazioni, consulta Monitoraggio dei log del gateway SiteWise Edge.

È inoltre possibile configurare AWS IoT Core la registrazione delle informazioni nei CloudWatch registri se si sta risolvendo un'azione relativa a una AWS IoT SiteWise regola. Per ulteriori informazioni, consulta Risoluzione dei problemi e azioni AWS IoT SiteWise relative alle regole.

Indice

Gestire l'accesso AWS IoT SiteWise

Utilizza la AWS IoT SiteWise console o AWS CLI per le seguenti attività di configurazione della registrazione.

Individuazione del livello di registrazione

Console

Utilizza la procedura seguente per trovare il livello di registrazione corrente nella console AWS IoT SiteWise .

Per trovare il tuo attuale livello di AWS IoT SiteWise registrazione

1. Passare alla console AWS IoT SiteWise.

2. Nel riquadro di navigazione a sinistra, scegliere Logging options (Opzioni di registrazione).

   Lo stato di registrazione corrente viene visualizzato in Logging status (Stato di registrazione). Se la registrazione è attivata, il livello di registrazione corrente viene visualizzato in Livello di dettaglio.

AWS CLI

Esegui il comando seguente per trovare il tuo attuale livello di AWS IoT SiteWise registrazione con. AWS CLI

```
aws iotsitewise describe-logging-options
```

L'operazione restituisce una risposta contenente il livello di registrazione nel formato seguente.

```
{
  "loggingOptions": {
    "level": "String"
  }
}
```

Modifica del livello di registrazione

Utilizzare la procedura seguente per modificare il livello di registrazione nella AWS IoT SiteWise console o in uso. AWS CLI

Console

Per modificare il livello di AWS IoT SiteWise registrazione

1. Passare alla console AWS IoT SiteWise.
2. Nel riquadro di navigazione a sinistra, scegliere Logging options (Opzioni di registrazione).
3. Scegli Modifica.
4. Scegli il livello di verbosità da attivare.
5. Selezionare Salva.

AWS CLI

Esegui il AWS CLI comando seguente per modificare il livello di AWS IoT SiteWise registrazione. Sostituisci *logging-level* con il livello di registrazione desiderato.

```
aws iotsitewise put-logging-options --logging-options level=logging-level
```

Esempio: voci dei file di AWS IoT SiteWise registro

Ogni voce di AWS IoT SiteWise registro include informazioni sull'evento e risorse pertinenti per quell'evento, in modo da poter comprendere e analizzare i dati di registro.

L'esempio seguente mostra una voce CloudWatch Logs che AWS IoT SiteWise registra quando si crea correttamente un modello di asset.

```
{
  "eventTime": "2020-05-05T00:10:22.902Z",
  "logLevel": "INFO",
  "eventType": "AssetModelCreationSuccess",
  "message": "Successfully created asset model.",
  "resources": {
    "assetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE"
  }
}
```

Monitoraggio dei log del gateway SiteWise Edge

Puoi configurare il tuo gateway AWS IoT SiteWise Edge per registrare le informazioni su Amazon CloudWatch Logs o sul file system locale.

Argomenti

- Utilizzo di Amazon CloudWatch Logs
- Utilizzo dei registri di servizio
- Utilizzo dei registri degli eventi

Utilizzo di Amazon CloudWatch Logs

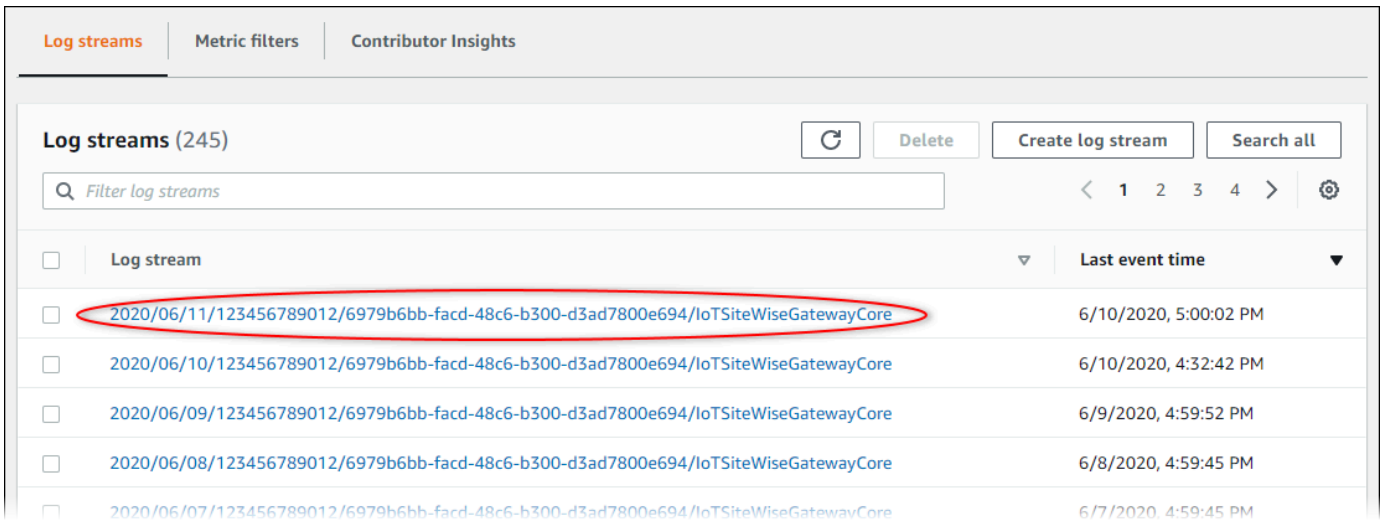
Puoi configurare il tuo gateway SiteWise Edge per inviare log a CloudWatch Logs. Per ulteriori informazioni, consulta Abilitare la registrazione per CloudWatch i registri nella Guida per gli sviluppatori.AWS IoT Greengrass Version 2

Per configurare e accedere ai CloudWatch registri (console)

1. Passare alla console CloudWatch.
2. Nel pannello di navigazione, selezionare Log groups (Gruppi di log).
3. È possibile trovare i registri AWS IoT SiteWise dei componenti nei seguenti gruppi di log:

   - `/aws/greengrass/UserComponent/region/aws.iot.SiteWiseEdgeCollectorOpcua`— I log del componente del gateway SiteWise Edge che raccoglie i dati dalle fonti OPC-UA del gateway SiteWise Edge.
   - `/aws/greengrass/UserComponent/region/aws.iot.SiteWiseEdgePublisher`— I registri del componente del gateway SiteWise Edge su cui pubblica i flussi di dati OPC-UA. AWS IoT SiteWise

   Scegliere il gruppo di log per il debug della funzione.
4. Scegliete un flusso di log il cui nome termini con il nome del gruppo. AWS IoT Greengrass Per impostazione predefinita, CloudWatch visualizza per primo il flusso di log più recente.



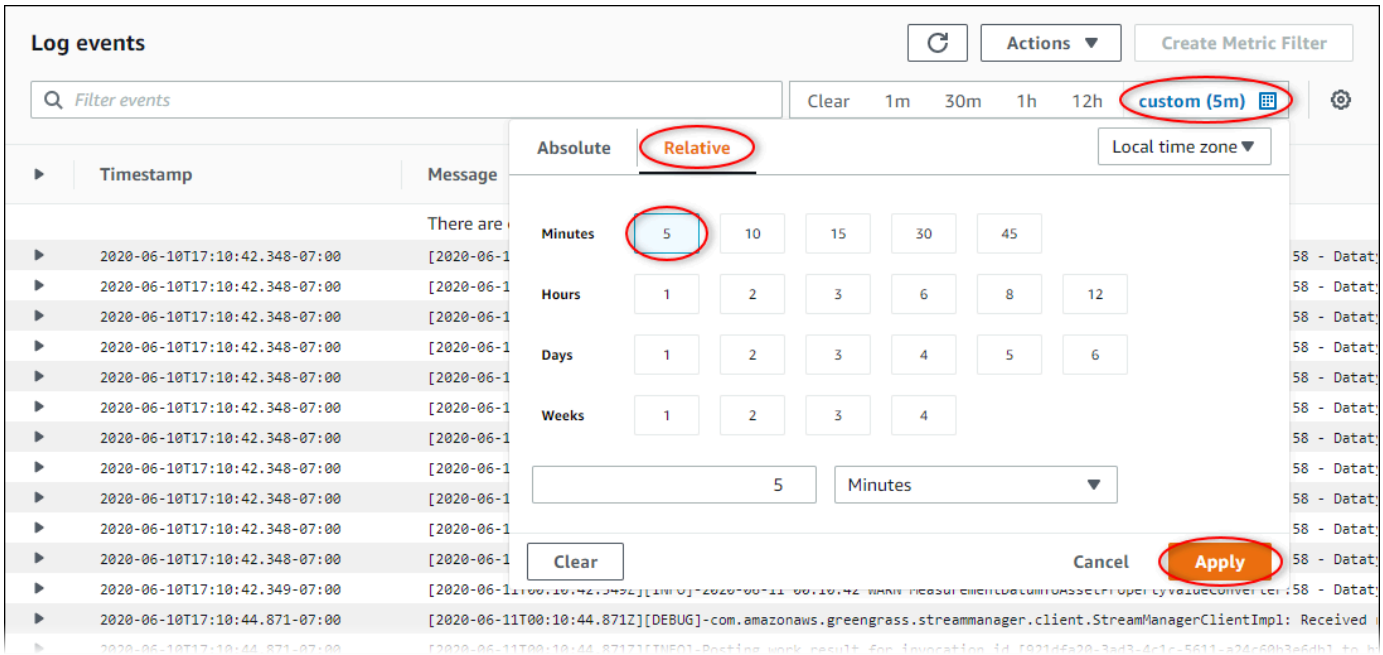
5. Per visualizzare i log degli ultimi 5 minuti, effettua le seguenti operazioni:

   a. Scegli custom (personalizzato) nell'angolo in alto a destra.

b. Scegli Relative (Relativo).

c. Scegli 5 minuti.

d. Scegli Applica.



6. (Facoltativo) Per visualizzare meno log, è possibile scegliere 1m nell'angolo in alto a destra.

7. Scorrere verso il basso l'elenco delle voci di log per visualizzare le più recenti.

Utilizzo dei registri di servizio

SiteWise I dispositivi Edge Gateway includono file di registro dei servizi per facilitare il debug dei problemi. Le seguenti sezioni ti aiuteranno a trovare e utilizzare i file di registro del servizio per i componenti AWS IoT SiteWise OPC-UA Collector e Publisher. AWS IoT SiteWise

AWS IoT SiteWise File di registro del servizio OPC-UA Collector

Il componente AWS IoT SiteWise OPC-UA Collector utilizza il seguente file di registro.

Linux

```
/greengrass/v2/logs/aws.iot.SiteWiseEdgeCollectorOpcua.log
```

Windows

```
C:\greengrass\v2\logs\aws.iot.SiteWiseEdgeCollectorOpcua.log
```

Per visualizzare i log di questo componente

- Esegui il seguente comando sul dispositivo principale per visualizzare il file di registro di questo componente in tempo reale. Sostituisci */greengrass/v2* o *C:\greengrass\v2* con il percorso della cartella AWS IoT Greengrass principale.

  Linux

  ```
  sudo tail -f /greengrass/v2/logs/aws.iot.SiteWiseEdgeCollectorOpcua.log
  ```

  Windows (PowerShell)

  ```
  Get-Content C:\greengrass\v2\logs\aws.iot.SiteWiseEdgeCollectorOpcua.log -Tail
   10 -Wait
  ```

AWS IoT SiteWise File di registro del servizio Publisher

Il componente AWS IoT SiteWise Publisher utilizza il seguente file di registro.

Linux

```
/greengrass/v2/logs/aws.iot.SiteWiseEdgePublisher.log
```

Windows

```
C:\greengrass\v2\logs\aws.iot.SiteWiseEdgePublisher.log
```

Per visualizzare i registri di questo componente

- Esegui il seguente comando sul dispositivo principale per visualizzare il file di registro di questo componente in tempo reale. Sostituisci */greengrass/v2* o *C:\greengrass\v2* con il percorso della cartella AWS IoT Greengrass principale.

Linux

```
sudo tail -f /greengrass/v2/logs/aws.iot.SiteWiseEdgePublisher.log
```

Windows (PowerShell)

```
Get-Content C:\greengrass\v2\logs\aws.iot.SiteWiseEdgePublisher.log -Tail 10 -
Wait
```

Utilizzo dei registri degli eventi

SiteWise I dispositivi Edge Gateway includono file di registro degli eventi per facilitare il debug dei problemi. Le seguenti sezioni ti aiuteranno a trovare e utilizzare i file di registro degli eventi per i componenti AWS IoT SiteWise OPC-UA Collector e Publisher. AWS IoT SiteWise

AWS IoT SiteWise Registri degli eventi di OPC-UA Collector

Il componente AWS IoT SiteWise OPC-UA Collector include un registro degli eventi per aiutare i clienti a identificare e risolvere i problemi. Il file di registro è separato dal file di registro locale e si trova nella seguente posizione. Sostituire */greengrass/v2*o *C:\greengrass\v2* con il percorso della cartella AWS IoT Greengrass principale.

Linux

```
/greengrass/v2/work/aws.iot.SiteWiseEdgeCollectorOpcua/logs/
IotSiteWiseOpcUaCollectorEvents.log
```

Windows

```
C:\greengrass\v2\work\aws.iot.SiteWiseEdgeCollectorOpcua\logs
\IotSiteWiseOpcUaCollectorEvents.log
```

Questo registro include informazioni dettagliate e istruzioni per la risoluzione dei problemi. Oltre alla diagnostica, vengono fornite informazioni sulla risoluzione dei problemi, con una descrizione di come risolvere il problema e, a volte, con collegamenti a ulteriori informazioni. Le informazioni diagnostiche includono quanto segue:

- Livello di gravità
- Timestamp
- Informazioni aggiuntive specifiche sull'evento

Example Log di esempio

```
dataSourceConnectionSuccess:
  Summary: Successfully connected to OpcUa server
  Level: INFO
  Timestamp: '2023-06-15T21:04:16.303Z'
  Description: Successfully connected to the data source.
  AssociatedMetrics:
  - Name: FetchedDataStreams
    Description: The number of fetched data streams for this data source
    Value: 1.0
    Namespace: IoTSiteWise
    Dimensions:
    - Name: SourceName
      Value: SourceName{value=OPC-UA Server}
    - Name: ThingName
      Value: test-core
  AssociatedData:
  - Name: DataSourceTrace
    Description: Name of the data source
    Data:
    - OPC-UA Server
  - Name: EndpointUri
    Description: The endpoint to which the connection was attempted.
    Data:
    - '"opc.tcp://10.0.0.1:1234"'
```

AWS IoT SiteWise Registri degli eventi di Publisher

Il componente AWS IoT SiteWise Publisher include un registro degli eventi per aiutare i clienti a identificare e risolvere i problemi. Il file di registro è separato dal file di registro locale e si trova nella seguente posizione. Sostituire */greengrass/v2*o *C:\greengrass\v2* con il percorso della cartella AWS IoT Greengrass principale.

Linux

```
/greengrass/v2/work/aws.iot.SiteWiseEdgePublisher/logs/
IotSiteWisePublisherEvents.log
```

Windows

```
C:\greengrass\v2\work\aws.iot.SiteWiseEdgePublisher\logs
\IotSiteWisePublisherEvents.log
```

Questo registro include informazioni dettagliate e istruzioni per la risoluzione dei problemi. Oltre alla diagnostica, vengono fornite informazioni sulla risoluzione dei problemi, con una descrizione di come risolvere il problema e, a volte, con collegamenti a ulteriori informazioni. Le informazioni diagnostiche includono quanto segue:

- Livello di gravità
- Timestamp
- Informazioni aggiuntive specifiche sull'evento

Example Log di esempio

```
accountBeingThrottled:
  Summary: Data upload speed slowed due to quota limits
  Level: WARN
  Timestamp: '2023-06-09T21:30:24.654Z'
  Description: The IoT SiteWise Publisher is limited to the "Rate of data points
 ingested"
    quota for a customers account. See the associated documentation and associated
    metric for the number of requests that were limited for more information. Note
    that this may be temporary and not require any change, although if the issue
 continues
    you may need to request an increase for the mentioned quota.
  FurtherInformation:
  - https://docs.aws.amazon.com/iot-sitewise/latest/userguide/quotas.html
  - https://docs.aws.amazon.com/iot-sitewise/latest/userguide/troubleshooting-
gateway.html#gateway-issue-data-streams
  AssociatedMetrics:
  - Name: TotalErrorCount
    Description: The total number of errors of this type that occurred.
```

```
    Value: 327724.0
  AssociatedData:
  - Name: AggregatePropertyAliases
    Description: The aggregated property aliases of the throttled data.
    FileLocation: /greengrass/v2/work/aws.iot.SiteWiseEdgePublisher/./logs/data/
AggregatePropertyAliases_1686346224654.log
```

Monitoraggio AWS IoT SiteWise con i CloudWatch parametri di Amazon

È possibile monitorare AWS IoT SiteWise l'utilizzo CloudWatch, che raccoglie dati grezzi e li elabora in metriche leggibili e quasi in tempo reale. Queste statistiche vengono conservate per un periodo di 15 mesi, per permettere l'accesso alle informazioni storiche e offrire una prospettiva migliore sulle prestazioni del servizio o dell'applicazione web. È anche possibile impostare allarmi che controllano determinate soglie e inviare notifiche o intraprendere azioni quando queste soglie vengono raggiunte. Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.

AWS IoT SiteWise pubblica le metriche e le dimensioni elencate nelle sezioni seguenti nel namespace. `AWS/IoTSiteWise`

> **Tip**
>
> AWS IoT SiteWise pubblica le metriche a intervalli di un minuto. Quando visualizzi queste metriche nei grafici nella CloudWatch console, ti consigliamo di scegliere un periodo di 1 minuto. In questo modo puoi visualizzare la risoluzione massima disponibile dei dati di parametro.

Argomenti

AWS IoT Greengrass Version 2 metriche del gateway

AWS IoT SiteWise pubblica le seguenti metriche del gateway SiteWise Edge. Tutte le metriche del gateway SiteWise Edge vengono pubblicate a intervalli di un minuto.

SiteWise Metriche del gateway Edge

Parametro	Descrizione
`Gateway.CpuUsage`	L'utilizzo della CPU di un gateway SiteWise Edge. Unità: percentuale Dimensione: nessuna
`Gateway.TotalDiskSpace`	Lo spazio totale su disco di un gateway SiteWise Edge. Unità: byte Dimensione: nessuna
`Gateway.UsedDiskSpace`	Lo spazio su disco utilizzato di un gateway SiteWise Edge. Unità: byte Dimensione: nessuna
`Gateway.AvailableDiskSpace`	Lo spazio su disco disponibile di un gateway SiteWise Edge. Unità: byte Dimensione: nessuna
`Gateway.UsedPercentageDiskSpace`	La percentuale di spazio su disco utilizzata di un gateway SiteWise Edge. Unità: byte Dimensione: nessuna
`Gateway.TotalMemory`	La memoria totale di un gateway SiteWise Edge.

Parametro	Descrizione
	Unità: byte Dimensione: nessuna
`Gateway.UsedMemory`	La memoria utilizzata di un gateway SiteWise Edge. Unità: byte Dimensione: nessuna
`Gateway.AvailableMemory`	La memoria disponibile di un gateway SiteWise Edge. Unità: byte Dimensione: nessuna
`Gateway.UsedPercentageMemory`	La percentuale di memoria utilizzata di un gateway SiteWise Edge. Unità: byte Dimensione: nessuna
`Gateway.CloudConnectivity`	Lo stato della connettività cloud di un gateway SiteWise Edge. Unità: nessuna Dimensione: GatewayId
`Gateway.SWE.Component.RunningStatus`	Lo stato di funzionamento dei componenti su un gateway SiteWise Edge. Unità: nessuna Dimensione: GatewayId

Metriche del collettore OPC-UA

Parametro	Descrizione
`OpcUaCollector.Heartbeat`	Generato ogni minuto per ogni sorgente OPC-UA (`sourceName`) connessa a un gateway Edge (). SiteWise `gatewayId` Unità: Numero (1 che rappresenta la sorgente è connessa e 0 che rappresenta la sorgente è disconnessa). Dimensioni: GatewayId, SourceName
`OpcUaCollector.ActiveDataStreamCount`	Il numero di flussi di dati a cui un gateway SiteWise Edge (`gatewayId`) si è abbonato per una fonte OPC-UA (). `sourceName` Unità: numero Dimensioni:,, GatewayId SourceName PropertyGroup
`OpcUaCollector.IncomingValuesCount`	Il numero di punti dati che un gateway SiteWise Edge (`gatewayId`) ha ricevuto per una fonte OPC-UA (`sourceName`), generato ogni minuto. Unità: numero Dimensioni: GatewayId,, SourceName PropertyGroup
`OpcUaCollector.IncomingValuesError`	Il numero di punti dati che un gateway SiteWise Edge (`gatewayId`) riceve da una fonte OPC-UA (`sourceName`) che non sono valori validi. Questi punti dati non vengono acquisiti dal OpcUa Collector, generati ogni minuto. Unità: numero

Parametro	Descrizione
	Dimensioni:,, GatewayId SourceName PropertyGroup
`OpcUaCollector.ConversionErrors`	Il numero di punti dati che un gateway SiteWise Edge (`gatewayId`) ha ricevuto per una fonte OPC-UA (`sourceName`) che ha provocato errori di conversione durante l'invio dei dati a. AWS IoT SiteWise Questi punti dati non verranno acquisiti da Collector. OpcUa Unità: numero Dimensioni:, GatewayId SourceName

AWS IoT SiteWise metriche degli editori

Parametro	Descrizione
`IoTSiteWisePublisher.Heartbeat`	Generato ogni minuto dal gateway Publisher in the SiteWise Edge. Unità: 1 (1 che rappresenta Publisher è in esecuzione e manca il punto dati che rappresenta Publisher non è in esecuzione). Dimensioni: GatewayId
`IoTSiteWisePublisher.PublishSuccessCount`	Il numero di punti dati che un gateway SiteWise Edge (`GatewayId`) ha pubblicato con successo sul cloud, generato ogni minuto. Unità: numero Dimensioni: GatewayId
`IoTSiteWisePublisher.PublishFailureCount`	Il numero di punti dati che un gateway SiteWise Edge (`GatewayId`) non è riuscito a pubblicare, generato ogni minuto.

Parametro	Descrizione
	Unità: numero Dimensioni: GatewayId
`IoTSiteWisePublisher.PublishRejectedCount`	Il numero di punti dati che un gateway SiteWise Edge (`GatewayId `) ha rifiutato dal lato cloud, generato ogni minuto. Unità: numero Dimensioni: GatewayId
`IoTSiteWisePublisher.DroppedCount`	Il numero di punti dati che vengono eliminati da un gateway SiteWise Edge (`GatewayId `) e non pubblicati sul cloud, generati ogni minuto. Unità: numero Dimensioni: GatewayId

AWS IoT Greengrass Version 1 metriche del gateway

AWS IoT SiteWise pubblica le seguenti metriche del gateway SiteWise Edge. Tutte le metriche del gateway SiteWise Edge vengono pubblicate a intervalli di un minuto.

> **Important**
>
> Per ricevere i parametri del gateway SiteWise Edge, è necessario utilizzare almeno la versione 6 del AWS IoT SiteWise connettore sul SiteWise gateway Edge. Per ulteriori informazioni, consulta AWS IoT SiteWise OPC-UA Collector nella Developer Guide.AWS IoT Greengrass Version 1

SiteWise Metriche del gateway Edge

Parametro	Descrizione
`Gateway.Heartbeat`	Generato ogni minuto per ogni gateway SiteWise Edge (`gatewayId`) connesso. Unità: 1 (1 che rappresenta il gateway SiteWise Edge è attivo e manca il datapoint che rappresenta il gateway SiteWise Edge viene disconnesso dal cloud). Dimensione: GatewayId
`Gateway.PublishSuccessCount`	Il numero di punti dati che un gateway SiteWise Edge (`gatewayId`) ha pubblicato con successo. Unità: numero Dimensione: GatewayId
`Gateway.PublishFailureCount`	Il numero di punti dati che un gateway SiteWise Edge (`gatewayId`) non è riuscito a pubblicar e. Questa metrica conta gli errori derivanti dalle chiamate del gateway SiteWise Edge all'BatchPutAssetPropertyValueoperazion e. Per ulteriori informazioni sulla risoluzio ne dei problemi dei gateway SiteWise Edge, consulta. Risoluzione dei problemi di un gateway SiteWise Edge Unità: numero Dimensione: GatewayId
`Gateway.ProcessFailureCount`	Il numero di punti dati che un gateway SiteWise Edge (`gatewayId`) non è riuscito a elaborare.

Parametro	Descrizione
	Questa metrica conta gli errori che si verifican o tra il gateway SiteWise Edge e le sorgenti del gateway SiteWise Edge, inclusi gli errori segnalati dalle fonti. Per ulteriori informazi oni sulla risoluzione dei problemi dei gateway SiteWise Edge, consulta. Risoluzione dei problemi di un gateway SiteWise Edge Unità: numero Dimensione: GatewayId
`Gateway.PublishRejectedCount`	Il numero di punti dati provenienti da un gateway SiteWise Edge (`gatewayId`) che vengono rifiutati. Unità: numero Dimensione: GatewayId

Metriche relative all'OPC-UA

Parametro	Descrizione
`OPCUACollector.Heartbeat`	Generato ogni minuto per ogni sorgente OPC-UA (`sourceName`) connessa a un SiteWise gateway Edge (). `gatewayId` Unità: Numero (1 che rappresenta la sorgente è connessa e 0 che rappresenta la sorgente è disconnessa). Dimensioni: GatewayId, SourceName
`OPCUACollector.ActiveDataSt reamCount`	Il numero di flussi di dati a cui un gateway SiteWise Edge (`gatewayId`) si è abbonato per una fonte OPC-UA (). `sourceName`

Parametro	Descrizione
	Unità: numero Dimensioni:,, GatewayId SourceName PropertyGroup
`OpcUaCollector.IncomingValuesCount`	Il numero di punti dati che un gateway SiteWise Edge (`gatewayId`) ha ricevuto per una fonte OPC-UA (`sourceName`), generato ogni minuto. Unità: numero Dimensioni: GatewayId,, SourceName PropertyGroup
`OpcUaCollector.IncomingValuesError`	Il numero di punti dati che un gateway SiteWise Edge (`gatewayId`) ha ricevuto da una fonte OPC-UA (`sourceName`) che non sono valori validi. Questi punti dati non verranno acquisiti dal OpcUa Collector, generati ogni minuto. Unità: numero Dimensioni:,, GatewayId SourceName PropertyGroup
`OpcUaCollector.ConversionErrors`	Il numero di punti dati che un gateway SiteWise Edge (`gatewayId`) ha ricevuto per una fonte OPC-UA (`sourceName`) che ha provocato errori di conversione durante l'invio dei dati a. AWS IoT SiteWise Questi punti dati non verranno acquisiti da Collector. OpcUa Unità: numero Dimensioni:, GatewayId SourceName

Metriche relative all'EIP

Parametro	Descrizione
`EIPCollector.Heartbeat`	Generato ogni minuto per ogni sorgente EIP (`sourceName`) connessa a un gateway SiteWise Edge (). `gatewayId` Unità: 1 (1 che rappresenta la sorgente è connessa e manca il datapoint che rappresenta la sorgente viene disconnesso.) GatewayIdDimensioni:, SourceName
`EIPCollector.IncomingValuesCount`	Il numero di flussi di dati a cui è sottoscritto un gateway SiteWise Edge (`gatewayId`) per un'origine EIP (). `sourceName` Unità: numero Dimensioni:, GatewayId SourceName
`EIPCollector.ActiveDataStreamCount`	Il numero di punti dati che un gateway SiteWise Edge (`gatewayId`) ha ricevuto per un'origine EIP (`sourceName`). Unità: numero Dimensioni: GatewayId, SourceName

Metriche relative a Modbus

Parametro	Descrizione
`ModbusTCPCollector.Heartbeat`	Generato ogni minuto per ogni sorgente Modbus (`sourceName`) connessa a un gateway SiteWise Edge (). `gatewayId`

Parametro	Descrizione
	Unità: 1 (1 che rappresenta la sorgente Modbus è connessa e manca il datapoint che rappresen ta la sorgente viene disconnesso.) GatewayIdDimensioni:, SourceName
`ModbusTCPCollector.Incoming ValuesCount`	Il numero di flussi di dati a cui è sottoscritto un gateway SiteWise Edge (`gatewayId`) per una sorgente Modbus (). `sourceName` Unità: numero Dimensioni:, GatewayId SourceName
`ModbusTCPCollector.ActiveDa taStreamCount`	Il numero di punti dati che un gateway SiteWise Edge (`gatewayId`) ha ricevuto per una sorgente Modbus (`sourceName`). Unità: numero Dimensioni: GatewayId, SourceName

Registrazione delle chiamate AWS IoT SiteWise API con AWS CloudTrail

AWS IoT SiteWise è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o AWS servizio in AWS IoT SiteWise. CloudTrail acquisisce le chiamate API AWS IoT SiteWise come eventi. Le chiamate acquisite includono chiamate dalla AWS IoT SiteWise console e chiamate di codice alle operazioni AWS IoT SiteWise API. Se crei un trail, puoi attivare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per. AWS IoT SiteWise Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare a quale richiesta è stata inviata AWS IoT SiteWise, l'indirizzo IP da cui è stata effettuata, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni in merito CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

AWS IoT SiteWise informazioni in CloudTrail

CloudTrail viene attivato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività di evento supportata in AWS IoT SiteWise, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nel tuo AWS account. Per ulteriori informazioni, consulta Visualizzazione degli eventi con cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi di AWS IoT SiteWise, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando crei un percorso nella console, il percorso si applica a tutte le AWS regioni. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

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

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 credenziali utente root o AWS Identity and Access Management (IAM).
- 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 AWS servizio.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

AWS IoT SiteWise eventi di dati in CloudTrail

Gli eventi di dati forniscono informazioni sulle operazioni delle risorse eseguite su o in una risorsa (ad esempio, lettura o scrittura su un oggetto Amazon S3). Queste operazioni sono definite anche

operazioni del piano dei dati. Gli eventi di dati sono spesso attività che interessano volumi elevati di dati. Per impostazione predefinita, CloudTrail non registra gli eventi relativi ai dati. La cronologia CloudTrail degli eventi non registra gli eventi relativi ai dati.

Per gli eventi di dati sono previsti costi aggiuntivi. Per ulteriori informazioni sui CloudTrail prezzi, consulta la sezione AWS CloudTrail Prezzi.

Puoi registrare gli eventi relativi ai dati per i tipi di AWS IoT SiteWise risorse utilizzando la CloudTrail console o AWS CLI le operazioni CloudTrail dell'API. La tabella in questa sezione mostra i tipi di risorse disponibili per AWS IoT SiteWise.

- Per registrare gli eventi relativi ai dati utilizzando la CloudTrail console, crea un percorso o un data store di eventi per registrare gli eventi di dati oppure aggiorna un trail o un data store di eventi esistente per registrare gli eventi di dati.

  1. Scegli Data events per registrare gli eventi relativi ai dati.
  2. Dall'elenco Tipo di evento Data, scegli il tipo di risorsa per il quale desideri registrare gli eventi relativi ai dati.
  3. Scegli il modello di selettore di registro che desideri utilizzare. Puoi registrare tutti gli eventi relativi ai dati per il tipo di risorsa, registrare tutti `readOnly` gli eventi, registrare tutti `writeOnly` gli eventi o creare un modello di selettore di registro personalizzato per filtrare i `readOnly` campi`eventName`, `eresources.ARN`.
- Per registrare gli eventi relativi ai dati utilizzando il AWS CLI, configura il `--advanced-event-selectors` parametro in modo che il `eventCategory` campo sia uguale `Data` e il `resources.type` campo uguale al valore del tipo di risorsa (vedi tabella). È possibile aggiungere condizioni per filtrare i valori dei `resources.ARN` campi `readOnly`e`eventName`, e.
  - Per configurare un percorso per registrare gli eventi relativi ai dati, esegui il AWS CloudTrail put-event-selectorscomando. Per ulteriori informazioni, vedere Registrazione degli eventi relativi ai dati per i AWS CLI sentieri con.
  - Per configurare un Event Data Store per registrare gli eventi di dati, esegui il AWS CloudTrail create-event-data-storecomando per creare un nuovo Event Data Store per registrare gli eventi di dati oppure esegui il AWS CloudTrail update-event-data-storecomando per aggiornare un Event Data Store esistente. Per ulteriori informazioni, vedere Registrazione degli eventi di dati per i data store di eventi con. AWS CLI

La tabella seguente elenca i tipi di AWS IoT SiteWise risorse. La colonna Data event type (console) mostra il valore da scegliere dall'elenco Data event type sulla CloudTrail console. La colonna del

valore resources.type mostra il `resources.type` valore da specificare durante la configurazione dei selettori di eventi avanzati utilizzando le API o. AWS CLI CloudTrail La CloudTrail colonna Data API loggate mostra le chiamate API registrate per il tipo di risorsa. CloudTrail

Tipo di evento di dati (console)	valore resources.type	API di dati registrate su* CloudTrail
AWS IoT SiteWise asset	`AWS::IoTSiteWise::Asset`	• BatchPutAssetPropertyValue • GetAssetPropertyValue • GetAssetPropertyValueHistory • GetAssetPropertyAggregates • GetInterpolatedAssetPropertyValues • BatchGetAssetPropertyValue • BatchGetAssetPropertyValueHistory • BatchGetAssetPropertyAggregates
AWS IoT SiteWise serie temporali	`AWS::IoTSiteWise::TimeSeries`	• BatchPutAssetPropertyValue • GetAssetPropertyValue • GetAssetPropertyValueHistory • GetAssetPropertyAggregates • GetInterpolatedAssetPropertyValues • BatchGetAssetPropertyValue

Tipo di evento di dati (console)	valore resources.type	API di dati registrate su* CloudTrail
		• BatchGetAssetPropertyValueHistory • BatchGetAssetPropertyAggregates

> **Note**
>
> Il resources.type registrato nell'evento Cloudtrail dipende dall'identificatore utilizzato nella richiesta API. Se nella richiesta viene specificato un id di risorsa, viene registrato Asset resources.type, altrimenti viene registrato resources.type. TimeSeries

*Puoi configurare selettori di eventi avanzati per filtrare e `resources.ARN` campi per registrare solo gli `eventName` eventi che ritieni `readOnly` importanti. Per ulteriori informazioni sui campi, consulta AdvancedFieldSelector.

AWS IoT SiteWise gestione degli eventi in CloudTrail

Gli eventi di gestione forniscono informazioni sulle operazioni di gestione eseguite sulle risorse AWS dell'account. Queste operazioni sono definite anche operazioni del piano di controllo (control-plane). Per impostazione predefinita, CloudTrail registra gli eventi di gestione.

AWS IoT SiteWise registra tutte le operazioni AWS IoT SiteWise del piano di controllo come eventi di gestione. Per un elenco delle operazioni del piano di AWS IoT SiteWise controllo a cui si AWS IoT SiteWise effettua l'accesso CloudTrail, consulta l'AWS IoT SiteWise API Reference.

Esempio: voci dei file di AWS IoT SiteWise registro

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'operazione richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia stack ordinata delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che dimostra l'`CreateAsset`operazione.


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::123456789012:user/Administrator",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Administrator",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2020-03-11T17:26:40Z"
      }
    },
    "invokedBy": "signin.amazonaws.com"
  },
  "eventTime": "2020-03-11T18:01:22Z",
  "eventSource": "iotsitewise.amazonaws.com",
  "eventName": "CreateAsset",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.0",
  "userAgent": "signin.amazonaws.com",
  "requestParameters": {
    "assetName": "Wind Turbine 1",
    "assetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
    "clientToken": "a1b2c3d4-5678-90ab-cdef-00000EXAMPLE"
  },
  "responseElements": {
    "assetId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
    "assetArn": "arn:aws:iotsitewise:us-east-1:123456789012:asset/a1b2c3d4-5678-90ab-
cdef-22222EXAMPLE",
    "assetStatus": {
      "state": "CREATING"
    }
  },
  "requestID": "a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE",
  "eventID": "a1b2c3d4-5678-90ab-cdef-bbbbbEXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
```

```
}
```

Taggare le tue risorse AWS IoT SiteWise

L'etichettatura AWS IoT SiteWise delle risorse offre un modo efficace per classificare, gestire e recuperare le risorse organizzative in modo efficiente. Assegnando tag, che consistono in coppie chiave-valore, puoi allegare metadati descrittivi alle tue risorse. I metadati dei tag possono essere utilizzati per semplificare le operazioni. Ad esempio, in uno scenario di parco eolico, i tag consentono di etichettare le turbine con attributi specifici come posizione, capacità e stato operativo, consentendo una rapida identificazione e gestione all'interno. AWS IoT SiteWise

L'integrazione dei tag con le policy AWS Identity and Access Management (IAM) migliora la sicurezza e il controllo operativo definendo regole di accesso condizionale. Ciò significa che puoi specificare che siano ammessi solo gli utenti con determinati tag. Ad esempio, solo le persone etichettate con un determinato ruolo o reparto possono accedere o modificare risorse particolari.

Utilizzo dei tag in AWS IoT SiteWise

Utilizza i tag per classificare le AWS IoT SiteWise risorse in base allo scopo, al proprietario, all'ambiente o a qualsiasi altra classificazione adatta al tuo caso d'uso. In presenza di un numero elevato di risorse, puoi individuare rapidamente una risorsa specifica in base ai suoi tag.

Ogni tag è composto da una chiave e da un valore opzionale specificato dall'utente. Ad esempio, potete stabilire una serie di tag per i vostri modelli di asset per tracciarli in base ai processi industriali che supportano. Si consiglia di sviluppare un set personalizzato di chiavi di tag per ogni tipo di risorsa gestita. L'utilizzo di un set coerente di chiavi di tag può semplificare la gestione delle risorse.

Etichettatura con AWS Management Console

Il Tag Editor di the AWS Management Console fornisce un modo centralizzato e unificato per creare e gestire i tag per le risorse di tutti i AWS servizi. Per ulteriori informazioni, consulta Editor di tag nella Guida per l'utente di AWS Resource Groups .

Etichettatura con l'API AWS IoT SiteWise

L' AWS IoT SiteWise API utilizza anche i tag. Prima di creare i tag, tenere presente le limitazioni relative al tagging. Per ulteriori informazioni, consulta la sezione relativa alle convenzioni di denominazione e utilizzo dei tag nella Riferimenti generali di AWS.

- Per aggiungere i tag durante la creazione di una risorsa, definirli nella proprietà `tags` della risorsa.

- Per aggiungere tag a una risorsa esistente o aggiornare i valori dei tag, utilizzate l'TagResourceoperazione.
- Per rimuovere i tag da una risorsa, usa l'UntagResourceoperazione.
- Per recuperare i tag associati a una risorsa, utilizzate l'ListTagsForResourceoperazione o descrivete la risorsa e controllatene le `tags` proprietà.

La tabella seguente elenca le risorse a cui è possibile etichettare utilizzando l' AWS IoT SiteWise API e le relative `Create` operazioni. `Describe`

Risorse taggabili AWS IoT SiteWise

Risorsa	Creare l'operazione	Descrivere l'operazione
Modello di asset o modello di componente	CreateAssetModel	DescribeAssetModel
Asset	CreateAsset	DescribeAsset
SiteWise Gateway Edge	CreateGateway	DescribeGateway
Portal	CreatePortal	DescribePortal
Progetto	CreateProject	DescribeProject
Dashboard	CreateDashboard	DescribeDashboard
Policy di accesso	CreateAccessPolicy	DescribeAccessPolicy
Serie temporali	BatchPutAssetPropertyValue	DescribeTimeSeries

È `BatchPutAssetPropertyValue` infatti possibile configurare le fonti di dati a cui inviare dati industriali AWS IoT SiteWise prima di creare modelli e asset. AWS IoT SiteWise crea automaticamente flussi di dati per ricevere flussi di dati grezzi dalle apparecchiature. Per ulteriori informazioni, vedere Gestione dell'ingestione dei dati.

Utilizza le operazioni seguenti per elencare e gestire i tag per le risorse che supportano il tagging:

- TagResource— Aggiunge tag a una risorsa o aggiorna il valore di un tag esistente.
- ListTagsForResource— Elenca i tag di una risorsa.

- UntagResource— Rimuove i tag da una risorsa.

Aggiungi o rimuovi tag da una risorsa in qualsiasi momento. Per aggiornare il valore di una chiave di tag esistente, aggiungi un nuovo tag con la stessa chiave e il nuovo valore desiderato alla risorsa. Questa azione sostituisce il vecchio valore con quello nuovo. Sebbene sia possibile assegnare una stringa vuota come valore di tag, non è possibile assegnare un valore nullo.

L'eliminazione di una risorsa rimuove anche tutti i tag ad essa collegati.

Utilizzo dei tag con policy IAM

Utilizza i tag delle risorse nelle tue policy IAM per controllare l'accesso e le autorizzazioni degli utenti. Ad esempio, le policy possono consentire agli utenti di creare solo risorse a cui è associato un tag specifico. Le policy possono anche limitare gli utenti nella creazione o nella modifica di risorse con determinati tag.

> **Note**
>
> Se utilizzi tag per consentire o rifiutare agli utenti di accedere alle risorse, devi negare agli utenti la possibilità di aggiungere o rimuovere tali tag dalle stesse risorse. Altrimenti, un utente potrebbe aggirare le tue restrizioni e accedere a una risorsa modificandone i tag.

Puoi utilizzare le chiavi di contesto della condizione e i valori riportati di seguito nell'elemento `Condition` (denominato anche blocco `Condition`) di una dichiarazione di policy.

`aws:ResourceTag/`*`tag-key`*`: `*`tag-value`*

Consentire o negare agli utenti operazioni su risorse con tag specifici.

`aws:RequestTag/`*`tag-key`*`: `*`tag-value`*

Richiedere che un tag specifico venga utilizzato (o non utilizzato) durante la creazione o la modifica di una risorsa compatibile con l'applicazione dei tag.

`aws:TagKeys: [`*`tag-key`*`, ...]`

Richiedere che un set di chiavi di tag specifico venga utilizzato (o non utilizzato) durante la creazione o la modifica di una risorsa compatibile con l'applicazione dei tag.

> **Note**
>
> Le chiavi e i valori del contesto della condizione in una policy IAM si applicano solo alle azioni che hanno una risorsa taggabile come parametro obbligatorio. Ad esempio, puoi impostare l'accesso condizionale basato su tag per. ListAssets Non puoi attivare l'accesso condizionale basato su tag PutLoggingOptionsperché nella richiesta non viene fatto riferimento a nessuna risorsa taggabile.

Per ulteriori informazioni, consulta Controllare l'accesso alle AWS risorse utilizzando i tag di risorsa e il riferimento alla policy IAM JSON nella IAM User Guide.

Esempi di politiche IAM che utilizzano i tag

- Visualizzazione di asset AWS IoT SiteWise in base ai tag

Risoluzione dei problemi AWS IoT SiteWise

Utilizza le informazioni contenute in queste sezioni per risolvere i problemi relativi a. AWS IoT SiteWise

Argomenti

Risoluzione dei problemi relativi alle operazioni di importazione ed esportazione in blocco

Per gestire e diagnosticare gli errori prodotti durante un processo di trasferimento, consulta l' AWS IoT TwinMaker GetMetadataTransferJobAPI:

1. Dopo aver creato ed eseguito un processo di trasferimento, chiama l'GetMetadataTransferJobAPI:

```
aws iottwinmaker get-metadata-transfer-job \
--metadata-transfer-job-id your_metadata_transfer_job_id \
--region us-east-1
```

2. Lo stato del lavoro cambia in uno dei seguenti stati:
   - COMPLETED
   - CANCELLED
   - ERRORE
3. L'GetMetadataTransferJobAPI restituisce un MetadataTransferJobProgressoggetto.
4. L'MetadataTransferJobProgressoggetto contiene i seguenti parametri:
   - FailedCount: indica il numero di asset che hanno avuto esito negativo durante il processo di trasferimento.

- SkippedCount: indica il numero di asset che sono stati ignorati durante il processo di trasferimento.
- successeededCount: indica il numero di asset che hanno avuto successo durante il processo di trasferimento.
- totalCount: indica il numero totale di asset coinvolti nel processo di trasferimento.

5. Inoltre, la chiamata API restituisce un elemento reportURL, che contiene un URL prefirmato. Se il processo di trasferimento presenta errori che richiedono un'analisi, puoi scaricare un rapporto di errore completo a questo URL.

Risoluzione dei problemi relativi a un AWS IoT SiteWise portale

Risolvi i problemi più comuni con i tuoi AWS IoT SiteWise portali.

Gli utenti e gli amministratori non possono accedere al portale AWS IoT SiteWise

Se gli utenti o gli amministratori non possono accedere AWS IoT SiteWise al tuo portale, potresti avere autorizzazioni limitate nelle policy allegate AWS Identity and Access Management (IAM) che impediscono il successo degli accessi.

Guarda i seguenti esempi di politiche IAM che comporteranno errori di accesso:

> **Note**
>
> Qualsiasi policy IAM allegata che includa un `"Condition"` elemento causerà un errore di accesso.

Esempio 1: la condizione qui è un IP limitato e ciò causerà un errore di accesso.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iotsitewise:DescribePortal"
```

```
            ],
            "Resource": "*",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": [
                        "REPLACESAMPLEIP"
                    ]
                }
            }
        }
    ]
}
```

Esempio 2: la condizione qui è un tag incluso e ciò causerà un errore di accesso.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iotsitewise:DescribePortal"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/project": "*"
                }
            }
        }
    ]
}
```

Quando aggiungi utenti o amministratori al portale, evita di creare policy IAM che limitino le autorizzazioni degli utenti, come l'IP limitato. Qualsiasi policy allegata con autorizzazioni limitate non sarà in grado di connettersi al portale. AWS IoT SiteWise

Risoluzione dei problemi di un gateway SiteWise Edge

AWS IoT SiteWise Gli edge gateway eseguono un set di componenti. AWS IoT Greengrass Puoi configurare il tuo gateway SiteWise Edge per registrare gli eventi del connettore su Amazon

CloudWatch e sul file system locale del tuo gateway SiteWise Edge. Quindi, puoi visualizzare i file di registro associati al connettore per risolvere i problemi relativi al gateway SiteWise Edge.

È inoltre possibile visualizzare le CloudWatch metriche riportate dai gateway SiteWise Edge per risolvere problemi di connettività o flussi di dati. Per ulteriori informazioni, consulta AWS IoT Greengrass Version 1 metriche del gateway.

Argomenti

- Configurazione e accesso ai log del gateway Edge SiteWise
- Risoluzione dei problemi relativi SiteWise al gateway Edge
- Risoluzione dei AWS IoT Greengrass problemi

Configurazione e accesso ai log del gateway Edge SiteWise

Prima di poter visualizzare i log del gateway SiteWise Edge, devi configurare il gateway SiteWise Edge per inviare i log ad Amazon CloudWatch Logs o archiviare i log sul file system locale.

- Usa CloudWatch Logs se desideri utilizzare il per visualizzare i file di log del AWS Management Console tuo gateway SiteWise Edge. Per ulteriori informazioni, consulta Utilizzo di Amazon CloudWatch Logs.
- Utilizza i log del file system locale se desideri utilizzare la riga di comando o il software locale per visualizzare i file di registro del gateway SiteWise Edge. Per ulteriori informazioni, consulta Utilizzo dei registri di servizio.

Risoluzione dei problemi relativi SiteWise al gateway Edge

Utilizza le seguenti informazioni per risolvere i problemi relativi al gateway SiteWise Edge.

Problemi

- Impossibile distribuire i pacchetti sui gateway Edge SiteWise
- Le sorgenti Modbus TCP non sono sincronizzate
- Impossibile connettersi allo stream manager
- Impossibile connettersi a una sorgente OPC-UA
- AWS IoT SiteWise non riceve dati dai server OPC-UA
- Nessun dato è stato visualizzato nel pannello di controllo

- «Impossibile trovare o caricare la classe principale» visualizzato in aws.iot. SiteWiseEdgePublisher registra l'errore /greengrass/v2/logs

Impossibile distribuire i pacchetti sui gateway Edge SiteWise

Se il componente AWS IoT Greengrass nucleus (`aws.greengrass.Nucleus`) non è aggiornato, potresti non essere in grado di distribuire i pacchetti sul tuo gateway Edge. SiteWise Puoi usare la AWS IoT Greengrass V2 console per aggiornare il componente AWS IoT Greengrass nucleus.

Aggiorna il componente AWS IoT Greengrass nucleus (console)

1. Passare alla console AWS IoT Greengrass.
2. Nel riquadro di navigazione, sotto AWS IoT Greengrass, scegli Distribuzioni.
3. Nell'elenco Distribuzioni, seleziona la distribuzione che desideri modificare.
4. Scegli Rivedi.
5. Nella pagina Specificare la destinazione, scegli Avanti.
6. Nella pagina Seleziona componenti, in Componenti pubblici, nella casella di ricerca**`aws.greengrass.Nucleus`**, inserisci e quindi seleziona AWS.GreenGrass.Nucleus.
7. Seleziona Avanti.
8. Nella pagina Configura componenti, scegli Avanti.
9. Nella pagina Configura impostazioni avanzate, scegli Avanti.
10. Nella pagina Review (Verifica), scegli Deploy (Distribuisci).

Le sorgenti Modbus TCP non sono sincronizzate

La tua sorgente Modbus TCP potrebbe non essere sincronizzata se il tipo di dati di origine è ASCII, UTF8 o ISO8859 e stai utilizzando una vecchia versione del connettore Modbus-TCP Protocol Adapter. Per aggiornare il connettore alla versione più recente, procedi come segue:

1. Accedi alla console AWS IoT Greengrass V1.
2. Nel riquadro di navigazione, selezionare Groups (Gruppi).
3. In AWS IoT Greengrass Gruppi, scegli il gruppo target.
4. Nel riquadro di navigazione, scegli Connettori.
5. Nella colonna Aggiornamento, scegli Disponibile.

6. Nella pagina Upgrade connector, scegli la versione più recente, quindi scegli Aggiorna.

Per ulteriori informazioni, consulta il connettore Modbus-TCP Protocol Adapter nella Developer Guide. AWS IoT Greengrass Version 1

Impossibile connettersi allo stream manager

Potresti visualizzare il seguente messaggio `swPublisher` di registro degli errori se lo stream manager non è abilitato nel AWS IoT Greengrass gruppo del gateway SiteWise Edge.

```
com.amazonaws.greengrass.streammanager.client.StreamManagerClientImpl: Connect failed
```

A partire dalla versione 6, il AWS IoT SiteWise connettore richiede lo stream manager. Per ulteriori informazioni su come abilitare lo stream manager, consulta il passaggio 5 diConfigurazione di un gruppo AWS IoT Greengrass.

Impossibile connettersi a una sorgente OPC-UA

Potresti visualizzare il seguente messaggio di registro `OPCUACollector` degli errori se la versione di OpenJDK installata non è supportata.

```
java.security.KeyStoreException: Key protection  algorithm not found:
 java.security.UnrecoverableKeyException: Encrypt Private Key failed: unrecognized
 algorithm name: PBEWithSHA1AndDESede
          Failed to start OPC-UA Connection for Source 'Server 1': Failed to add key to
 store
```

Per effettuare il downgrade alla versione OpenJDK supportata, segui i passaggi in questa sezione. Questi passaggi presuppongono l'utilizzo di un dispositivo con Ubuntu. Se utilizzi una distribuzione Linux diversa, consulta la documentazione pertinente per il tuo dispositivo.

Per effettuare il downgrade al supporto Amazon Corretto 8

1. Per disinstallare l'attuale OpenJDK, esegui uno dei seguenti comandi.

   - ```
     sudo apt purge -y openjdk-8-jre-headless
     ```
   - ```
     sudo apt-get purge -y java-1.8.0-amazon-corretto-jdk
     ```

2. Per scaricare e installare il supporto di Amazon Corretto 8, esegui il comando seguente.

```
curl -s https://corretto.aws/downloads/resources/8.282.08.1/java-1.8.0-amazon-
corretto-jdk_8.282.08-1_amd64.deb --output /tmp/java-1.8.0-amazon-corretto-
jdk_8.282.08-1_amd64.deb
sudo apt-get update && sudo apt-get install java-common
sudo dpkg --install /tmp/java-1.8.0-amazon-corretto-jdk_8.282.08-1_amd64.deb
```

3. Per riavviare il software AWS IoT Greengrass V1 Core, esegui il comando seguente.

```
sudo /greengrass/ggc/core/greengrassd restart
```

AWS IoT SiteWise non riceve dati dai server OPC-UA

Se le tue AWS IoT SiteWise risorse non ricevono i dati inviati dai tuoi server OPC-UA, puoi cercare nei log del tuo gateway SiteWise Edge per risolvere i problemi. Cerca i log a livello di informazioni che contengono il seguente `swPublisher` messaggio.

```
Emitting diagnostic name=PublishError.SomeException
```

*`SomeException`*In base al tipo di registro, utilizza i seguenti tipi di eccezione e i problemi corrispondenti per risolvere i problemi del gateway Edge: SiteWise

- ResourceNotFoundException— I server OPC-UA inviano dati che non corrispondono a un alias di proprietà per nessuna risorsa. Questa eccezione può verificarsi in due casi:
  - Gli alias di proprietà non corrispondono esattamente alle variabili OPC-UA, incluso qualsiasi prefisso sorgente definito. Verificare che gli alias delle proprietà e i prefissi di origine siano corretti.
  - Non sono state mappate le variabili OPC-UA alle proprietà delle risorse. Per ulteriori informazioni, consulta Mappatura dei flussi di dati industriali alle proprietà degli asset.

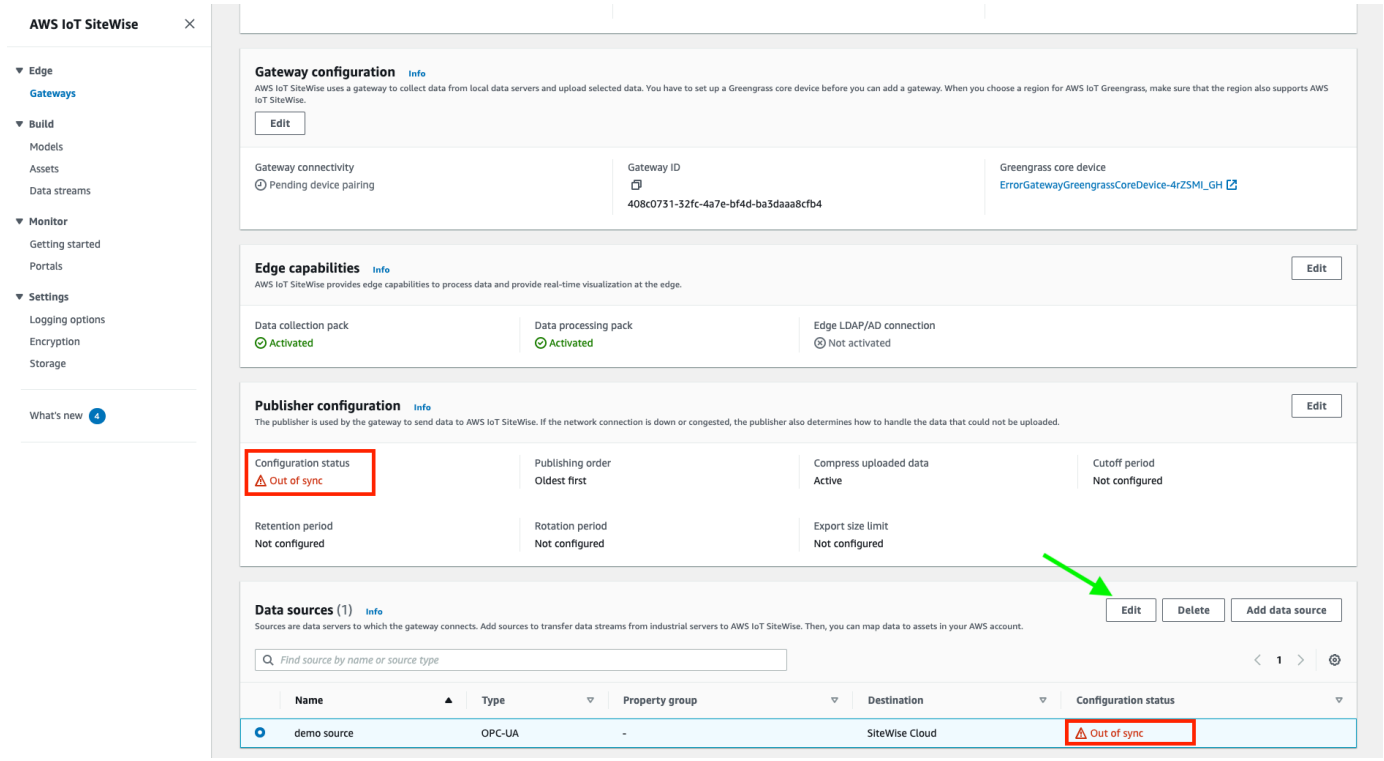
    Se hai già mappato tutte le variabili OPC-UA che desideri inserire AWS IoT SiteWise, puoi filtrare le variabili OPC-UA inviate dal gateway Edge. SiteWise Per ulteriori informazioni, consulta Utilizzo dei filtri dei nodi OPC-UA.
- AccessDeniedException— Il AWS IoT Greengrass gruppo del gateway SiteWise Edge non dispone di autorizzazioni sufficienti per utilizzare l'BatchPutAssetPropertyValueoperazione per inviare dati alle proprietà degli asset. Per ulteriori informazioni, consulta la sezione Requisiti del connettore AWS IoT SiteWise

- InvalidRequestException— I tipi di dati delle variabili OPC-UA non corrispondono ai tipi di dati delle proprietà degli asset. Se, ad esempio, una variabile OPC-UA presenta dati di tipo "numero intero", la proprietà di asset corrispondente deve prevedere il tipo di dati “numero intero”. Una proprietà con tipo doppio non può ricevere valori OPC-UA a numero intero. Per risolvere questo problema, definire nuove proprietà con i tipi di dati corretti.
- TimestampOutOfRangeException— Il gateway SiteWise Edge invia dati che non rientrano nell'intervallo consentito. AWS IoT SiteWise AWS IoT SiteWise rifiuta tutti i punti dati con timestamp precedenti a 7 giorni o più recenti di 5 minuti nel futuro. Se il gateway SiteWise Edge ha perso l'alimentazione o la connessione al AWS Cloud, potrebbe essere necessario cancellare la cache del gateway SiteWise Edge.
- ThrottlingExceptionoppure LimitExceededException: la richiesta ha superato una quota di AWS IoT SiteWise servizio, ad esempio la velocità di acquisizione dei punti dati o la frequenza di richiesta per le operazioni API relative ai dati relativi alle proprietà degli asset. Verificare che la configurazione non superi il valore AWS IoT SiteWise quote.

Nessun dato è stato visualizzato nel pannello di controllo

Se non vengono visualizzati dati nella dashboard, nella AWS IoT SiteWise console, controlla se la configurazione di Publisher e l'origine dati non sono sincronizzate. Per risolvere questo problema, utilizza i seguenti prodotti:

1. Accedi alla AWS IoT SiteWise console.
2. Nella sezione Edge, apri la sezione Gateways.
3. In Origini dati, seleziona Modifica.



4. Seleziona un nuovo nome di origine e seleziona Salva per confermare la modifica.
5. Verifica le modifiche confermando che il nome dell'origine dati è stato aggiornato nella tabella Origini dati.

La modifica del nome dell'origine dati può accelerare la sincronizzazione dal cloud all'edge, correggendo l'errore Out of sync.

«Impossibile trovare o caricare la classe principale» visualizzato in aws.iot. SiteWiseEdgePublisher registra l'errore /greengrass/v2/logs

Se viene visualizzato questo errore, potrebbe essere necessario aggiornare la versione java del gateway Edge. SiteWise

- Da un terminale, esegui il comando seguente:

```
java -version
```

La versione di java con cui è in esecuzione il gateway SiteWise Edge verrà visualizzata sotto`OpenJDK Runtime Environment`. Vedrai una risposta simile alla seguente:

```
openjdk version "11.0.20" 2023-07-18 LTS
```

```
OpenJDK Runtime Environment Corretto011.0.20.8.1 (build 11.0.20+8-LTS
OpenJDK 64-Bit Server VM Corretto-11.0.20.8.1 (build 11.0.20+8-LTS, mixed node)
```

Se si utilizza la versione Java 11.0.20.8.1, è necessario aggiornare il pacchetto IoT SiteWise Publisher alla versione 2.4.1 o successiva. È interessata solo la versione java 11.0.20.8.1, gli ambienti con altre versioni di Java possono continuare a utilizzare versioni precedenti del componente SiteWise IoT Publisher. Per ulteriori informazioni sull'aggiornamento di un pacchetto di componenti, vedere. Modifica della versione dei pacchetti di componenti del gateway SiteWise Edge

Risoluzione dei AWS IoT Greengrass problemi

Per trovare soluzioni a molti problemi relativi alla configurazione o all'implementazione del gateway SiteWise Edge AWS IoT Greengrass, consulta Risoluzione dei problemi AWS IoT Greengrass nella Guida per gli sviluppatori. AWS IoT Greengrass

Risoluzione dei problemi e azioni AWS IoT SiteWise relative alle regole

Per risolvere i problemi relativi all'azione della AWS IoT SiteWise regola in AWS IoT Core, è possibile eseguire una delle seguenti procedure:

- Configurazione di Amazon CloudWatch Logs
- Configurare un'azione di ripubblicazione dell'errore per la regola

Quindi, confrontare i messaggi di errore con gli errori presenti in questo argomento per risolvere il problema.

Argomenti

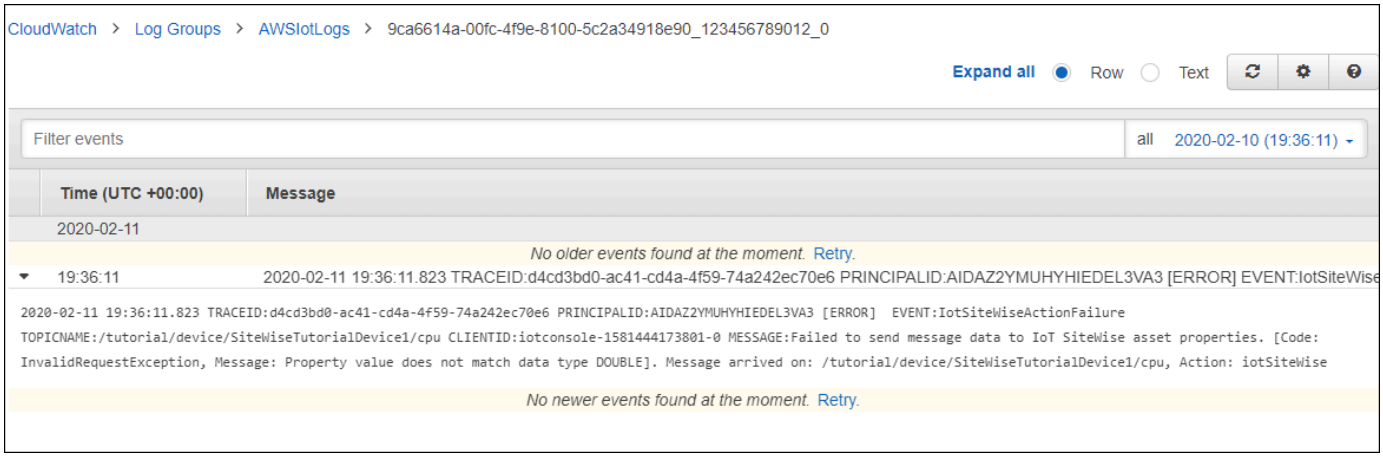
- Configurazione dei log AWS IoT Core
- Configurazione di un'azione di ripubblicazione dell'errore
- Risoluzione dei problemi
- Risoluzione dei problemi relativi a una regola
- Risoluzione dei problemi relativi a una regola

Configurazione dei log AWS IoT Core

È possibile configurare AWS IoT la registrazione di vari livelli di informazioni nei registri. CloudWatch

Per configurare e accedere ai registri CloudWatch

1. Per configurare la registrazione per AWS IoT Core, consulta Monitoring with CloudWatch Logs nella Developer Guide.AWS IoT
2. Passare alla console CloudWatch .
3. Nel pannello di navigazione, selezionare Log groups (Gruppi di log).
4. Scegli il gruppo. AWSIotLogs
5. Scegliere un flusso di log recente. Per impostazione predefinita, CloudWatch visualizza per primo il flusso di log più recente.
6. Scegliere una voce di log per espandere il messaggio di log. La voce di log potrebbe essere simile allo screenshot seguente.



7. Confrontare i messaggi di errore con gli errori in questo argomento per risolvere il problema.

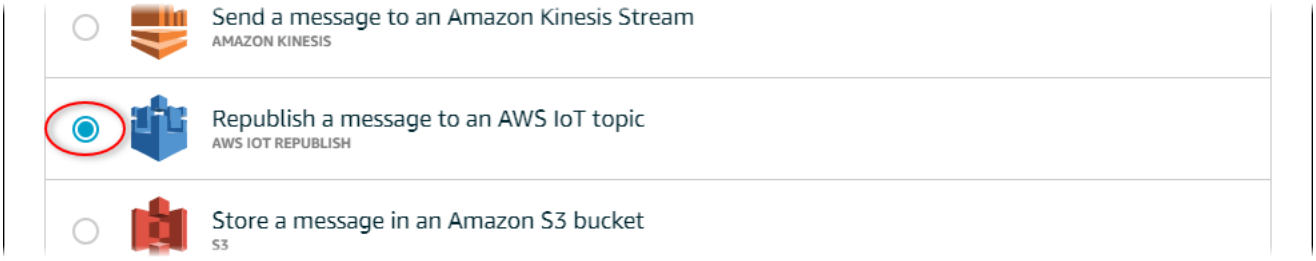
Configurazione di un'azione di ripubblicazione dell'errore

Puoi configurare un'azione di errore sulla regola per gestire i messaggi di errore. In questa procedura, è possibile configurare l'azione regola di ripubblicazione come azione di errore per visualizzare i messaggi di errore nel client di test MQTT.

> **Note**
>
> L'azione di ripubblicazione dell'errore genera solo un output equivalente ai log a livello di ERROR. Se desideri registri più dettagliati, devi configurare i registri. CloudWatch

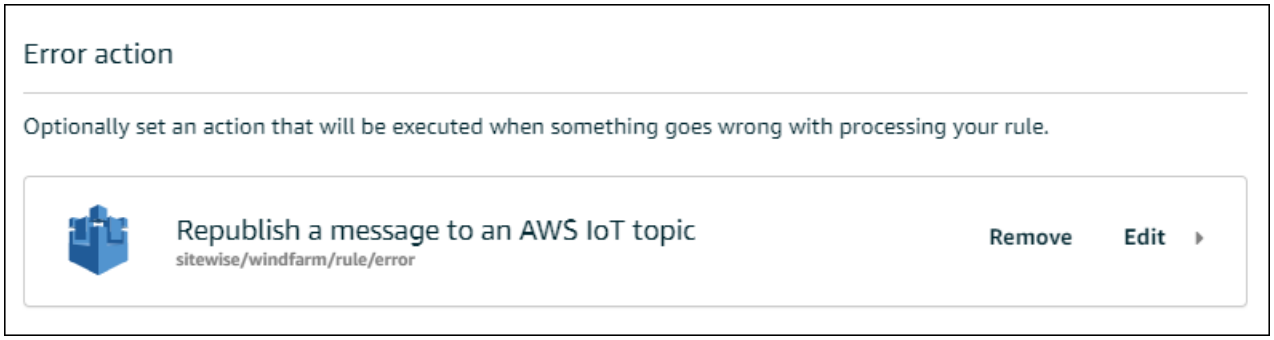
Per aggiungere un'azione di errore di ripubblicazione a una regola

1. Passare alla console AWS IoT.
2. Nel riquadro di navigazione sinistro scegliere Atti e quindi Regole.
3. Scegliere la regola.
4. In Azione errore, scegliere Aggiungi azione.
5. Scegli Ripubblica un messaggio su un argomento. AWS IoT



6. Scegliere Configura azione nella parte inferiore della pagina.
7. In Argomento, inserisci un argomento unico (ad esempio,**`sitewise/windfarm/rule/error`**). AWS IoT Core ripubblicherà i messaggi di errore relativi a questo argomento.
8. Scegli Seleziona per concedere AWS IoT Core l'accesso per eseguire l'azione di errore.
9. Scegliere Select (Seleziona) accanto al ruolo creato per la regola.
10. Scegliere Aggiorna ruolo per aggiungere le autorizzazioni aggiuntive al ruolo.
11. Selezionare Add action (Aggiungi operazione).

L'azione di errore della regola è simile allo screenshot seguente.



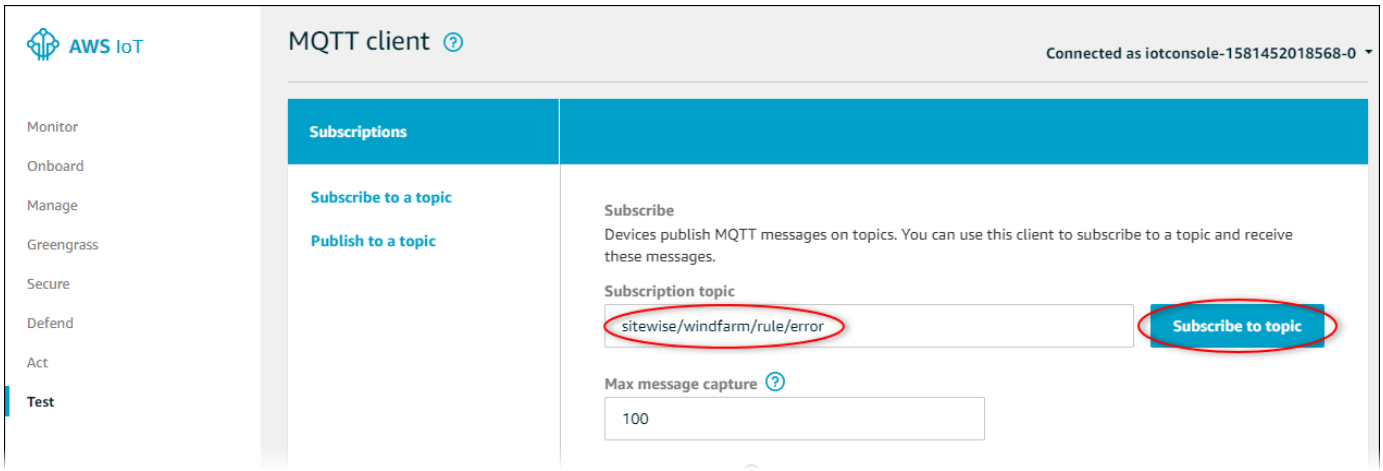
12. Scegli la freccia rivolta verso il basso nella parte superiore sinistra della console per tornare alla home page della AWS IoT console.

Dopo aver impostato l'azione di ripubblicazione dell'errore, è possibile visualizzare i messaggi di errore nel client di test MQTT in AWS IoT Core.

Nella procedura seguente, si sottoscrive l'argomento di errore nel client di test MQTT. Nel client di test MQTT, è possibile ricevere i messaggi di errore della regola per risolvere il problema.

Per sottoscrivere l'argomento dell'azione di errore

1. Passare alla console AWS IoT.
2. Nel riquadro di navigazione a sinistra, scegliere Test per aprire il client di test MQTT.
3. Nel campo Subscription topic (Argomento sottoscrizione) immettere l'argomento di errore configurato in precedenza (ad esempio **`sitewise/windfarm/rule/error`**) e scegliere Subscribe to topic (Effettua sottoscrizione all'argomento).



4. Controllare se vengono visualizzati messaggi di errore e quindi espandere l'array `failures` in qualsiasi messaggio di errore.

   Confronta i messaggi di errore con gli errori presenti in questo argomento per risolvere il problema.

Risoluzione dei problemi

Utilizzare le seguenti informazioni per risolvere i problemi relativi alle regole.

Problemi

Errore: il membro deve essere entro 604800 secondi prima e 300 secondi dopo il timestamp corrente

Il timestamp è più vecchio di 7 giorni o più recente di 5 minuti, rispetto all'ora attuale di Unix. Eseguire quanto segue:

- Controllare che il timestamp sia nell'ora in formato epoch Unix (UTC). Se si fornisce un timestamp con un fuso orario diverso, si riceve questo errore.
- Verifica che il timestamp sia espresso in secondi. AWS IoT SiteWise prevede che i timestamp siano suddivisi in secondi (in epoca Unix) e offset in nanosecondi.
- Verifica di caricare dati con data e ora non più tardi di 7 giorni nel passato.

Errore: il valore della proprietà non corrisponde al tipo di dati <type>

Una voce nell'azione di regola ha un tipo di dati diverso dalla proprietà dell'asset di destinazione. Ad esempio, la proprietà dell'asset di destinazione è di tipo `DOUBLE` ed è stato selezionato il tipo di dati Integer o è stato passato il valore `integerValue`. Eseguire quanto segue:

- Se configuri la regola dalla AWS IoT console, verifica di aver scelto il tipo di dati corretto per ogni immissione.
- Se configuri la regola dall'API o AWS Command Line Interface (AWS CLI), verifica che l'`value`oggetto utilizzi il campo di tipo corretto (ad esempio, `doubleValue` per una `DOUBLE` proprietà).

Errore: Utente: <role-arn>non autorizzato a eseguire: iotsitewise: on resource BatchPutAssetPropertyValue

La regola non è autorizzata ad accedere alla proprietà dell'asset di destinazione oppure la proprietà dell'asset di destinazione non esiste. Eseguire quanto segue:

- Verificare che l'alias della proprietà sia corretto e che si disponga di una proprietà dell'asset con l'alias di proprietà specificato. Per ulteriori informazioni, consulta Mappatura dei flussi di dati industriali alle proprietà degli asset.
- Verificare che la regola abbia un ruolo e che il ruolo conceda l'autorizzazione `iotsitewise:BatchPutAssetPropertyValue` alla proprietà dell'asset di destinazione, ad esempio tramite la gerarchia dell'asset di destinazione. Per ulteriori informazioni, consulta Concessione AWS IoT dell'accesso richiesto.

Errore: iot.amazonaws.com non è in grado di eseguire: sts: on resource: AssumeRole <role-arn>

Il tuo utente non è autorizzato ad assumere il ruolo previsto dalla tua regola in (IAM). AWS Identity and Access Management

Verifica che al tuo utente sia concessa l'`iam:PassRole`autorizzazione per il ruolo in base alla tua regola. Per ulteriori informazioni, consulta Pass role permissions nella AWS IoT Developer Guide.

Info: nessuna richiesta è stata inviata. PutAssetPropertyValueEntries era vuoto dopo aver eseguito i modelli sostitutivi.

> **Note**
>
> Questo messaggio è un log a livello di `INFO`.

La richiesta deve includere almeno una voce con tutti i parametri richiesti.

Verificare che i parametri della regola, inclusi i modelli di sostituzione, restituiscano valori non vuoti. I modelli di sostituzione non possono accedere ai valori definiti nelle clausole AS dell'istruzione della query della regola. Per ulteriori informazioni, consulta Modelli sostitutivi nella Guida per gli sviluppatori.AWS IoT

Risoluzione dei problemi relativi a una regola

Segui i passaggi di questa procedura per risolvere i problemi relativi alla regola se i dati sull'utilizzo della CPU e della memoria non vengono visualizzati come previsto. AWS IoT SiteWise In questa procedura, è possibile configurare l'azione regola di ripubblicazione come azione di errore per visualizzare i messaggi di errore nel client di test MQTT. Puoi anche configurare la registrazione su Logs per la risoluzione dei problemi. CloudWatch Per ulteriori informazioni, consulta Risoluzione dei problemi e azioni AWS IoT SiteWise relative alle regole.

Per aggiungere un'azione di errore di ripubblicazione a una regola

1. Passare alla console AWS IoT.
2. Nel riquadro di navigazione a sinistra, scegli Routing dei messaggi, quindi scegli Regole.
3. Scegli la regola che hai creato in precedenza e scegli Modifica.
4. In Azione di errore - facoltativa, scegli Aggiungi azione di errore.
5. Scegli Ripubblica un messaggio su un AWS IoT argomento.
6. In Argomento, inserisci il percorso dell'errore (ad esempio,**`sitewise/rule/tutorial/error`**). AWS IoT Core ripubblicherà i messaggi di errore relativi a questo argomento.
7. Scegli il ruolo che hai creato in precedenza (ad esempio, SiteWiseTutorialDeviceRuleRole).
8. Scegli Aggiorna.

Dopo aver impostato l'azione di ripubblicazione dell'errore, è possibile visualizzare i messaggi di errore nel client di test MQTT in AWS IoT Core.

Nella procedura seguente, si sottoscrive l'argomento di errore nel client di test MQTT.

Per sottoscrivere l'argomento dell'azione di errore

1. Passare alla console AWS IoT.
2. Nella pagina di navigazione a sinistra, scegliete MQTT test client per aprire il client di test MQTT.
3. Nel campo Filtro argomento, inserisci **`sitewise/rule/tutorial/error`** e scegli Iscriviti.

Quando vengono visualizzati messaggi di errore, visualizzare l'array `failures` in qualsiasi messaggio di errore per diagnosticare i problemi. Per ulteriori informazioni sui possibili problemi e su come risolverli, consultare Risoluzione dei problemi e azioni AWS IoT SiteWise relative alle regole.

Se non vengono visualizzati errori, verificare che la regola sia abilitata e che sia stato sottoscritto lo stesso argomento configurato nell'azione errore di ripubblicazione. Se dopo questa operazione ancora non vengono visualizzati gli errori, verificare che lo script del dispositivo sia in esecuzione e aggiornare correttamente la shadow del dispositivo.

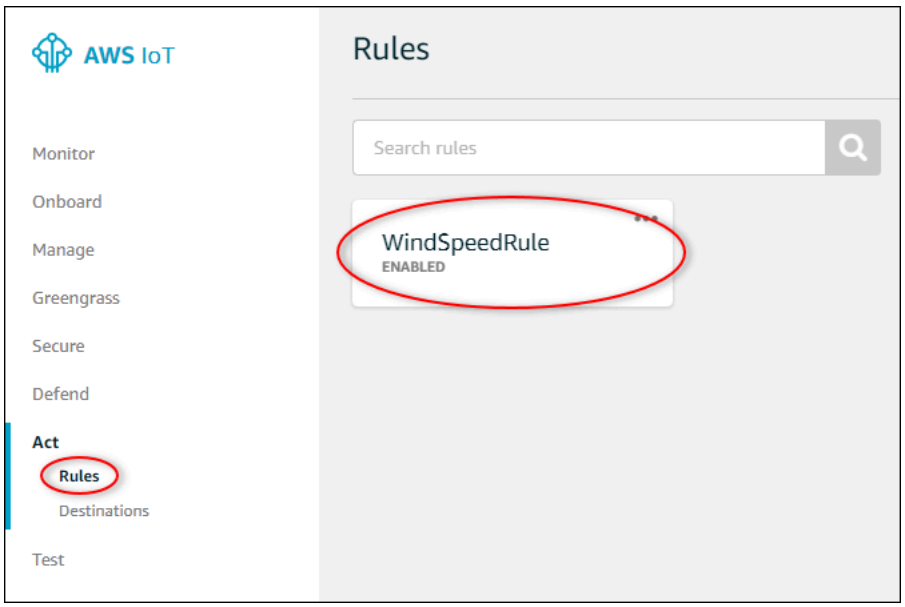
> **Note**
>
> Puoi anche iscriverti all'argomento Shadow Update del tuo dispositivo per visualizzare il payload analizzato dall' AWS IoT SiteWise azione. A tale scopo, eseguire la sottoscrizione al seguente argomento.
>
> ```
> $aws/things/+/shadow/update/accepted
> ```

Risoluzione dei problemi relativi a una regola

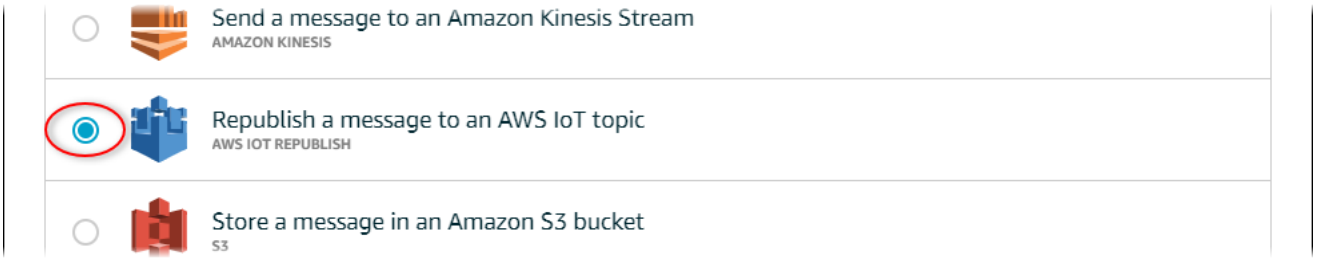
Segui i passaggi di questa procedura per risolvere i problemi relativi alla regola se i dati dell'asset demo non vengono visualizzati nella tabella DynamoDB come previsto. In questa procedura, è possibile configurare l'azione regola di ripubblicazione come azione di errore per visualizzare i messaggi di errore nel client di test MQTT. Puoi anche configurare la registrazione su Logs per risolvere i problemi. CloudWatch Per ulteriori informazioni, consulta Monitoring with CloudWatch Logs nella Developer Guide.AWS IoT

Per aggiungere un'azione di errore di ripubblicazione a una regola

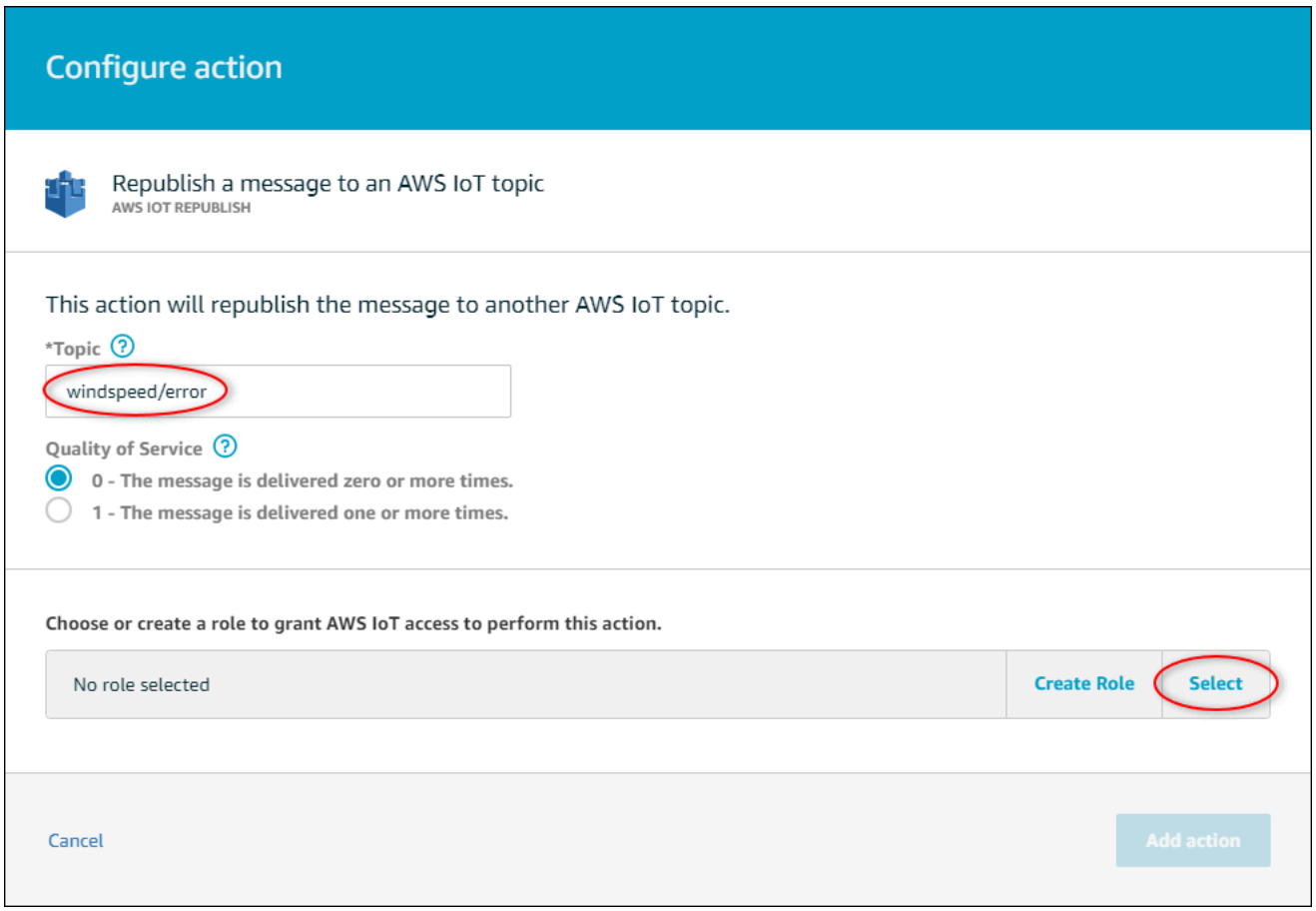
1. Passare alla console AWS IoT.
2. Nel riquadro di navigazione sinistro scegliere Atti e quindi Regole.
3. Scegliere la regola creata in precedenza.



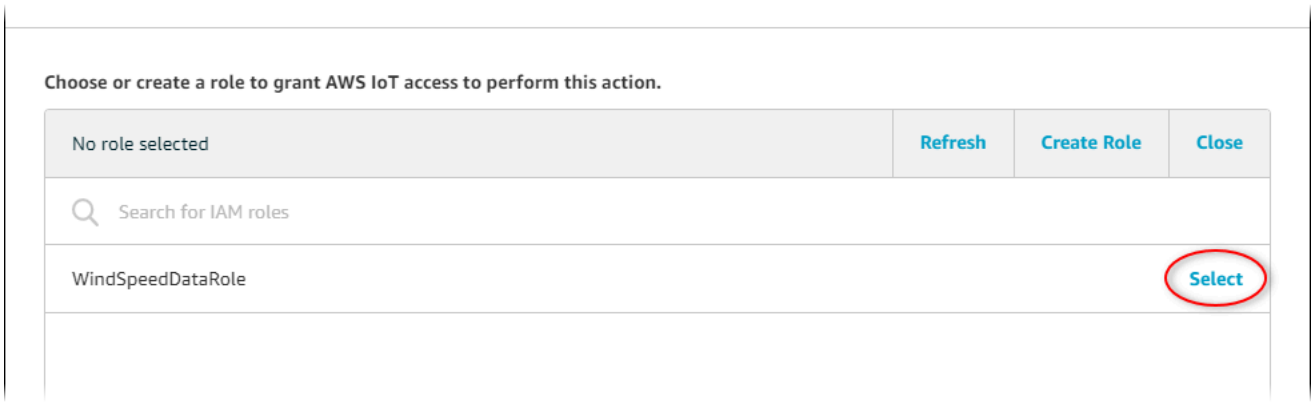
4. In Azione errore, scegliere Aggiungi azione.
5. Scegli Ripubblica un messaggio su un argomento. AWS IoT



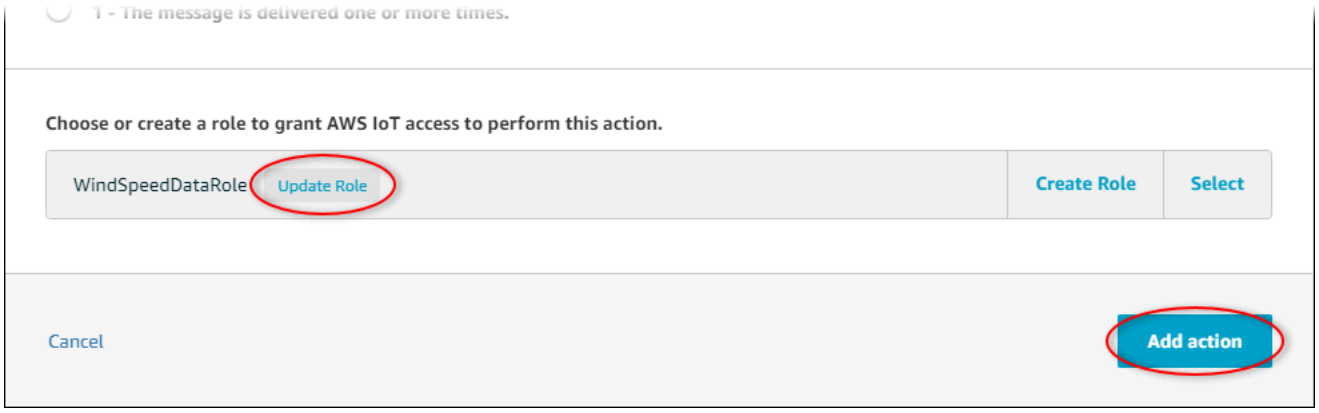
6. Scegliere Configura azione nella parte inferiore della pagina.
7. In Topic (Argomento), inserisci **`windspeed/error`**. AWS IoT Core ripubblicherà i messaggi di errore su questo argomento.



8. Scegli Seleziona per concedere a AWS IoT Core l'accesso per eseguire l'azione di errore utilizzando il ruolo che hai creato in precedenza.
9. Scegli Seleziona accanto al tuo ruolo.



10. Scegliere Aggiorna ruolo per aggiungere le autorizzazioni aggiuntive al ruolo.



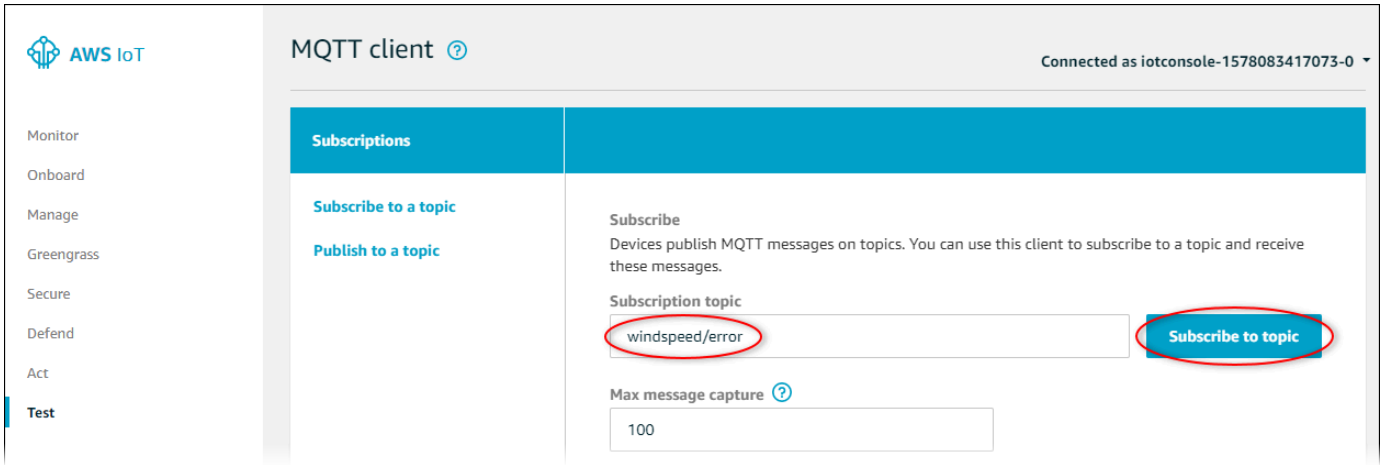
11. Scegliere Aggiungi azione per completare l'aggiunta dell'azione di errore.
12. Scegli la freccia indietro nella parte superiore sinistra della console per tornare alla home page della console AWS IoT Core.

Dopo aver impostato l'azione di errore di ripubblicazione, è possibile visualizzare i messaggi di errore nel client di test MQTT in AWS IoT Core.

Nella procedura seguente, si sottoscrive l'argomento di errore nel client di test MQTT.

Per sottoscrivere l'argomento dell'azione di errore

1. Nella pagina di navigazione a sinistra della console AWS IoT Core, scegli Test.
2. Nel campo Argomento della sottoscrizione immettere **`windspeed/error`** e scegliere Iscriviti all'argomento.



3. Controlla la visualizzazione dei messaggi di errore ed esplora l'array `failures` in un messaggio di errore per diagnosticare i seguenti problemi comuni:

   - Errori di battitura nell'istruzione query regola

- Autorizzazioni ruolo insufficienti

Se non vengono visualizzati errori, verificare che la regola sia abilitata e che sia stato sottoscritto lo stesso argomento configurato nell'azione errore di ripubblicazione. Se ancora non vengono visualizzati errori, verificare che le risorse del parco eolico dimostrativo esistano ancora e che siano state abilitate le notifiche sulle proprietà della velocità del vento. Se le tue risorse demo sono scadute e sono scomparse da AWS IoT SiteWise, puoi creare una nuova demo e aggiornare l'istruzione Rule Query in modo che rifletta il modello di asset e gli ID delle proprietà aggiornati.

AWS IoT SiteWise endpoint e quote

Le sezioni seguenti descrivono gli endpoint e le quote per. AWS IoT SiteWise

Indice

AWS IoT SiteWise punti finali

Per connettersi a livello di codice AWS IoT SiteWise, si utilizza un endpoint. Gli AWS SDK e AWS Command Line Interface (AWS CLI) utilizzano automaticamente l'endpoint predefinito in una regione. AWS Per ulteriori informazioni sulle regioni in cui AWS IoT SiteWise è disponibile, consulta AWS IoT SiteWise endpoint e quote in. Riferimenti generali di AWS

AWS IoT SiteWise supporta i seguenti endpoint.

Utilizza questo endpoint per accedere alle seguenti operazioni API del piano dati:,, e. BatchPutAssetPropertyValueGetAssetPropertyAggregatesGetAssetPropertyValueGetAssetPropertyValueHis Sostituisci *region* con la tua AWS regione.

AWS IoT SiteWise offre questo endpoint consolidato per le operazioni dell'API Control Plane che utilizzate per gestire modelli di asset, asset, gateway Edge, tag e configurazioni degli account. SiteWise Sostituisci *region* con la tua AWS regione.

> **Note**
>
> - Per impostazione predefinita, AWS IoT SiteWise utilizza l'endpoint consolidato quando si effettuano chiamate alle operazioni API del piano di controllo supportate.
> - Si consiglia di utilizzare l'endpoint consolidato per le operazioni API del piano di controllo supportate.
> - Non è possibile utilizzare l'endpoint consolidato per accedere alle operazioni dell' SiteWise API Monitor.

Le operazioni API del piano di controllo supportate includono AssociateAssetsCreateAssetCreateAssetModelDeleteAssetDeleteAssetModel, DeleteDashboard, DescribeAsset, DescribeAssetModel, DescribeAssetProperty, DescribeDashboard, DescribeLoggingOptions, DisassociateAssets, ListAssetModels, ListAssetRelationships, ListAssets, ListAssociatedAssets, PutLoggingOptionsUpdateAsset UpdateAssetModel, UpdateAssetProperty, CreateGateway, DeleteGateway, DescribeGateway, DescribeGatewayCapabilityConfiguration, ListGateways, UpdateGatewayUpdateGatewayCapabilityConfiguration, DescribeStorageConfiguration, PutStorageConfiguration, DescribeDefaultEncryptionConfiguration, ListTagsForResource, PutDefaultEncryptionConfiguration, TagResource, e UntagResource.

L'endpoint VPC dell'interfaccia per le operazioni dell'API del piano di controllo supporta solo l'endpoint consolidato. Per ulteriori informazioni, consulta Endpoint VPC .

iotsitewise.region.amazonaws.com

Utilizza questo endpoint per accedere alle seguenti operazioni API:,,,,, e. DescribeStorageConfigurationPutStorageConfigurationDescribeDefaultEncryptionConfigurationListTagsForR
Sostituisci *region* con la tua AWS regione.

Utilizza questo endpoint per accedere alle seguenti operazioni API:, AssociateAssets,,,,,,,,,,, CreateAssetCreateAssetModelDeleteAssetDeleteAssetModelDeleteDashboardDescribeAssetDescribeAsset
docs.aws.amazon.com/iot-sitewise/latest/APIReference/API_UpdateAsset.html, UpdateAssetModel, e. UpdateAssetProperty Sostituisci *region* con la tua AWS regione.

Utilizza questo endpoint per accedere alle seguenti operazioni API:,,,,, e. CreateGatewayDeleteGatewayDescribeGatewayDescribeGatewayCapabilityConfigurationListGatewaysUpda
Sostituisci *region* con la tua AWS regione.

Utilizza questo endpoint per accedere alle seguenti operazioni API:, BatchAssociateProjectAssets,,,,,,,,,,, BatchDisassociateProjectAssetsCreateAccessPolicyCreateDashboardCreatePortalCreateProjectDeleteAcce
docs.aws.amazon.com/iot-sitewise/latest/APIReference/API_UpdateAccessPolicy.html, UpdateDashboard, UpdatePortal, e. UpdateProject Sostituisci *region* con la tua AWS regione.

AWS IoT SiteWise quote

Le tabelle seguenti descrivono le quote in. AWS IoT SiteWise Per ulteriori informazioni sulle quote e su come richiedere aumenti delle quote, vedere le quote AWS di servizio nel. Riferimenti generali di AWS Per ulteriori informazioni sulle AWS IoT SiteWise quote, vedere AWS IoT SiteWise Service Quotas in. Riferimenti generali di AWS

Quote per asset e modelli di asset

Risorsa	Quota	Adattabile	Note
Numero di modelli di asset per regione per account AWS	1000	Sì	
Numero di asset per modello di asset	10.000	Sì	
Numero di asset figlio per asset padre	2000	Sì	
Profondità della struttura gerarchica del modello di asset	30	Sì	
Numero di definizioni della gerarchia per modello di asset	30	Sì	
Numero di proprietà nel livello principale per modello di asset	500	Sì	Questo numero massimo di `assetModelProperties` per ogni modello di asset. Questo conteggio non include `compositeModelProperties`. Questa quota si applica

Risorsa	Quota	Adattabile	Note
			anche a qualsiasi risorsa unica creata da questo modello di asset.
Numero di proprietà per modello di asset	5000	Sì	Il numero massimo di proprietà di un modello di asset di tipo `ASSET_MODEL` o `COMPONENT_MODEL` . Questo numero viene determinato combinando le proprietà del modello di asset principale e di qualsiasi modello composito incluso component-model-based o in linea. Questa quota si applica anche a qualsiasi risorsa unica creata da questo modello di asset.
Numero di proprietà per modello composito	100	Sì	Il numero massimo di proprietà consentite per i modelli compositi . Inoltre, il numero massimo di proprietà consentite per un tipo di modello di asset`COMPONENT_MODEL` .

Risorsa	Quota	Adattabile	Note
Profondità della struttura di proprietà per modello di asset	10	No	Un modello con una proprietà di trasformazione C che consuma una proprietà di trasformazione B che consuma, a sua volta, una proprietà di misurazione A, ad esempio, ha una profondità di 3.
Numero dei modelli di asset per struttura gerarchica	100	Sì	

Risorsa	Quota	Adattabile	Note
Numero di proprietà direttamente dipendenti per modello di asset	20	No	Questa quota limita il numero di proprietà che possono dipendere direttamente da una singola proprietà, come definito nelle espressioni formula di proprietà. Il numero di proprietà dipendenti per un modello di asset deve essere maggiore del numero di proprietà direttamente dipendenti per modello di asset. È necessario richiedere un aumento della quota per entrambi se il limite per il Numero di proprietà direttamente dipendenti per modello di asset è maggiore del limite per il Numero di proprietà dipendenti per modello di asset.

Risorsa	Quota	Adattabile	Note
Numero di proprietà dipendenti per modello di asset	30	No	Questa quota limita il numero di proprietà che possono dipendere direttamente o indirettamente da una singola proprietà , come definito nelle espressioni formula di proprietà.
Numero di modelli compositi per modello di asset	50	Sì	Il numero massimo di modelli compositi consentiti su un singolo modello di asset.
Profondità del modello composito	2	Sì	La profondità massima dell'albero del modello composito per modello di asset, inclusi i modelli in linea e component -model-based compositi.

Risorsa	Quota	Adattabile	Note
Numero di modelli di asset unici che utilizzano lo stesso modello di componenti	20	Sì	Il numero massimo di modelli di asset unici che dispongono di almeno un modello component-model-based composito che fa riferimento direttamente a un modello di asset specifico di tipo COMPONENT_MODEL.
Numero di variabili della proprietà per espressione formula di proprietà	10	No	Ad esempio, ci sono due variabili di proprietà `power` e `temp`, nell'espressione. `avg(power) + max(temp)` Ciò vale anche per i risultati del calcolo delle trasformazioni.
Numero di funzioni per espressione formula di proprietà	10	No	Ad esempio, ci sono due funzioni `avg` e `max`, nell'espressione `avg(power) + max(temp)` .

Quote per i dati delle proprietà asset

Risorsa	Quota	Adattabile	Note
Tasso di richiesta per le operazioni API dei	1000 richieste al secondo per regione per AWS account	Sì	Questa quota si applica alle operazioni API, quali `GetAssetP`

Risorsa	Quota	Adattabile	Note
dati delle proprietà asset			`ropertyValue` e `BatchPutA ssetPrope rtyValue` .
Numero di punti dati al secondo per qualità dei dati per proprietà di risorsa	10 punti dati	No	Questa quota si applica al numero massimo di punti dati timestamp-quality-value (TQV) con lo stesso timestamp in secondi per qualità dei dati per ciascuna proprietà dell'asse t. Puoi memorizza re questo numero di punti dati di buona qualità, qualità incerta e cattiva qualità per un dato secondo per ogni proprietà di risorsa.
Numero di `BatchPutA ssetPrope rtyValue` voci inserite al secondo per proprietà dell'asse t, per regione per account. AWS	10 voci per proprietà patrimoniale	No	Questa quota si applica alle `BatchPutA ssetPrope rtyValue` voci provenienti da tutte le fonti, inclusi gateway SiteWise Edge, AWS IoT Core regole e chiamate API.

Risorsa	Quota	Adattabile	Note
Percentuale di punti dati ingeriti	5000 punti dati al secondo per regione per account AWS	Sì	Punti dati Timestamp-quality-value (TQV).
Richiedi tariffa per `BatchGetAssetPropertyAggregates`	200	Sì	Il numero massimo di `BatchGetAssetPropertyAggregates` richieste al secondo che è possibile eseguire in questo account nella regione corrente.
Richiedi una tariffa per `BatchGetAssetPropertyValue`	500	Sì	Il numero massimo di `BatchGetAssetPropertyValue` richieste al secondo che è possibile eseguire in questo account nella regione corrente.
Richiedi una tariffa per `BatchGetAssetPropertyValueHistory`	200	Sì	Il numero massimo di `BatchGetAssetPropertyValueHistory` richieste al secondo che è possibile eseguire in questo account nella regione corrente.

Risorsa	Quota	Adattabile	Note
Numero di `BatchPutAssetPropertyValue` voci inserite al secondo per proprietà dell'asset, per AWS regione e account.	10 voci per proprietà patrimoniale	No	Questa quota si applica alle `BatchPutAssetPropertyValue` voci provenienti da tutte le fonti, inclusi gateway SiteWise Edge, AWS IoT Core regole e chiamate API.
Frequenza delle `GetAssetPropertyAggregates` richieste e delle interrogazioni di `BatchGetAssetPropertyAggregates` immissione per proprietà dell'asset	50	No	Il numero massimo di `GetAssetPropertyAggregates` richieste e `BatchGetAssetPropertyAggregates` immissioni totali per ogni proprietà dell'asset al secondo in questo account nella regione corrente.

Risorsa	Quota	Adattabile	Note
Frequenza delle `GetAssetPropertyValue` richieste e delle interrogazioni di `BatchGetAssetPropertyValue` immissione per proprietà dell'asset	500	No	Il numero massimo di `GetAssetPropertyValue` richieste e `BatchGetAssetPropertyValue` immissioni totali per ogni proprietà dell'asset al secondo in questo account nella regione corrente.
Frequenza delle `GetAssetPropertyValueHistory` richieste e delle interrogazioni di `BatchGetAssetPropertyValueHistory` immissione per proprietà dell'asset	30	No	Il numero massimo di `GetAssetPropertyValueHistory` richieste e `BatchGetAssetPropertyValueHistory` immissioni totali per ogni proprietà dell'asset al secondo in questo account nella regione corrente.

Risorsa	Quota	Adattabile	Note
Frequenza delle `GetInterpolatedAssetPropertyValues` richieste	500	Sì	Il numero massimo di `GetInterpolatedAssetPropertyValues` richieste al secondo che è possibile eseguire in questo account nella regione corrente.
Numero di risultati per `GetInterpolatedAssetPropertyValues` richiesta	10	Sì	Il numero massimo di risultati da restituire per richiesta impaginata. `GetInterpolatedAssetPropertyValues`

Risorsa	Quota	Adattabile	Note
Frequenza di punti dati recuperati da e `GetAssetPropertyValueHistory` `BatchGetAssetPropertyValueHistory`	100 MB di risposta in lettura al secondo per regione per account. AWS	Sì	La velocità massima in byte (MB/secondo) dei punti dati recuperati al secondo per regione per account tra e. AWS `GetAssetPropertyValueHistory` `BatchGetAssetPropertyValueHistory` Il payload di risposta valutato per questa quota utilizza i campi Timestamp-Quality-Value (TQV) per ogni datapoint e arrotonda la dimensione in byte per ogni richiesta API al successivo incremento di 4 KB. imestamp-quality-value I datapoint T (TQV) recuperati al secondo variano in base al tipo di dati: • Numero intero: fino a 5 milioni di TQV al secondo

Risorsa	Quota	Adattabile	Note
			• Doppio: fino a 4 milioni di TQV al secondo • Booleano: fino a 6 milioni di TQV al secondo • Stringa: varia in base alla dimensione del valore di ogni stringa.

Quote per i gateway SiteWise Edge

Risorsa	Quota	Regolabile
Numero di gateway SiteWise Edge per regione per account AWS	100	Sì
Numero di sorgenti OPC-UA per gateway Edge SiteWise	100	No

Quote per AWS IoT SiteWise Monitor

Risorsa	Quota	Regolabile
Numero di portali per regione per account AWS	100	Sì
Numero di progetti per portale	100	Sì
Numero di pannelli di controllo per progetto	100	Sì

Risorsa	Quota	Regolabile
Numero di asset principali per progetto	1	No
Numero di visualizzazioni per pannello di controllo	10	Sì
Numero di parametri per visualizzazione del pannello di controllo	5	Sì
Numero di soglie per visualizz azione del dashboard	12	No

Quote per l'importazione e l'esportazione in AWS IoT SiteWise blocco di metadati

Risorsa	Descrizione	Quota	Regolabile
Numero di processi di trasferimento di metadati in coda	Il numero massimo di processi di trasferim ento di `PENDING` metadati in coda.	10	Sì
Dimensione del file di importazione del processo di trasferim ento dei metadati	La dimensione massima del file importato (in MB).	100 MB	Sì
AWS IoT SiteWise quota di risorse per un processo di trasferim ento di metadati	Il numero massimo di risorse importate o esportate in un singolo lavoro. Una risorsa include risorse e modelli di asset.	5000	No

Quote per l'importazione in AWS IoT SiteWise blocco di dati

Risorsa	Quota	Regolabile
Numero di processi di importazione in blocco in esecuzione	100	No
Dimensione del file CSV	10 GB	No
Dimensione del file parquet non compresso	256 MB	No
Dimensione del CSV file per l'ingestione bufferizzata	256 MB	No
Dimensione del gruppo di file di parquet non compresso	64 MB	No
Numero di misurazioni uniche per gruppo di file di parquet	2000	Sì
Numero di giorni tra il timestamp del passato e quello odierno per l'ingestione tamponata	30	Sì
Richiedi la tariffa `CreateBulkImportJobs` per ogni regione in ogni account AWS	10	Sì
Richiedi la tariffa `ListBulkImportJobs` per ogni regione in ogni AWS account	50	Sì
Richiedi la tariffa `DescribeBulkImportJobs` per ogni regione in ogni AWS account	50	Sì

Quote per il rilevamento delle anomalie

Le quote per il rilevamento delle anomalie sono condivise tra AWS IoT SiteWise Amazon Lookout for Equipment e Amazon. Per ulteriori informazioni, vedere Quote per l'utilizzo di Lookout for Equipment.

Cronologia dei documenti per la Guida per AWS IoT SiteWise l'utente

La tabella seguente descrive la documentazione per questa versione di AWS IoT SiteWise.

- Versione API: 02-12-2019

Modifica	Descrizione	Data
È stato aggiunto il supporto per l'esecuzione di SiteWise Edge su Siemens Industrial Edge	AWS IoT SiteWise ora supporta l'esecuzione di SiteWise Edge su dispositivi Siemens Industrial Edge.	26 novembre 2023
È stato aggiunto il supporto per lo storage a livello caldo	AWS IoT SiteWise ora supporta il warm storage, un livello di storage completam ente gestito che consente ai clienti di archiviare e accedere in modo sicuro ai dati industria li.	15 novembre 2023
È stato aggiunto il supporto per identificatori univoci definiti dall'utente	AWS IoT SiteWise ora supporta l'uso di identificatori univoci definiti dall'utente per asset, modelli di asset, proprietà e gerarchie.	15 novembre 2023
È stato aggiunto il supporto per il rilevamento di anomalie multivariate degli asset industriali	AWS IoT SiteWise ora supporta il rilevamento multivariato delle anomalie degli asset industriali mediante l'integrazione di dati storici e in tempo reale sulle apparecch iature con Amazon Lookout for Equipment.	15 novembre 2023

È stato aggiunto il supporto per l'inserimento conveniente e scalabile di dati di serie temporali in AWS IoT SiteWise	AWS IoT SiteWise ora supporta l'inserimento conveniente e scalabile dei dati di serie temporali necessari per i casi d'uso analitici.	15 novembre 2023
È stato aggiunto il supporto per l'importazione, l'esportazione e l'aggiornamento in blocco	AWS IoT SiteWise ora supporta l'importazione, l'esportazione e l'aggiornamento in blocco dei metadati delle apparecchiature industriali.	15 novembre 2023
È stato aggiunto il supporto per i componenti del modello di asset	AWS IoT SiteWise ora supporta i componenti del modello Asset per aiutare i clienti industriali a creare componenti riutilizzabili.	15 novembre 2023
Aggiunto supporto per l'applicazione dashboard IoT	AWS IoT SiteWise ora supporta un'applicazione dashboard open source in cui è possibile visualizzare e interagire con i dati operativi.	15 novembre 2023
Sono stati aggiornati i ruoli collegati ai servizi per AWS IoT SiteWise	AWS IoT SiteWise dispone di nuovi ruoli collegati ai servizi e può eseguire una query di ricerca di metadati sul database. AWS IoT TwinMaker	6 novembre 2023
Etichettatura aggiornata per le risorse del flusso di dati AWS IoT SiteWise	È stato aggiunto il supporto per l'etichettatura delle risorse del flusso di dati.	18 agosto 2022

Gateway SiteWise Edge aggiornati	Ora puoi configurare l'editore per controllare quali dati vengono inviati dall'edge al cloud e l'ordine in cui vengono inviati al cloud.	12 gennaio 2022
È stata aggiornata la AWS IoT SiteWise demo	Ora puoi usare la demo per creare un portale SiteWise Monitor.	10 gennaio 2022
Gestione aggiornata dello storage	Ora puoi definire un periodo di conservazione per controlla re per quanto tempo i dati vengono conservati nel livello più elevato.	29 novembre 2021
È stato aggiunto il supporto per la gestione del flusso di dati	Ora puoi inserire i dati AWS IoT SiteWise prima di creare modelli e asset di asset.	24 novembre 2021
Gerarchie di modelli di asset aggiornate	Un modello di asset figlio ora può essere associato a più modelli di asset principali.	28 ottobre 2021
Avvio della regione	Lanciato AWS IoT SiteWise in AWS GovCloud (Stati Uniti occidentali).	29 settembre 2021

Funzioni aggiornate	Sono state aggiunte le seguenti funzionalità • Nelle metriche, è possibile utilizzare espressioni annidate nelle funzioni di aggregazione e nelle funzioni temporali. • Nelle trasformazioni, potete utilizzare la funzione pretrigger () per recuperare e il valore di una variabile prima dell'aggiornamento della proprietà che ha attivato il calcolo della trasformazione corrente.	10 agosto 2021
Intervallo di tempo metrico personalizzato	È stato aggiunto il supporto per intervalli di tempo e offset personalizzati nelle metriche.	3 agosto 2021
Utilizzo AWS IoT SiteWise sul bordo	La funzione di elaborazione dei bordi è ora disponibile a livello generale.	29 luglio 2021
Esportazione di dati su Amazon S3	AWS IoT SiteWise ora può esportare dati su Amazon S3.	27 luglio 2021
Endpoint VPC ()AWS PrivateLink	L'endpoint VPC dell'interfaccia per le operazioni dell'API del piano di controllo è ora disponibile a livello generale.	15 luglio 2021
Trasformazioni	Le trasformazioni ora possono inserire più variabili di proprietà degli asset.	8 luglio 2021

È stata aggiornata la funzione timestamp ()	Nelle trasformazioni, ora puoi fornire una variabile come argomento della funzione. `timestamp()`	16 giugno 2021
Disponibilità generale degli allarmi	La funzionalità degli allarmi è ora disponibile a livello generale.	27 maggio 2021
È stata rilasciata la versione 2 dell'adattatore di protocollo Modbus-TCP	È disponibile la versione 2 del connettore Modbus-TCP Protocol Adapter. Questa versione ha aggiunto il supporto per le stringhe sorgente codificate ASCII, UTF8 e ISO8859.	24 maggio 2021
Quote di servizio aggiornate	Sono state aggiunte le seguenti quote per l'GetInterpolatedAssetPropertyValuesAPI: frequenza delle `GetInterpolatedAssetPropertyValues` richieste, numero di risultati per `GetInterpolatedAssetPropertyValues` richiesta e numero di giorni tra la data di inizio passata e quella odierna di. `GetInterpolatedAssetPropertyValues`	29 aprile 2021

Espressioni di formule aggiornate	Sono stati aggiunti i seguenti operatori e funzioni: • Sono stati aggiunti i seguenti operatori: `< > <=>=,==,!=,!,and,or, enot`. • È stata aggiunta la seguente funzione di confronto :`neq(x, y)`. • Sono state aggiunte le seguenti funzioni di stringa: `join()format()`, `ef''`.	22 Aprile 2021
Endpoint VPC ()AWS PrivateLink	Sono state aggiunte informazioni su come stabilire una connessione privata tra il cloud privato virtuale (VPC) e le API del piano di AWS IoT SiteWise controllo creando un endpoint VPC di interfaccia.	16 marzo 2021
Federazione IAM	Gli amministratori e gli utenti del portale SiteWise Monitor possono ora accedere ai portali assegnati con le proprie credenziali IAM.	16 marzo 2021
Lancio della regione	Lanciato AWS IoT SiteWise in Cina (Pechino).	3 febbraio 2021

Rilasciata la versione 10 del SiteWise connettore IoT	È disponibile la versione 10 del SiteWise connettor e IoT. Questa versione è configurata `StreamManager` per migliorare la gestione quando la connessione di origine viene persa e ristabili ta. Questa versione accetta anche valori OPC-UA con un `ServerTimestamp` quando no è disponibile. `SourceTim estamp`	22 gennaio 2021
Funzioni di data e ora	AWS IoT SiteWise ora supporta le funzioni di data e ora.	21 gennaio 2021
Sintassi della funzione	È ora possibile utilizzare la sintassi UFCS (Uniform Function Call Syntax) per le funzioni. AWS IoT SiteWise	11 gennaio 2021
Integrazione con Grafana	Sono state aggiunte informazi oni su come visualizzare AWS IoT SiteWise i dati nelle dashboard di Grafana.	15 dicembre 2020

AWS IoT SiteWise versione di funzionalità	Ora puoi monitorare i tuoi dati con allarmi, elaborare i dati industriali sull'edge, utilizzar e sorgenti Modbus TCP ed EtherNet/IP sul tuo gateway SiteWise Edge, filtrare i dati in entrata con bande morte e altro ancora. • È stata aggiunta la sezione Dati di monitoraggio con allarmi che è possibile utilizzare per definire, configurare e rispondere agli allarmi. AWS IoT SiteWise • È stata aggiunta la sezione Elaborazione perimetrale che è possibile utilizzare per configurare l'elabora zione dei dati industriali sui dispositivi periferici. • Sono state aggiunte le sezioni Modbus TCP ed EtherNet/IP alla documenta zione di origine del gateway Edge. SiteWise • È stata aggiunta la sezione di destinazione dell'origine che è possibile utilizzare per personalizzare la destinazi one di invio dei dati industria li in entrata. • È stata aggiunta la sezione di filtro OPC-UA che è possibile utilizzare per controllare la frequenza e il	15 dicembre 2020

	tipo di dati inviati al gateway SiteWise Edge dal server locale industriale.	
AWS IoT SiteWise ora supporta le CMK gestite dai clienti.	AWS IoT SiteWise ora supporta la crittografia con CMK gestite dal cliente.	24 novembre 2020
Rilasciata la versione 8 del SiteWise connettore IoT	È disponibile la versione 8 del SiteWise connettore IoT. Questa versione migliora la stabilità quando il connettore presenta una connettività di rete intermittente.	19 novembre 2020
Utilizzo di stringhe e condizionali nelle espressioni delle formule	Sono state aggiunte informazioni sull'utilizzo di stringhe e funzioni condizionali nelle espressioni di formule per trasformazioni e metriche.	16 Novembre 2020
Acquisizione di dati tramite stream manager AWS IoT Greengrass	Sono state aggiunte informazioni su come importare dati IoT ad alto volume da fonti di dati locali utilizzando un dispositivo AWS IoT Greengrass perimetrale.	16 settembre 2020
Endpoint VPC ()AWS PrivateLink	Sono state aggiunte informazioni su come stabilire una connessione privata tra il cloud privato virtuale (VPC) e le API di AWS IoT SiteWise dati creando un endpoint VPC di interfaccia.	4 settembre 2020

Rilasciata la versione 7 del SiteWise connettore IoT	È disponibile la versione 7 del SiteWise connettore IoT. Questa versione corregge un problema relativo alle metriche del gateway SiteWise Edge.	14 agosto 2020
Creazione di utenti IAM Identity Center dalla console AWS IoT SiteWise	Sono state aggiunte informazioni su come creare utenti IAM Identity Center nella AWS IoT SiteWise console. Ora puoi creare utenti IAM Identity Center quando assegni gli utenti a un portale nuovo o esistente. È stato aggiornato il tutorial sulla visualizzazione e la condivisione dei dati dei parchi eolici per utilizzare questa funzionalità. Questa modifica riduce il numero di passaggi del tutorial.	4 agosto 2020
Risoluzione dei problemi migliorata del gateway SiteWise Edge	Sono state aggiunte ulteriori informazioni su come risolvere i problemi di un gateway SiteWise Edge e su come esportare il certificato client OPC-UA come fonte.	18 giugno 2020

Documentazione sulle attività della console	Aggiunta della documentazione delle attività della console per la modellazione degli asset industriali, l'esecuzione di query sui dati delle proprietà di asset e l'interazione con altri servizi. Puoi seguire queste istruzioni per completare le attività nella console AWS IoT SiteWise .	11 giugno 2020
Tutorial sull'analisi dei dati esportati	È stato aggiunto un tutorial che puoi seguire per imparare a usare Amazon Athena per analizzare i dati degli asset che hai esportato in S3 con il modello di funzionalità di esportazione. AWS CloudFormation	27 maggio 2020
Migliorato utilizzando espressioni di formule	Sono state aggiunte informazioni dettagliate sul comportamento delle proprietà delle AWS IoT SiteWise formule e aggiunto un esempio di come contare i punti dati filtrati.	18 maggio 2020

Rilasciata la versione 6 del SiteWise connettore IoT	È disponibile la versione 6 del SiteWise connettore IoT. Questa versione aggiunge il supporto per le CloudWatch metriche e l'individuazione automatica di nuovi tag OPC-UA. Ciò significa che non è necessario riavviare il gateway SiteWise Edge quando i tag cambiano per le sorgenti OPC-UA. Questa versione del connettore richiede lo stream manager e il software AWS IoT Greengrass Core v1.10.0 o superiore.	29 aprile 2020

AWS IoT SiteWise versione di funzionalità	AWS IoT SiteWise versione di funzionalità. Ora puoi gestire i gateway SiteWise Edge con l'API, aggiungere il tuo logo ai portali, visualizzare le metriche dei gateway SiteWise Edge e altro ancora. • È stata aggiunta la sezione Esportazione di dati in Amazon S3 con AWS CloudFormation un modello che puoi utilizzare per esportare nuovi valori di dati in un bucket S3. • È stata aggiunta la sezione Configurazione delle fonti di dati che migliora la documentazione sui sorgenti di SiteWise Edge Gateway e include le nuove API Edge Gateway. SiteWise • È stata aggiunta la sezione relativa alle metriche del gateway SiteWise Edge che descrive le CloudWatc h metriche pubblicate dai gateway Edge. SiteWise • È stata aggiunta la sezione Configurazione di un gateway SiteWise Edge su Amazon EC2 con AWS CloudFormation un modello che è possibile utilizzare per SiteWise configurare rapidamente le dipendenz	29 aprile 2020

	e del gateway Edge su un'istanza Amazon EC2. • È stata aggiunta la sezione sui ruoli del servizio di portale che descrive la nuova funzionalità di autorizzazione dei portali Monitor. SiteWise • È stata aggiornata la documentazione del portale per ruoli del servizio del portale e loghi del portale. • È stata aggiunta la sezione Taggare le risorse AWS IoT SiteWise. • È stata aggiornata la sezione Creazione di pannelli di controllo (CLI) per la nuova struttura di definizione del pannello di controllo. • È stata aggiunta la sezione relativa alla sicurezza.	
Acquisizione di dati da AWS IoT Events	Sono state aggiunte informazioni su come importare dati da AWS IoT Events quando si verifica un evento.	20 aprile 2020
Visualizzazione e condivisione dei dati dei parchi eolici nel tutorial Monitor SiteWise	È stato aggiunto un tutorial che puoi seguire per imparare a utilizzare AWS IoT SiteWise Monitor per visualizzare e condividere i dati degli asset.	12 marzo 2020

AWS IoT SiteWise concetti	È stato aggiunto un glossario di AWS IoT SiteWise concetti che è possibile utilizzare per conoscere il servizio e i termini più comuni.	5 marzo 2020
Istruzioni di AWS IoT Greengrass installazione rimosse	Sono state rimosse le istruzioni di installazione del software di AWS IoT Greengrass base dalla Guida AWS IoT SiteWise per l'utente. La AWS IoT Greengrass Developer Guide offre uno script di configurazione del dispositivo e istruzioni per la configurazione AWS IoT Greengrass su altre piattaforme come Amazon EC2 e Docker.	14 febbraio 2020
Migliore acquisizione dei dati tramite regole AWS IoT Core	Sono state aggiunte informazioni dettagliate sull'utilizzo e sulla risoluzione dei problemi dell'azione della AWS IoT SiteWise regola, che è possibile utilizzare per importare dati dai messaggi MQTT. AWS IoT Core	14 febbraio 2020
Rilasciata la versione 5 del SiteWise connettore IoT	È disponibile la versione 5 del SiteWise connettore IoT. Questa versione corregge un problema di compatibilità con il software AWS IoT Greengrass Core v1.9.4.	12 febbraio 2020

Rilasciata la versione 4 del SiteWise connettore IoT	È disponibile la versione 4 del SiteWise connettore IoT. Questa versione consente di correggere un problema con la riconnessione del server OPC-UA.	7 febbraio 2020
Asset industriali di modellazione ristrutturati	È stata ristrutturata la sezione Aggiornamento di asset e modelli in più argomenti relativi alla modellazione degli asset industriali. • Stati di asset e modelli • Mappatura dei flussi di dati industriali alle proprietà degli asset • Aggiornamento dei valori degli attributi • Associazione e annullamento dell'associazione degli asset • Aggiornamento di asset e modelli • Eliminazione di asset e modelli	4 febbraio 2020
Tutorial sull'acquisizione di dati da oggetti AWS IoT	È stato aggiunto un tutorial che puoi seguire per imparare a configurare un'azione della AWS IoT SiteWise regola per importare dati da una flotta di cose nuova o esistente. AWS IoT	4 febbraio 2020

Recupero di dati ristrutturato da AWS IoT SiteWise	Ha ristrutturato la sezione Recupero dei dati in due sezioni di primo livello: interrogazione dei valori e degli aggregati delle proprietà degli asset e interazione con altri servizi. AWS	21 gennaio 2020
Tutorial sulla pubblicazione degli aggiornamenti dei valori delle proprietà in Amazon DynamoDB	È stato aggiunto un tutorial che puoi seguire per imparare a utilizzare le notifiche sui valori delle proprietà per archiviare i dati degli asset in DynamoDB.	8 gennaio 2020
Usare le espressioni delle formule	Aggiunto il riferimento all'espressione di formula per organizzare le costanti e le funzioni disponibili per l'uso nelle proprietà di trasforma zione e dei parametri. Sono state ristrutturate le proprietà dell'asset in argomenti separati per ogni tipo di proprietà.	7 gennaio 2020
Utilizzo dei filtri di nodo OPC-UA	Sono state aggiunte informazi oni su come utilizzare i filtri dei nodi OPC-UA per migliorar e le prestazioni del gateway SiteWise Edge durante l'aggiunta SiteWise di sorgenti gateway Edge.	3 gennaio 2020

Aggiornamento di un connettore	Sono state aggiunte informazioni su come aggiornare un gateway SiteWise Edge quando viene rilasciata una nuova versione del connettore.	30 dicembre 2019
Rilasciata la versione 3 del SiteWise connettore IoT	È disponibile la versione 3 del SiteWise connettore IoT. Questa versione rimuove il requisito di autorizzazione iot:*.	17 dicembre 2019
Rilasciata la versione 2 del SiteWise connettore IoT	È disponibile la versione 2 del SiteWise connettore IoT. Questa versione aggiunge il supporto per più risorse segrete OPC-UA.	10 dicembre 2019
Creazione di dashboard ()AWS CLI	Sono state aggiunte informazioni su come creare una dashboard AWS IoT SiteWise Monitor utilizzando. AWS CLI	6 dicembre 2019

AWS IoT SiteWise è stata rilasciata la versione 2	Anteprima rilasciata per la versione 2 di AWS IoT SiteWise. Ora puoi importare dati su OPC-UA, MQTT e HTTP, modellare i dati in gerarchie di asset e visualizzare i tuoi dati con Monitor. SiteWise • Riscritta la sezione dedicata alla modellazione degli asset per le modifiche apportate agli asset con i propri modelli e le relative gerarchie. • È stata aggiornata la sezione relativa all'inserimento dei dati per includere le fasi del connettore e le sezioni relative all'inserimento dei dati non relative al gateway. AWS IoT Greengrass • È stata aggiunta la AWS IoT SiteWise Monitorsezione e una guida all'applicazione separata che mostra come utilizzare l'applicazione web Monitor. SiteWise • Aggiunte le sezioni Interroga dati da AWS IoT SiteWise e Interazione con altri servizi AWS. • Riscritta la sezione Nozioni di base in conformità	2 dicembre 2019

	all'aggiornamento dell'esperienza demo.	
AWS IoT SiteWise è stata rilasciata la versione 1	Rilasciata l'anteprima iniziale per la versione 1 di AWS IoT SiteWise.	25 febbraio 2019

Glossario AWS

Per la terminologia AWS più recente, consultare il glossario AWS nella documentazione di riferimento per Glossario AWS.

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.