Guía del usuario

AWS IoT SiteWise

AWS IoT SiteWise: Guía del usuario

Table of Contents

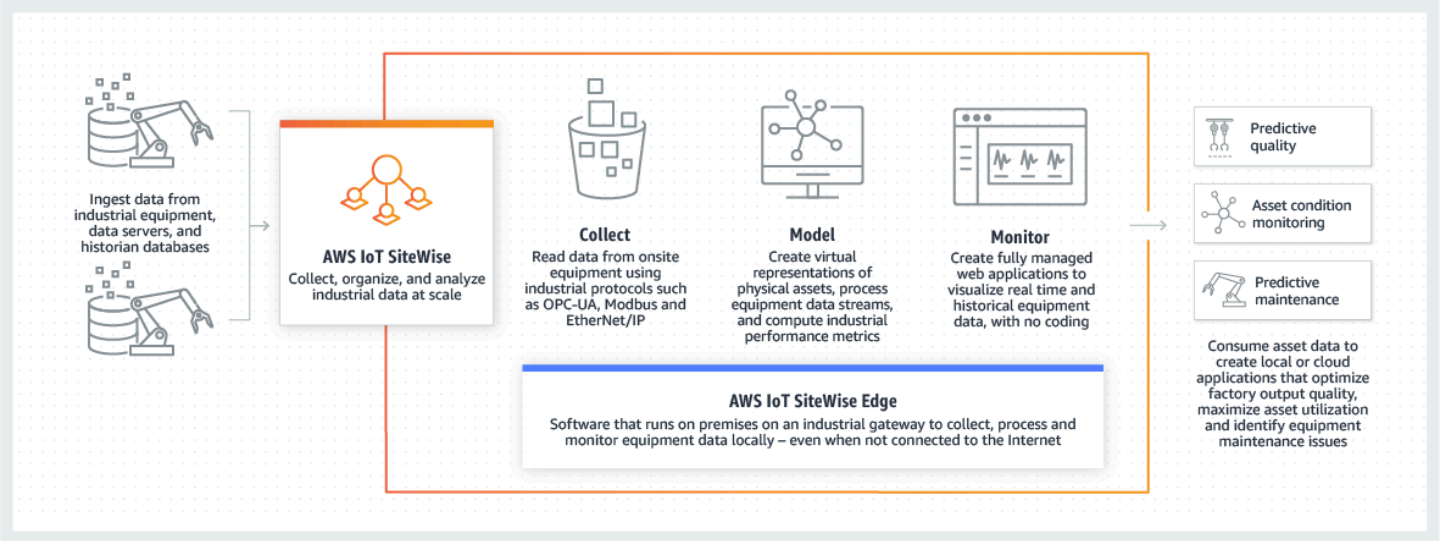
¿Qué es AWS IoT SiteWise?

AWS IoT SiteWise es un servicio gestionado que facilita la recopilación, el almacenamiento, la organización y la supervisión de los datos de los equipos industriales a escala para ayudarle a tomar mejores decisiones basadas en los datos. Se puede utilizar AWS IoT SiteWise para supervisar las operaciones en todas las instalaciones, calcular rápidamente las métricas comunes de rendimiento industrial y crear aplicaciones que analicen los datos de los equipos industriales para evitar problemas costosos con los equipos y reducir las brechas en la producción.

AWS IoT SiteWise Monitor permite a sus usuarios operativos crear rápidamente aplicaciones web para ver y analizar sus datos industriales en tiempo real. Puede obtener información sobre sus operaciones industriales configurando y monitoreando métricas como el tiempo medio entre fallas y la efectividad general del equipo (OEE).

AWS IoT SiteWise Edge es un componente AWS IoT SiteWise que permite la recopilación, el almacenamiento y el procesamiento de datos en dispositivos locales. Esto resulta útil si tiene acceso limitado a Internet o si necesita mantener la privacidad de sus datos.

El siguiente diagrama muestra la arquitectura básica de AWS IoT SiteWise:



Temas

- Cómo AWS IoT SiteWise funciona
- AWS IoT SiteWise conceptos
- Casos de uso para AWS IoT SiteWise

Cómo AWS IoT SiteWise funciona

AWS IoT SiteWise ofrece un marco de modelado de recursos que puede utilizar para crear representaciones de sus dispositivos, procesos e instalaciones industriales. Las representaciones de sus equipos y procesos se denominan modelos de activos en este documento AWS IoT SiteWise. Con los modelos de activos, usted define los datos sin procesar que se van a consumir y cómo procesarlos para convertirlos en métricas útiles. Cree y visualice activos y modelos para sus operaciones industriales en la AWS IoT SiteWise consola. También puede configurar modelos de activos para recopilar y procesar datos en la periferia o en la AWS nube.

Temas

Ingiera datos industriales

Comience a utilizarlos AWS IoT SiteWise ingiriendo datos industriales. La ingestión de los datos se realiza de varias maneras:

- Adquisición directa desde los servidores in situ: utilice protocolos como el OPC-UA para leer los datos directamente desde los dispositivos in situ. Implemente el software de puerta de enlace SiteWise Edge, compatible con AWS IoT Greengrass V2él, en una amplia gama de plataformas, como las puertas de enlace industriales comunes o los servidores virtuales. Puede conectar hasta 100 servidores OPC-UA a una sola puerta de enlace. AWS IoT SiteWise Para obtener más información, consulte SiteWise Requisitos de Edge Gateway.

  Tenga en cuenta que protocolos como Modbus TCP y EtherNet/IP (EIP) son compatibles con nuestra asociación en el contexto de. Domatica AWS IoT Greengrass V2
- Procesamiento de datos perimetrales con paquetes: mejore su pasarela SiteWise perimetral añadiendo paquetes para disponer de funciones perimetrales integrales. Con SiteWise Edge, disponible en AWS IoT Greengrass V2, el procesamiento de datos se ejecuta directamente in

situ antes de transmitirlos de forma segura a la AWS nube mediante una AWS IoT Greengrass transmisión. Para obtener más información, consulte Uso de los paquetes.

- Ingestión adaptativa a través de Amazon S3 con operaciones masivas: cuando trabaje con un gran número de activos o modelos de activos, utilice las operaciones masivas para importar y exportar recursos de forma masiva desde los buckets de Amazon S3. Para obtener más información, consulte Operaciones masivas con activos y modelos.
- Mensajes MQTT con reglas AWS IoT básicas: en el caso de los dispositivos conectados a AWS IoT Core que envían mensajes MQTT, utilice el motor de reglas AWS IoT Core para dirigir esos mensajes hacia ellos AWS IoT SiteWise. Si tiene dispositivos conectados a AWS IoT Core que envían mensajes MQTT, utilice el motor de reglas AWS IoT Core para enrutar esos mensajes. AWS IoT SiteWise Para obtener más información, consulte Ingerir datos mediante reglas AWS IoT Core.
- Ingesta de datos activada por eventos: utilice AWS IoT Events acciones para configurar la SiteWise acción de IoT AWS IoT Events para enviar datos AWS IoT SiteWise cuando se produzcan eventos. Para obtener más información, consulte Ingerir datos de AWS IoT Events.
- AWS IoT SiteWise API: sus aplicaciones en Edge o en la nube pueden enviar datos directamente a. AWS IoT SiteWise Para más información, consulte Ingerir datos mediante la API AWS IoT SiteWise

Modele los activos para contextualizar los datos recopilados

Después de ingerir los datos, puede usarlos para crear representaciones virtuales de sus activos, procesos e instalaciones mediante la creación de modelos de sus operaciones físicas. Un activo, que representa un dispositivo o un proceso, transmite flujos de datos a la AWS nube. Los activos también pueden significar agrupaciones lógicas de dispositivos. Las jerarquías se forman asociando activos para reflejar operaciones complejas. Estas jerarquías permiten a los activos acceder a los datos de los activos secundarios asociados. Los activos se crean a partir de modelos de activos. Los modelos de activos son estructuras declarativas que estandarizan los formatos de los activos. Reutilice los componentes de los activos para organizar y mantener sus modelos. Para más información, consulte Crear modelos de activos industriales

Con AWS IoT SiteWiseél, puede configurar sus activos para transformar los datos entrantes en métricas y transformaciones contextuales.

- Transforma el trabajo al recibir datos del equipo.
- Las métricas se calculan en los intervalos que usted defina.

Las métricas y las transformaciones se aplican tanto a activos individuales como a varios activos.AWS IoT SiteWise calcula automáticamente los agregados estadísticos más utilizados, como el promedio, la suma y el recuento, en varios períodos de tiempo relevantes para los datos, las métricas y las transformaciones de su equipo.

Los activos se pueden sincronizar utilizando. AWS IoT TwinMaker Para obtener más información, consulte

Para integrarlo AWS IoT SiteWiseAWS IoT TwinMaker, debe tener lo siguiente:

- AWS IoT SiteWisefunción vinculada al servicio configurada en su cuenta

- AWS IoT TwinMakerfunción vinculada a un servicio configurada en tu cuenta
- AWS IoT TwinMakerespacio de trabajo con un ID `IoTSiteWiseDefaultWorkspace` en tu cuenta en la región.

Para integrarlo mediante la AWS IoT SiteWise consola

Cuando veas el AWS IoT TwinMaker banner Integrar con en la consola, selecciona Conceder permiso. Los requisitos previos se crean en su cuenta.

Para realizar la integración mediante el AWS CLI

Para integrar AWS IoT SiteWise y AWS IoT TwinMaker utilizar elAWS CLI, introduzca los siguientes comandos:

1. Llame `CreateServiceLinkedRole` con un `AWSServiceName` `deiotsitewise.amazonaws.com`.

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

2. Llama `CreateServiceLinkedRole` con un `AWSServiceName` of `iottwinmaker.amazonaws.com`.

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

3. Llama `CreateWorkspace` con un `ID` of`IoTSiteWiseDefaultWorkspace`.

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

.

Analice mediante consultas, alarmas y predicciones

Analice los datos recopilados AWS IoT SiteWise mediante la ejecución de consultas y la configuración de alarmas. También puede usar Amazon Lookout para detectar automáticamente las anomalías en las métricas e identificar sus causas principales.

- Establezca alarmas específicas para alertar a su equipo cuando los equipos o los procesos se desvíen del rendimiento óptimo, lo que garantiza una rápida identificación y resolución de los problemas. Para obtener más información, consulte Monitoreo de datos con alarmas.
- Utilice las operaciones de la AWS IoT SiteWise API para consultar los valores actuales, históricos y agregados de sus propiedades de activos en intervalos de tiempo específicos. Para obtener más información, consulte Consulta datos de AWS IoT SiteWise.
- Utilice la detección de anomalías con Amazon Lookout for Equipment para identificar y visualizar los cambios en el equipo o en las condiciones de funcionamiento. Con la detección de anomalías, puede determinar las medidas de mantenimiento preventivo para sus operaciones. Esta integración permite a los clientes sincronizar datos entre AWS IoT SiteWise y Amazon Lookout for Equipment. Para obtener más información, consulte

> **Note**
>
> La detección de anomalías solo está disponible en las regiones en las que está disponible Amazon Lookout for Equipment.

Puede realizar la integración AWS IoT SiteWise con Amazon Lookout for Equipment para obtener información sobre sus equipos industriales mediante la detección de anomalías y el mantenimiento predictivo de los equipos industriales. Lookout for Equipment es un servicio de aprendizaje automático (ML) para monitorear equipos industriales que detecta un comportamiento anormal del equipo e identifica posibles fallas. Con Lookout for Equipment, puede implementar programas de mantenimiento predictivo e identificar los procesos de los equipos que no son óptimos. Para obtener más información sobre Lookout for Equipment, consulta ¿Qué es Amazon Lookout for Equipment? en la Guía del usuario de Amazon Lookout for Equipment.

Al crear una predicción para entrenar un modelo de aprendizaje automático a fin de detectar el comportamiento anómalo del equipo, AWS IoT SiteWise envía los valores de las propiedades

de los activos a Lookout for Equipment para entrenar un modelo de aprendizaje automático a fin de detectar el comportamiento anómalo del equipo. Para definir una definición de predicción en un modelo de activos, debe especificar las funciones de IAM necesarias para que Lookout for Equipment acceda a sus datos y las propiedades que envíe a Lookout for Equipment y envíe los datos procesados a Amazon S3. Para obtener más información, consulte Creación de modelos de activos.

Para integrar AWS IoT SiteWise Lookout for Equipment, realizarás los siguientes pasos de alto nivel:

- Añada una definición de predicción a un modelo de activos que describa las propiedades de las que quiere hacer un seguimiento. La definición de predicción es un conjunto reutilizable de medidas, transformaciones y métricas que se utiliza para crear predicciones sobre los activos que se basan en ese modelo de activos.
- Entrene la predicción en función de los datos históricos que proporcione.
- Programa la inferencia, que indica la AWS IoT SiteWise frecuencia con la que se debe ejecutar una predicción específica.

Una vez programada la inferencia, el modelo Lookout for Equipment monitorea los datos que recibe de su equipo y busca anomalías en el comportamiento del equipo. Puede ver y analizar los resultados en SiteWise Monitor, mediante las operaciones de la API AWS IoT SiteWise GET o la consola Lookout for Equipment. También puede crear alarmas utilizando detectores de alarmas del modelo de activos para alertarlo sobre el comportamiento anormal del equipo.

Temas

Añadir una definición de predicción (consola)

Para empezar a enviar los datos recopilados por AWS IoT SiteWise Lookout for Equipment, debes añadir AWS IoT SiteWise una definición de predicción a un modelo de activos.

Para añadir una definición de predicción a un modelo de AWS IoT SiteWise activos

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Modelos y seleccione el modelo de activo al que desee añadir la definición de predicción.
3. Elija Predicciones.
4. Seleccione Añadir definición de predicción.
5. Defina los detalles sobre la definición de predicción.
   a. Introduzca un nombre único y una descripción para la definición de predicción. Elija el nombre con cuidado, ya que después de crear la definición de predicción, no podrá cambiarlo.
   b. Cree o seleccione un rol de permisos de IAM que le permita AWS IoT SiteWise compartir los datos de sus activos con Amazon Lookout for Equipment. El rol debe tener las siguientes políticas de confianza y de IAM. Para obtener ayuda para crear el rol, consulte Crear un rol mediante políticas de confianza personalizadas (consola).

      Política de 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/*"
        }
    ]
}
```

Política de confianza

```
{
    "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. Elija Siguiente.

6. Selecciona los atributos de datos (medidas, transformaciones y métricas) que quieras enviar a Lookout for Equipment.

a. (Opcional) Seleccione las medidas.

b. (Opcional) Seleccione las transformaciones.

c. (Opcional) Seleccione las métricas.

d. Elija Siguiente.

7. Revise sus selecciones. Para añadir la definición de predicción al modelo de activos, en la página de resumen, seleccione Añadir definición de predicción.

También puede editar o eliminar una definición de predicción existente que tenga predicciones activas adjuntas.

Entrenar una predicción (consola)

Después de añadir una definición de predicción a un modelo de activos, puede entrenar las predicciones que se incluyen en sus activos.

Para entrenar una predicción en AWS IoT SiteWise

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Activos y seleccione el activo que desee supervisar.
3. Elija Predicciones.
4. Selecciona las predicciones que quieres entrenar.
5. En Acciones, selecciona Empezar a entrenar y haz lo siguiente:
   a. En Detalles de la predicción, selecciona un rol de permisos de IAM que te permita AWS IoT SiteWise compartir los datos de tus activos con Lookout for Equipment. Si necesitas crear un nuevo rol, selecciona Crear un nuevo rol.
   b. En la configuración de los datos de entrenamiento, introduce un rango de tiempo de datos de entrenamiento para seleccionar qué datos usar para entrenar la predicción.
   c. (Opcional) En el caso de las etiquetas de datos, proporciona un depósito y un prefijo de Amazon S3 que contengan los datos de etiquetado. Para obtener más información sobre el etiquetado de datos, consulta Cómo etiquetar tus datos en la Guía del usuario de Amazon Lookout for Equipment.
   d. Elija Siguiente.
6. (Opcional) Si quieres que la predicción esté activa en cuanto termine el entrenamiento, en Configuración avanzada, selecciona Activar automáticamente la predicción después del entrenamiento y, a continuación, haz lo siguiente:
   a. En Datos de entrada, en Frecuencia de carga de datos, define la frecuencia con la que se cargan los datos y, en Tiempo de retardo de compensación, define la cantidad de búfer que se va a utilizar.
   b. Elija Siguiente.
7. Revisa los detalles de la predicción y selecciona Guardar e iniciar.

Iniciar o detener la inferencia en una predicción (consola)

> **Note**
>
> Los cargos de Lookout for Equipment se aplican a las inferencias programadas con los datos transferidos AWS IoT SiteWise entre Lookout for Equipment y Lookout for Equipment. Para obtener más información, consulta los precios de Amazon Lookout for Equipment.

Si has añadido una predicción pero no has decidido activarla después del entrenamiento, debes activarla para que pueda empezar a monitorizar tus activos.

Para iniciar la inferencia de una predicción

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Activos y seleccione el activo al que se añade la predicción.
3. Elija Predicciones.
4. Seleccione las predicciones que desee activar.
5. En Acciones, elija Iniciar inferencia y haga lo siguiente:
   a. En Datos de entrada, en Frecuencia de carga de datos, defina la frecuencia con la que se cargan los datos y, en Tiempo de retardo de compensación, defina la cantidad de búfer que se va a utilizar.
   b. Selecciona Guardar e iniciar.

Para detener la inferencia de una predicción

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Activos y seleccione el activo al que se añade la predicción.
3. Elija Predicciones.
4. Seleccione las predicciones que desee detener.
5. En Acciones, elija Detener la inferencia.

Añadir una definición de predicción (CLI)

Para definir una definición de predicción en un modelo de activos nuevo o existente, puede usar AWS Command Line Interface (AWS CLI). Tras definir la definición de predicción en el modelo de activos, entrena y programa la inferencia de una predicción sobre un activo para detectar anomalías con Lookout for Equipment. AWS IoT SiteWise

Requisitos previos

Para completar estos pasos, debe tener un modelo de activos y crear al menos un activo. Para obtener más información, consulte Crear un modelo de activos (AWS CLI) y Crear un activo ()AWS CLI.

Si es la primera vez que lo usa AWS IoT SiteWise, debe llamar a la operación de la `CreateBulkImportJob` API para importar los valores de las propiedades de los activos AWS IoT SiteWise, que se utilizarán para entrenar el modelo. Para obtener más información, consulte Crea un trabajo de importación por lotes (AWS CLI).

Para añadir una definición de predicción

1. Cree un archivo denominado `asset-model-payload.json`. Siga los pasos de estas otras secciones para añadir los detalles de su modelo de activo al archivo, pero no envíe la solicitud para crear o actualizar el modelo de activo.
   - Para obtener más información sobre cómo crear un modelo de activos, consulte Crear un modelo de activos (AWS CLI)
   - Para obtener más información sobre cómo actualizar un modelo de activos existente, consulte Actualización de un modelo de activo o componente (AWS CLI)
2. Añada un modelo compuesto de Lookout for Equipment `assetModelCompositeModels` () al modelo de activos añadiendo el siguiente código.
   - *`Property`*Sustitúyalo por el ID de las propiedades que desee incluir. Para obtener esos identificadores, llame `DescribeAssetModel`.
   - *`RoleARN`*Sustitúyalo por el ARN de un rol de IAM que permita a Lookout for Equipment acceder a tus datos. 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. Cree el modelo de activo o actualice el modelo de activo existente. Realice una de las acciones siguientes:

- Para crear el modelo de activos, ejecute el siguiente comando:

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

- Ejecute el siguiente comando para actualizar el modelo de activo existente. *asset-model-id*Sustitúyalo por el ID del modelo de activos que desee actualizar.

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

Después de ejecutar el comando, anote `assetModelId` en la respuesta.

Entrenamiento de una predicción e inferencia inicial (CLI)

Ahora que la definición de predicción está definida, puede entrenar los activos en función de ella e iniciar la inferencia. Si quiere entrenar su predicción pero no iniciar la inferencia, pase a. Entrenamiento de una predicción (CLI) Para entrenar la predicción e iniciar la inferencia sobre el activo, necesitará el `assetId` recurso objetivo.

Para entrenar e iniciar la inferencia de la predicción

1. Ejecute el siguiente comando para encontrar la parte `assetModelCompositeModelId` inferior`assetModelCompositeModelSummaries`. *asset-model-id*Sustitúyalo por el ID del modelo de activos en el que lo creasteActualización de un modelo de activo o componente (AWS CLI).

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

2. Ejecute el siguiente comando para encontrar `actionDefinitionId` la `TrainingWithInference` acción. *asset-model-id*Sustitúyala por la ID utilizada en el paso anterior y *asset-model-composite-model-id*sustitúyala por la ID devuelta en el paso anterior.

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

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

3. Cree un archivo llamado `train-start-inference-prediction.json` y añada el siguiente código, sustituyendo el siguiente:
   - *asset-id*con el ID del activo de destino
   - *action-definition-id*con el ID de la TrainingWithInference acción
   - *StartTime*con el inicio de los datos de entrenamiento, proporcionados en segundos
   - *EndTime*con el final de los datos de entrenamiento, proporcionados en segundos de época

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

4. Ejecute el siguiente comando para iniciar el entrenamiento y la inferencia:

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

Entrenamiento de una predicción (CLI)

Ahora que la definición de predicción está definida, puede entrenar los activos en función de ella. Para entrenar la predicción sobre el activo, necesitará la `assetId` del recurso objetivo.

Para entrenar la predicción

1. Ejecuta el siguiente comando para encontrar la parte `assetModelCompositeModelId` inferior`assetModelCompositeModelSummaries`. *asset-model-id*Sustitúyalo por

el ID del modelo de activos en el que lo creasteActualización de un modelo de activo o componente (AWS CLI).

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

2. Ejecute el siguiente comando para encontrar `actionDefinitionId` la `Training` acción. *`asset-model-id`*Sustitúyala por la ID utilizada en el paso anterior y *`asset-model-composite-model-id`*sustitúyala por la ID devuelta en el paso anterior.

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

3. Cree un archivo llamado `train-prediction.json` y añada el siguiente código, sustituyendo el siguiente:
   - *`asset-id`*con el ID del activo de destino
   - *`action-definition-id`*con el ID de la acción formativa
   - *`StartTime`*con el inicio de los datos de entrenamiento, proporcionados en segundos
   - *`EndTime`*con el final de los datos de entrenamiento, proporcionados en segundos de época
   - (Opcional) *`BucketName`* con el nombre del depósito de Amazon S3 que contiene los datos de la etiqueta
   - (Opcional) *`Prefix`* con el prefijo asociado al bucket de Amazon S3.

   > **Note**
   >
   > Incluya el nombre y el prefijo del bucket o ninguno de ellos.

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

```
  \"labelInputConfiguration\": {\"bucketName\": \"BucketName\", \"prefix\":
  \"Prefix\"}}}"
```

```
}
}
```

4. Ejecute el siguiente comando para iniciar el entrenamiento:

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

Antes de poder iniciar la inferencia, se debe completar el entrenamiento. Para comprobar el estado de la formación, realice una de las siguientes acciones:

- Desde la consola, navega hasta el activo en el que se encuentra la predicción.

- Desde el AWS CLI, llame `BatchGetAssetPropertyValue` utilizando el `propertyId` de la `trainingStatus` propiedad.

Iniciar o detener la inferencia de una predicción (CLI)

Una vez entrenada la predicción, puedes iniciar la inferencia para decirle a Lookout for Equipment que comience a monitorizar tus activos. Para iniciar o detener la inferencia, necesitarás el recurso `assetId` objetivo.

Para iniciar la inferencia

1. Ejecute el siguiente comando para encontrar la parte `assetModelCompositeModelId` inferior`assetModelCompositeModelSummaries`. *`asset-model-id`*Sustitúyalo por el ID del modelo de activos en el que lo creasteActualización de un modelo de activo o componente (AWS CLI).

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

2. Ejecute el siguiente comando para encontrar `actionDefinitionId` la `Inference` acción. *`asset-model-id`*Sustitúyala por la ID utilizada en el paso anterior y *`asset-model-composite-model-id`*sustitúyala por la ID devuelta en el paso anterior.

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

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

3. Cree un archivo llamado `start-inference.json` y añada el siguiente código, sustituyendo el siguiente:
   - *`asset-id`*con el ID del activo de destino
   - *`action-definition-id`*con el ID de la acción de inferencia inicial
   - *`Offset`*con la cantidad de búfer a utilizar
   - *`Frequency`*con qué frecuencia se cargan los datos

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

4. Ejecute el siguiente comando para iniciar la inferencia:

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

Para detener la inferencia

1. Ejecute el siguiente comando para encontrar la parte `assetModelCompositeModelId` inferior`assetModelCompositeModelSummaries`. *`asset-model-id`*Sustitúyalo por el ID del modelo de activos en el que lo creasteActualización de un modelo de activo o componente (AWS CLI).

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

2. Ejecute el siguiente comando para encontrar `actionDefinitionId` la `Inference` acción. *`asset-model-id`*Sustitúyala por la ID utilizada en el paso anterior y *`asset-model-composite-model-id`*sustitúyala por la ID devuelta en el paso anterior.

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

3. Cree un archivo llamado `stop-inference.json` y añada el siguiente código, sustituyendo el siguiente:
   - *asset-id*con el ID del activo de destino
   - *action-definition-id*con el ID de la acción de inferencia inicial

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

4. Ejecute el siguiente comando para detener la inferencia:

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

.

Visualice las operaciones

Configure SiteWise Monitor para crear aplicaciones web para sus empleados operativos. Las aplicaciones web ayudan a los empleados a visualizar sus operaciones. Gestione distintos niveles de acceso para sus empleados mediante IAM Identity Center o IAM. Configure inicios de sesión y permisos únicos para cada empleado a fin de ver subconjuntos específicos de toda una operación industrial. AWS IoT SiteWise proporciona una guía de aplicación para que estos empleados aprendan a usar SiteWise Monitor.

Para obtener más información sobre la visualización de sus operaciones, consulte Monitorización de datos con AWS IoT SiteWise Monitor

Almacenar datos

Puede integrar el almacenamiento de series temporales con su lago de datos industriales. AWS IoT SiteWise tiene tres niveles de almacenamiento para datos industriales:

- Un nivel de almacenamiento activo que está optimizado para aplicaciones en tiempo real.
- Un nivel de almacenamiento en caliente optimizado para cargas de trabajo analíticas.
- Un nivel de almacenamiento en frío gestionado por el cliente que utiliza Amazon S3 para aplicaciones de datos operativos con alta tolerancia a la latencia.

AWS IoT SiteWise le ayuda a gestionar los costes de almacenamiento al mantener los datos recientes en el nivel de almacenamiento activo. A continuación, defina las políticas de retención de datos para mover los datos históricos a un almacenamiento de nivel caliente o frío. Para obtener más información, consulte

Puede configurarlo AWS IoT SiteWise para guardar sus datos en los siguientes niveles de almacenamiento:

Nivel de acceso frecuente

El nivel de almacenamiento activo es un almacenamiento de series temporales AWS IoT SiteWise gestionado. El nivel activo es más eficaz para los datos a los que se accede con frecuencia, con baja write-to-read latencia. Los datos almacenados en la capa activa son utilizados por aplicaciones industriales que necesitan un acceso rápido a los valores más recientes de las mediciones de su equipo. Esto incluye aplicaciones que visualizan métricas en tiempo real con un panel interactivo o aplicaciones que monitorean las operaciones y activan alarmas para identificar problemas de rendimiento.

De forma predeterminada, los datos ingresados AWS IoT SiteWise se almacenan en la capa activa. Puede definir un período de retención para el nivel activo, tras el cual AWS IoT SiteWise se transfieren los datos del nivel activo a un almacenamiento de nivel caliente o frío, según su configuración. Para obtener el mejor rendimiento y rentabilidad, configure el período de retención del nivel activo para que sea más largo que el tiempo que se tarda en recuperar los datos con frecuencia. Esto se usa para métricas, alarmas y escenarios de monitoreo en tiempo real. Si no se establece un período de retención, sus datos se almacenan indefinidamente en la capa activa.

Nivel cálido

El nivel de almacenamiento en caliente es un nivel AWS IoT SiteWise gestionado que resulta eficaz para el almacenamiento rentable de datos históricos. Se utiliza mejor para recuperar grandes volúmenes de datos con características de write-to-read latencia media. Utilice el nivel cálido para almacenar los datos históricos necesarios para grandes cargas de trabajo. Por ejemplo, se utiliza para la recuperación de datos para el análisis, las aplicaciones de inteligencia empresarial (BI), las herramientas de elaboración de informes y el entrenamiento de modelos de aprendizaje automático (ML). Si habilita el nivel de almacenamiento en frío, puede definir un período de retención del nivel cálido. Una vez finalizado el período de retención, AWS IoT SiteWise elimina los datos del nivel cálido.

Nivel inactivo

La capa de almacenamiento en frío utiliza un depósito de Amazon S3 para almacenar datos que se utilizan con poca frecuencia. Con la capa fría habilitada, AWS IoT SiteWise replica las series temporales, incluidas las mediciones, las métricas, las transformaciones y los agregados, y las definiciones de los modelos de activos cada 6 horas. La capa fría se utiliza para almacenar datos que toleran una latencia de lectura alta para los informes históricos y las copias de seguridad.

Temas

Configurar los ajustes de almacenamiento

Puede configurar los ajustes de almacenamiento para optar por el almacenamiento de nivel cálido gestionado por el servicio y también para replicar los datos en el nivel frío. Para obtener más información sobre el período de retención de los niveles cálido y caliente, consulteImpacto en la retención de datos. Al configurar los ajustes de almacenamiento, haga lo siguiente:

- Retención en la capa activa: establece un período de retención durante el cual tus datos se almacenan en la capa activa antes de que se eliminen y se transfieren al almacenamiento en capa caliente o almacenamiento en capa fría gestionado por el servicio en función de tu configuración de almacenamiento. AWS IoT SiteWise eliminará todos los datos de la capa activa que existieran

antes de que finalice el período de retención. Si no estableces un período de retención, tus datos se almacenan indefinidamente en la capa activa.

- Retención en la capa cálida: establece un período de retención para el tiempo que tus datos permanecerán almacenados en la capa cálida antes de que se eliminen del AWS IoT SiteWise almacenamiento y se trasladen al almacenamiento en la capa fría gestionada por el cliente. AWS IoT SiteWise elimina todos los datos de la capa cálida que existían antes de que finalizara el período de retención. Si no se establece un período de retención, sus datos se almacenan indefinidamente en el nivel cálido.

> **Note**
>
> Para mejorar el rendimiento de las consultas, establece un período de retención en el nivel activo con el almacenamiento en el nivel cálido.

Impacto de la retención de datos en el almacenamiento de nivel caliente y caliente

- Al reducir el período de retención del almacenamiento de capa activa, los datos se mueven permanentemente de la capa activa a la capa caliente o fría. Al reducir el período de retención de la capa cálida, los datos se mueven a la capa fría y se eliminan permanentemente de la capa cálida.
- Al aumentar el período de retención del almacenamiento de nivel caliente o caliente, el cambio afecta a los datos que se envíen a AWS IoT SiteWise partir de ese momento. AWS IoT SiteWise no recupera los datos del almacenamiento caliente o frío para poblarlos en el nivel activo. Por ejemplo, si el período de retención del almacenamiento de capa activa se establece inicialmente en 30 días y luego se aumenta a 60 días, el almacenamiento de capa activa tarda 30 días en contener datos de 60 días.

Temas

Configure los ajustes de almacenamiento para el nivel cálido (consola)

El siguiente procedimiento muestra cómo configurar los ajustes de almacenamiento para replicar los datos en el nivel cálido de la AWS IoT SiteWise consola.

Para configurar los parámetros de disponibilidad en la consola

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, en Configuración, seleccione Listas.
3. En la esquina superior derecha, elija Edit (Editar).
4. En la página Editar acción, haga lo siguiente:
5. Para configurar el nivel activo, haga lo siguiente:
   - Si quieres establecer un período de retención durante el cual tus datos se almacenarán en la capa activa antes de que se eliminen y se trasladen a la capa caliente gestionada por el servicio, selecciona Habilitar el período de retención.
   - Para configurar un período de retención, introduzca un número entero y elija una unidad. El periodo de retención debe ser mayor o igual a 30 días.

   AWS IoT SiteWise elimina todos los datos de la capa activa que sean anteriores al período de retención. Si no establece un período de retención, sus datos se almacenarán indefinidamente.
6. (Recomendado) Para la configuración del nivel cálido, haga lo siguiente:
   - Para optar por el almacenamiento en el nivel cálido, selecciona Confirmo la suscripción al almacenamiento en el nivel cálido para optar por el almacenamiento en el nivel cálido.
   - (Opcional) Para configurar un período de retención, introduce un número entero y elige una unidad. El período de retención debe ser superior o igual a 365 días.

   AWS IoT SiteWise elimina los datos del nivel cálido que existían antes del período de retención. Si no establece un período de retención, sus datos se almacenarán indefinidamente.

   > **Note**
   >
   > - Si opta por el nivel cálido, la configuración se muestra solo una vez.

- Para configurar la retención en el nivel caliente, debe tener un almacenamiento en el nivel caliente o frío. Para lograr una mayor rentabilidad y recuperar datos históricos, se AWS IoT SiteWise recomienda almacenar los datos a largo plazo en el nivel cálido.

- Para configurar la retención en el nivel cálido, debe tener un almacenamiento en el nivel frío.

7. Selecciona Guardar para guardar la configuración de almacenamiento.

En la sección AWS IoT SiteWise de almacenamiento, el almacenamiento de nivel cálido se encuentra en uno de estos estados:

- Habilitado: si sus datos existían antes del período de retención del nivel AWS IoT SiteWise activo, los mueve al nivel cálido».

- Desactivado: el almacenamiento en el nivel cálido está desactivado.

Configure los ajustes de almacenamiento para el nivel cálido (AWS CLI)

Puede configurar los ajustes de almacenamiento para mover los datos al nivel cálido mediante AWS CLI los siguientes comandos.

Para evitar anular la configuración existente, recupere la información de configuración de almacenamiento actual ejecutando el siguiente comando:

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

Example respuesta sin la configuración de capa fría existente

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

Example respuesta con la configuración de niveles fríos existente

```
{
      "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"
}
```

Configure los ajustes de almacenamiento para el nivel cálido con AWS CLI

Ejecute el siguiente comando para configurar los ajustes de almacenamiento. `file-name`Sustitúyalo por el nombre del archivo que contiene la configuración AWS IoT SiteWise de almacenamiento.


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

Example AWS IoT SiteWise configuración con niveles caliente y cálido

Example Respuesta

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

Si tiene activado el almacenamiento en niveles de refrigeración, consulteConfigure los ajustes de almacenamiento con AWS CLI un nivel de refrigeración existente.

Configure los ajustes de almacenamiento con AWS CLI un nivel de refrigeración existente

Configure los ajustes de almacenamiento utilizando AWS CLI el almacenamiento en capa fría existente

- Ejecute el siguiente comando para configurar los ajustes de almacenamiento. Sustituya *file-name* por el nombre del archivo que contiene la configuración de almacenamiento de AWS IoT SiteWise .

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

  Example AWS IoT SiteWise configuración de almacenamiento

  - Sustituya *bucketname* por el nombre del bucket de Amazon S3.
  - Sustituya *prefix* por el prefijo de Amazon S3.
  - *aws-account-id*Sustitúyala por tu ID de AWS cuenta.
  - Sustituya el *nombre del rol* por el nombre del rol de acceso de Amazon S3 que permite AWS IoT SiteWise enviar datos a Amazon S3.
  - Sustituya *hot-tier-retention-in-days* por un número entero mayor o igual a 30 días.
  - Sustituya *warm-tier-retention-in-days* por un número entero mayor o igual a 365 días.

> **Note**
>
> AWS IoT SiteWise eliminará todos los datos del nivel cálido que sean anteriores al período de retención del nivel frío. Si no establece un período de retención, sus datos se almacenarán indefinidamente.

```
{
      "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 Respuesta

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

Configure los ajustes de almacenamiento para el nivel frío (consola)

El siguiente procedimiento muestra cómo configurar los ajustes de almacenamiento para replicar los datos en la capa fría de la AWS IoT SiteWise consola.

Para configurar los parámetros de disponibilidad en la consola

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, en Configuración, seleccione Listas.
3. En la esquina superior derecha, elija Edit (Editar).
4. En la página Editar acción, haga lo siguiente:
   a. En la Configuración de almacenamiento, seleccione Habilitar el almacenamiento en el nivel inactivo. El almacenamiento en el nivel inactivo está desactivado de forma predeterminada.
   b. En Ubicación del bucket de S3, introduzca el nombre de un bucket de Amazon S3 existente y un prefijo.

      > **Note**
      >
      > - Amazon S3 utiliza el prefijo como nombre de carpeta en el bucket de Amazon S3. El prefijo debe tener entre 1 y 255 caracteres y terminar con una barra diagonal (/). Sus AWS IoT SiteWise datos se guardan en esta carpeta.
      > - Si no dispone de un bucket de Amazon S3, seleccione Ver y, a continuación, cree uno en la consola de Amazon S3. Para obtener más información, consulte Creación del primer bucket de S3 en la Guía del usuario de Amazon S3.

   c. Para rol de acceso a S3, realice una de las operaciones siguientes:
      - Si selecciona Crear un rol a partir de una plantilla AWS gestionada, crea AWS automáticamente un rol de IAM que permite AWS IoT SiteWise enviar datos a Amazon S3.
      - Elija Usar un rol existente y, a continuación, elija el rol que creó de la lista.

      > **Note**
      >
      > - Debe usar el mismo nombre de bucket de Amazon S3 para la Ubicación del bucket de S3 que utilizó en el paso anterior y en su política de IAM.
      > - Asegúrese de que el rol tenga los permisos que se muestran en el siguiente ejemplo.

Example política de permisos:

```
{
      "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/*"
              ]
          }
      ]
  }
```

Reemplace *bucket-name* con el nombre de su bucket de Amazon S3.

d. Para configurar el nivel activo, consulte el paso 5 deConfigure los ajustes de almacenamiento para el nivel cálido (consola).

e. (Opcional) Para la integración de AWS IoT Analytics , haga lo siguiente.

   i. Si desea utilizarlo AWS IoT Analytics para consultar sus datos, elija Almacén de AWS IoT Analytics datos activado.

   ii. AWS IoT SiteWise genera un nombre para el banco de datos o puede introducir un nombre diferente.

   AWS IoT SiteWise crea automáticamente un almacén de datos AWS IoT Analytics para guardar sus datos. Para consultar los datos, puede utilizarlos AWS IoT Analytics para crear conjuntos de datos. Para obtener más información, consulte Trabajar con AWS IoT SiteWise datos en la Guía del AWS IoT Analytics usuario.

f. Seleccione Guardar.

En la sección Almacenamiento de AWS IoT SiteWise , el Almacenamiento en el nivel inactivo puede tener uno de los siguientes valores:

- Habilitado: AWS IoT SiteWise replica los datos en el bucket de Amazon S3 especificado.

- Habilitación: AWS IoT SiteWise está procesando su solicitud para habilitar el almacenamiento en capas frías. Este proceso puede tardar varios minutos en completarse.
- Enable_Failed: no se ha AWS IoT SiteWise podido procesar tu solicitud para habilitar el almacenamiento en capa fría. Si has habilitado AWS IoT SiteWise el envío de registros a Amazon CloudWatch Logs, puedes usar estos registros para solucionar problemas. Para obtener más información, consulte Supervisión con Amazon CloudWatch Logs.
- Deshabilitado: el almacenamiento en el nivel inactivo está desactivado.

Configure los ajustes de almacenamiento para la capa inactiva ()AWS CLI

El siguiente procedimiento muestra cómo configurar los ajustes de almacenamiento para replicar datos en el nivel inactivo mediante AWS CLI.

Para configurar los ajustes de almacenamiento mediante AWS CLI

1. Para exportar datos a un bucket de Amazon S3 en su cuenta, ejecute el siguiente comando para configurar los ajustes de almacenamiento. Sustituya *el nombre de archivo* por el nombre del archivo que contiene la configuración de AWS IoT SiteWise almacenamiento.

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

   Example AWS IoT SiteWise configuración de almacenamiento

   - Sustituya *bucketname* por el nombre del bucket de Amazon S3.
   - Sustituya *prefix* por el prefijo de Amazon S3.
   - *aws-account-id*Sustitúyala por tu ID de AWS cuenta.
   - Sustituya el *nombre del rol* por el nombre del rol de acceso de Amazon S3 que permite AWS IoT SiteWise enviar datos a Amazon S3.
   - *retention-in-days*Sustitúyalo por un número entero que sea mayor o igual a 30 días.

   ```
   {
         "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

- Debe usar el mismo nombre de bucket de Amazon S3 en la configuración de AWS IoT SiteWise almacenamiento y en la política de IAM.
- Asegúrese de que el rol tenga los permisos que se muestran en el siguiente ejemplo. Example política de permisos:

```
{
      "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/*"
              ]
          }
      ]
  }
```

Reemplace *bucket-name* con el nombre de su bucket de Amazon S3.

Example Respuesta

```
{
    "storageType": "MULTI_LAYER_STORAGE",
    "retentionPeriod": {
        "numberOfDays": 100,
        "unlimited": false
    },
    "configurationStatus": {
        "state": "UPDATE_IN_PROGRESS"
    }
}
```

> **Note**
>
> La actualización de la configuración de AWS IoT SiteWise almacenamiento puede tardar unos minutos.

2. Para recuperar la información de configuración del almacenamiento, ejecute el siguiente comando.

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

Example respuesta

```
{
      "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. Para detener la exportación de datos al bucket de Amazon S3, ejecute el siguiente comando para configurar los ajustes de almacenamiento.

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

> **Note**
>
> De forma predeterminada, los datos solo se almacenan en la capa activa de AWS IoT SiteWise.

Example Respuesta

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

4. Para recuperar la información de configuración del almacenamiento, ejecute el siguiente comando.

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

Example respuesta

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

```
}
```

(Opcional) Cree un almacén AWS IoT Analytics de datos (AWS CLI)

Un AWS IoT Analytics banco de datos es un repositorio escalable y consultable que recibe y almacena datos. Puede usar la AWS IoT SiteWise consola o AWS IoT Analytics las API para crear un banco de AWS IoT Analytics datos para guardar AWS IoT SiteWise los datos. Para consultar los datos, cree conjuntos de datos mediante AWS IoT Analytics. Para obtener más información, consulte Trabajo con datos de AWS IoT SiteWise en la Guía del usuario de AWS IoT Analytics .

Los siguientes pasos se utilizan AWS CLI para crear un almacén de datos en AWS IoT Analytics.

Ejecute el siguiente comando para crear un almacén de datos. Sustituya *file-name* por el nombre del archivo que contiene la configuración del almacén de datos.

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

> **Note**
>
> - Debe especificar el nombre de un bucket de Amazon S3 existente. Si no dispone de un bucket de Amazon S3, cree uno primero. Para obtener más información, consulte Creación del primer bucket de S3 en la Guía del usuario de Amazon S3.

- Debe usar el mismo nombre de bucket de Amazon S3 en la configuración de AWS IoT SiteWise almacenamiento, la política de IAM y la configuración del almacén de AWS IoT Analytics datos.

Example AWS IoT Analytics configuración del almacén de datos

Sustituya *data-store-name* y *s3-bucket-name por el nombre del* almacén de AWS IoT Analytics datos y el nombre del bucket de Amazon S3.

```
{
    "datastoreName": "data-store-name",
    "datastoreStorage": {
        "iotSiteWiseMultiLayerStorage": {
            "customerManagedS3Storage": {
```

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

Example Respuesta

```
{
    "datastoreName": "datastore_IoTSiteWise_demo",
    "datastoreArn": "arn:aws:iotanalytics:us-west-2:123456789012:datastore/
datastore_IoTSiteWise_demo",
    "retentionPeriod": {
        "numberOfDays": 90,
        "unlimited": false
    }
}
```

Solucionar problemas de configuración de almacenamiento

Utilice la siguiente información como ayuda para solucionar problemas con la configuración de almacenamiento.

Problemas

- Error: el bucket no existe
- Error: acceso denegado a la ruta de Amazon S3
- Error: no se puede asumir el ARN del rol

- Asegúrese de utilizar el mismo bucket de Amazon S3 que especificó en la política de IAM.

- Asegúrese de que el rol tenga los permisos que se muestran en el siguiente ejemplo.

  Example política de permisos

```
{
      "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/*"
              ]
          }
      ]
  }
```

  Reemplace *bucket-name* con el nombre de su bucket de Amazon S3.

Error: no se puede asumir el ARN del rol

Solución: no AWS IoT SiteWise pude asumir la función de IAM en su nombre. Asegúrese de que su rol confíe en el siguiente servicio: `iotsitewise.amazonaws.com`. Para obtener más información, consulte No puedo asumir un rol en la Guía del usuario de IAM.

Error: no se pudo acceder al bucket de Amazon S3 entre regiones

Solución: el bucket de Amazon S3 que especificó se encuentra en una AWS región diferente. Asegúrese de que su depósito de Amazon S3 y AWS IoT SiteWise sus activos estén en la misma región.

Rutas de archivos y esquemas de datos guardados en el nivel inactivo

AWS IoT SiteWise almacena sus datos en la capa fría replicando series temporales, incluidas las mediciones, las métricas, las transformaciones y los agregados, así como las definiciones de activos y modelos de activos. A continuación se describen las rutas de los archivos y los esquemas de datos que se envían al nivel inactivo.

Temas

Datos del equipo (mediciones)

AWS IoT SiteWise exporta los datos del equipo (mediciones) a la capa fría una vez cada seis horas. Los datos sin procesar se guardan en el nivel inactivo en formato Apache AVRO (`.avro`).

Ruta de archivo

AWS IoT SiteWise almacena los datos del equipo (mediciones) en la capa fría mediante la siguiente plantilla.

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

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

Cada ruta de archivo a datos sin procesar en Amazon S3 contiene los siguientes componentes.

`keyPrefix`	El prefijo de Amazon S3 que especificó en la configuración AWS IoT SiteWise de almacenamiento. Amazon S3 utiliza el prefijo como nombre de carpeta en el bucket.

`raw`	La carpeta que almacena los datos de serie temporal del equipo (mediciones). La carpeta `raw` se guarda en la carpeta de prefijos.
`seriesBucket`	Un número hexadecimal entre 00 y ff. Este número se deriva de `timeSeriesId` . Esta partición se utiliza para aumentar el rendimiento cuando se AWS IoT SiteWise escribe en la capa fría. Cuando se utiliza Amazon Athena para ejecutar consultas, la partición puede servir para realizar particiones refinadas a fin de mejorar la precisión de las consultas. `seriesBucket` y `timeSeriesBucket` son el mismo número en los metadatos del activo.
`startYear`	El año de la hora de inicio exclusiva asociada a los datos de serie temporal.
`startMonth`	El mes de la hora de inicio exclusiva asociada a los datos de serie temporal.
`startDay`	El día del mes de la hora de inicio exclusiva asociada a los datos de serie temporal.

`fileName`	El nombre del archivo utiliza el carácter de subrayado (_) como delimitador para separar lo siguiente:
	• El prefijo `raw`. • El valor `timeSeriesId` . • La marca temporal de fecha de inicio exclusiva asociada a los datos de serie temporal. • La calidad de datos. Valores aceptados: `GOOD`, `BAD` y `UNCERTAIN` . Para obtener más información, consulte AssetPropertyValuela referencia de la AWS IoT SiteWise API.
	El archivo se guarda en el formato `.avro` mediante la compresión Snappy.

Componente de ruta	Descripción

Example ruta del archivo a los datos sin procesar en el nivel inactivo

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

Campos

El esquema de datos sin procesar que se exporta al nivel inactivo contiene los siguientes campos.

`seriesId`	`string`	N/A	El identificador que identifica los datos de serie temporal del equipo (medicion

			es). Puede usar este campo para unir datos sin procesar y metadatos de activos en las consultas.
`timeInSeconds`	`long`	N/A	La marca temporal, en segundos, en formato de tiempo Unix. Los datos fraccionarios de nanosegundos los proporciona `offsetInNanos` .
`offsetInNanos`	`long`	N/A	El desfase de nanosegundos procedente de `timeInSeconds` .
`quality`	`string`	N/A	La calidad del valor de la serie temporal.
`doubleValue`	`double` o `null`	`null`	Datos de serie temporal de tipo doble (número de punto flotante).
`stringValue`	`string` o `null`	`null`	Datos de serie temporal de tipo cadena (secuencia de caracteres).

`integerValue`	`int` o `null`	`null`	Datos de serie temporal de tipo entero (número entero).
`booleanValue`	`boolean` o `null`	`null`	Datos de serie temporal de tipo booleano (verdadero o falso).
`jsonValue`	`string` o `null`	`null`	Datos de serie temporal de tipo JSON (tipos de datos complejos almacenados como una cadena).
`recordVersion`	`long` o `null`	`null`	El número de versión para el registro. Puede usar el número de versión para seleccionar el registro más reciente. Los registros más recientes tienen números de versión más grandes.

Nombre del campo	Tipos admitidos	Tipo predeterminado	Descripción

Example datos sin procesar en el nivel inactivo

```
{"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
```


Métricas, transformaciones y agregados

AWS IoT SiteWise exporta métricas, transforma y agrega a la capa fría una vez cada seis horas. Las métricas, las transformaciones y los agregados se guardan en el nivel inactivo en el formato Apache AVRO (`.avro`).

Ruta de archivo

AWS IoT SiteWise almacena las métricas, las transformaciones y los agregados en la capa fría mediante la siguiente plantilla.

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

Cada ruta de archivo a las métricas, las transformaciones y los agregados en Amazon S3 contiene los siguientes componentes.

`keyPrefix`	El prefijo de Amazon S3 que especificó en la configuración AWS IoT SiteWise de almacenamiento. Amazon S3 utiliza el prefijo como nombre de carpeta en el bucket.
`agg`	La carpeta que almacena los datos de serie temporal de las métricas. La carpeta `agg` se guarda en la carpeta de prefijos.
`seriesBucket`	Un número hexadecimal entre 00 y ff. Este

	partición se utiliza para aumentar el rendimiento cuando se AWS IoT SiteWise escribe en la capa fría. Cuando se utiliza Amazon Athena para ejecutar consultas, la partición puede servir para realizar particiones refinadas a fin de mejorar la precisión de las consultas. `seriesBucket` y `timeSeriesBucket` son el mismo número en los metadatos del activo.
`startYear`	El año de la hora de inicio exclusiva asociada a los datos de serie temporal.
`startMonth`	El mes de la hora de inicio exclusiva asociada a los datos de serie temporal.
`startDay`	El día del mes de la hora de inicio exclusiva asociada a los datos de serie temporal.

`fileName`	El nombre del archivo utiliza el carácter de subrayado (_) como delimitador para separar lo siguiente:
	• El prefijo `raw`. • El valor `timeSeriesId` . • La marca temporal de fecha de inicio exclusiva asociada a los datos de serie temporal. • La calidad de datos. Valores aceptados: `GOOD`, `BAD` y `UNCERTAIN` . Para obtener más información, consulte AssetPropertyValuela referencia de la AWS IoT SiteWise API.
	El archivo se guarda en el formato `.avro` mediante la compresión Snappy.

Componente de ruta	Descripción

Example ruta del archivo a las métricas en el nivel inactivo

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

Campos

El esquema de las métricas, las transformaciones y los agregados que se exportan al nivel inactivo contiene los siguientes campos.

`seriesId`	`string`	N/A	El ID que identifica los datos de serie temporal procedent

			es del equipo, de las métricas o de las transformaciones. Puede usar este campo para unir datos sin procesar y metadatos de activos en las consultas.
`timeInSeconds`	`long`	N/A	La marca temporal, en segundos, en formato de tiempo Unix. Los datos fraccionarios de nanosegundos los proporciona `offsetInNanos` .
`offsetInNanos`	`long`	N/A	El desfase de nanosegundos procedente de `timeInSeconds` .
`quality`	`string`	N/A	La calidad con la que se filtran los datos de los activos.
`resolution`	`string`	N/A	El intervalo de tiempo durante el que se van a agregar los datos.
`count`	`double` o `null`	`null`	El número total de puntos de datos para las variables dadas durante el intervalo de tiempo actual.

Nombre del campo	Tipos admitidos	Tipo predeterminado	Descripción
`average`	`double` o `null`	`null`	La media de los valores de las variables dadas durante el intervalo de tiempo actual.
`min`	`double` o `null`	`null`	El mínimo de los valores de las variables dadas durante el intervalo de tiempo actual.
`max`	`boolean` o `null`	`null`	El máximo de los valores de las variables dadas durante el intervalo de tiempo actual.
`sum`	`string` o `null`	`null`	La suma de los valores de las variables dadas durante el intervalo de tiempo actual.
`recordVersion`	`long` o `null`	`null`	El número de versión para el registro. Puede usar el número de versión para seleccionar el registro más reciente. Los registros más recientes tienen números de versión más grandes.

Example Datos métricos en el nivel inactivo


```
{"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}
```


Metadatos de los activos

Cuando habilitas AWS IoT SiteWise la exportación de datos a la capa fría por primera vez, los metadatos de los activos se exportan a la capa fría. Tras la configuración inicial, AWS IoT SiteWise

`keyPrefix`	El prefijo de Amazon S3 que especificó en la configuración de almacenamiento AWS IoT SiteWise s. Amazon S3 utiliza el prefijo como nombre de carpeta en el bucket.
`asset_metadata`	La carpeta que almacena los metadatos de los activos. La carpeta `asset_metadata` se guarda en la carpeta de prefijos.
`fileName`	El nombre del archivo utiliza el carácter de subrayado (_) como delimitador para separar lo siguiente: • El prefijo `asset`. • El valor `assetId`. El archivo se guarda en el formato `.ndjson`.

Componente de ruta	Descripción

Example ruta del archivo a los metadatos de los activos en el nivel inferior

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

Campos

El esquema de metadatos de activos que se exporta al nivel inactivo contiene los siguientes campos.

`assetId`	El ID del activo.
`assetName`	Nombre del activo.
`assetExternalId`	El ID externo del activo.
`assetModelId`	Id. del modelo de activo usado para crear el activo.

`assetModelName`	El nombre del modelo del activo.
`assetModelExternalId`	El identificador externo del modelo de activo.
`assetPropertyId`	El ID de la propiedad del activo.
`assetPropertyName`	El nombre de la propiedad del activo.
`assetPropertyExternalId`	El identificador externo de la propiedad del activo.
`assetPropertyDataType`	El tipo de datos de la propiedad del activo.
`assetPropertyUnit`	La unidad que usa la propiedad del activo (por ejemplo, `Newtons` y `RPM`).
`assetPropertyAlias`	El alias que identifica la propiedad del activo, como una ruta de flujo de datos del servidor OPC-UA (por ejemplo, `/company/windfarm/3/turbine/7/temperature`).
`timeSeriesId`	El ID que identifica los datos de serie temporal procedentes del equipo, de las métricas o de las transformaciones. Puede usar este campo para unir datos sin procesar y metadatos de activos en las consultas.

`timeSeriesBucket`	Un número hexadecimal entre 00 y ff. Este número se deriva de `timeSeriesId` . Esta partición se utiliza para aumentar el rendimiento cuando se AWS IoT SiteWise escribe en la capa fría. Cuando se utiliza Amazon Athena para ejecutar consultas, la partición puede servir para realizar particiones refinadas a fin de mejorar la precisión de las consultas. `timeSeriesBucket` y `seriesBucket` son el mismo número en la ruta del archivo a los datos sin procesar.
`assetCompositeModelId`	El ID del modelo compuesto.
`assetCompositeModelExternalId`	El identificador externo del modelo compuesto.
`assetCompositeModelDescription`	La descripción del modelo compuesto.
`assetCompositeModelName`	El nombre del modelo compuesto.
`assetCompositeModelType`	El tipo del modelo compuesto. Para los modelos compuestos de alarma, este tipo es `AWS/ALARM` .
`assetCreationDate`	La fecha en que se creó el activo, en formato de tiempo UNIX.
`assetLastUpdateDate`	La fecha en que el activo se actualizó por última vez, en fecha de inicio Unix.
`assetStatusErrorCode`	Código de error.
`assetStatusErrorMessage`	Mensaje de error.
`assetStatusState`	El estado actual del activo.
Nombre del campo	Descripción

Example metadatos de activos en el nivel inactivo


```
  {"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
```

el modelo de activos o en las definiciones de activos. Los metadatos de la jerarquía de activos se guardan en la capa fría en el formato JSON (`.ndjson`) delimitado por líneas nuevas.

Al llamar a la API, se recupera un identificador externo de la jerarquía, el activo de destino o el DescribeAssetactivo de origen.

Ruta de archivo

AWS IoT SiteWise almacena los metadatos de la jerarquía de activos en la capa fría mediante la siguiente plantilla.

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

Cada ruta de archivo a los metadatos de jerarquía de los activos en el nivel inactivo contiene los siguientes componentes.

Componente de ruta	Descripción
`keyPrefix`	El prefijo de Amazon S3 que especificó en la configuración AWS IoT SiteWise de almacenamiento. Amazon S3 utiliza el prefijo como nombre de carpeta en el bucket.
`asset_hierarchy_metadata`	La carpeta que almacena los metadatos de jerarquía de los activos. La carpeta `asset_hierarchy_metadata` se guarda en la carpeta de prefijos.
`fileName`	El nombre del archivo utiliza el carácter de subrayado (_) como delimitador para separar lo siguiente: • El valor `parentAssetId` . • El valor `hierarchyId` . El archivo se guarda en el formato `.ndjson`.

Example ruta del archivo a los metadatos de la jerarquía de activos en el nivel inactivo

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

Campos

El esquema de los metadatos de la jerarquía de activos que se exporta al nivel inactivo contiene los siguientes campos.

Nombre del campo	Descripción
`sourceAssetId`	El ID del activo de origen en esta relación de activos.
`targetAssetId`	El ID del activo de destino en esta relación de activos.
`hierarchyId`	El ID de la jerarquía.
`associationType`	El tipo de asociación de esta relación de activos.
	El valor debe ser `CHILD`. El activo de destino es una entidad secundaria del activo de origen.

Example los metadatos de jerarquía de los activos en el nivel inactivo

```
{"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"}
```


Para ver los datos en el nivel inactivo

1. Vaya a la consola de Amazon S3

2. En el panel de navegación, elija Buckets y, a continuación, elija el bucket de Amazon S3.

3. Navegue hasta la carpeta que contiene los datos sin procesar, los metadatos de los activos o los metadatos de jerarquía de los activos.

4. Seleccione los archivos y, a continuación, en Acciones, elija Descargar.

Almacenamiento de archivos índice de datos

AWS IoT SiteWise utiliza estos archivos para optimizar el rendimiento de las consultas de datos. Aparecen en u bucket de Amazon S3, pero no es necesario que los utilice.

Ruta de archivo

AWS IoT SiteWise almacena los archivos de índice de datos en la capa fría mediante la siguiente plantilla.

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

Example ruta del archivo al archivo índice de almacenamiento de datos

```
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
```

.

También puede importar y exportar metadatos de activos. Para más información, consulte

Cuando habilitas AWS IoT SiteWise la exportación de datos a la capa fría por primera vez, los metadatos de los activos se exportan a la capa fría. Tras la configuración inicial, AWS IoT SiteWise exporta los metadatos de los activos al nivel solo cuando se cambian las definiciones del modelo de activos o las definiciones de activos. Los metadatos de los activos se guardan en la capa fría en el formato JSON (`.ndjson`) delimitado por líneas nuevas.

Ruta de archivo

AWS IoT SiteWise almacena los metadatos de los activos en la capa fría mediante la siguiente plantilla.

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

Cada ruta de archivo a los metadatos de los activos en el nivel inactivo contiene los siguientes componentes.

Componente de ruta	Descripción
`keyPrefix`	El prefijo de Amazon S3 que especificó en la configuración de almacenamiento AWS IoT SiteWise s. Amazon S3 utiliza el prefijo como nombre de carpeta en el bucket.
`asset_metadata`	La carpeta que almacena los metadatos de los activos. La carpeta `asset_metadata` se guarda en la carpeta de prefijos.
`fileName`	El nombre del archivo utiliza el carácter de subrayado (_) como delimitador para separar lo siguiente: • El prefijo `asset`. • El valor `assetId`. El archivo se guarda en el formato `.ndjson`.

Example ruta del archivo a los metadatos de los activos en el nivel inferior

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

Campos

El esquema de metadatos de activos que se exporta al nivel inactivo contiene los siguientes campos.

`assetId`	El ID del activo.

`assetName`	Nombre del activo.
`assetExternalId`	El ID externo del activo.
`assetModelId`	Id. del modelo de activo usado para crear el activo.
`assetModelName`	El nombre del modelo del activo.
`assetModelExternalId`	El identificador externo del modelo de activo.
`assetPropertyId`	El ID de la propiedad del activo.
`assetPropertyName`	El nombre de la propiedad del activo.
`assetPropertyExternalId`	El identificador externo de la propiedad del activo.
`assetPropertyDataType`	El tipo de datos de la propiedad del activo.
`assetPropertyUnit`	La unidad que usa la propiedad del activo (por ejemplo, `Newtons` y `RPM`).
`assetPropertyAlias`	El alias que identifica la propiedad del activo, como una ruta de flujo de datos del servidor OPC-UA (por ejemplo, `/company/windfarm/3/turbine/7/temperature`).
`timeSeriesId`	El ID que identifica los datos de serie temporal procedentes del equipo, de las métricas o de las transformaciones. Puede usar este campo para unir datos sin procesar y metadatos de activos en las consultas.

`timeSeriesBucket`	Un número hexadecimal entre 00 y ff. Este número se deriva de `timeSeriesId` . Esta partición se utiliza para aumentar el rendimiento cuando se AWS IoT SiteWise escribe en la capa fría. Cuando se utiliza Amazon Athena para ejecutar consultas, la partición puede servir para realizar particiones refinadas a fin de mejorar la precisión de las consultas. `timeSeriesBucket` y `seriesBucket` son el mismo número en la ruta del archivo a los datos sin procesar.
`assetCompositeModelId`	El ID del modelo compuesto.
`assetCompositeModelExternalId`	El identificador externo del modelo compuesto.
`assetCompositeModelDescription`	La descripción del modelo compuesto.
`assetCompositeModelName`	El nombre del modelo compuesto.
`assetCompositeModelType`	El tipo del modelo compuesto. Para los modelos compuestos de alarma, este tipo es `AWS/ALARM` .
`assetCreationDate`	La fecha en que se creó el activo, en formato de tiempo UNIX.
`assetLastUpdateDate`	La fecha en que el activo se actualizó por última vez, en fecha de inicio Unix.
`assetStatusErrorCode`	Código de error.
`assetStatusErrorMessage`	Mensaje de error.
`assetStatusState`	El estado actual del activo.
Nombre del campo	Descripción

Example metadatos de activos en el nivel inactivo


```
 {"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-
```

Integración con otros servicios de

AWS IoT SiteWise se integra con varios AWS servicios para desarrollar una AWS IoT solución completa en la AWS nube. Para obtener más información, consulte Interacción con otros AWS servicios

AWS IoT SiteWise conceptos

Los siguientes son los conceptos básicos de AWS IoT SiteWise:

Agregado

Los agregados son métricas o mediciones fundamentales que AWS IoT SiteWise se calculan automáticamente para todos los datos de series temporales. Para obtener más información, consulte Consulta de agregados de propiedades de activos.

activo

Cuando introduce o ingiere datos de su equipo industrial, cada uno AWS IoT SiteWise de sus dispositivos, equipos y procesos se muestra como activos. Cada activo tiene datos asociados. Por ejemplo, un equipo puede tener un número de serie, una ubicación, una marca y modelo y una fecha de instalación. También puede tener valores de series temporales para la disponibilidad, el rendimiento, la calidad, la temperatura, la presión y más. Agrupe los activos en jerarquías para permitir que los activos accedan a los datos almacenados en sus activos secundarios. Para obtener más información, consulte Crear modelos de activos industriales.

Jerarquía de activos

Configure jerarquías de activos para crear representaciones lógicas de sus operaciones industriales. Para ello, defina una jerarquía en un modelo de activos y asocie los activos creados a partir de ese modelo con la jerarquía especificada. Las métricas de los activos principales pueden combinar datos de las propiedades de los activos secundarios, lo que le permite calcular métricas que ofrecen información sobre sus operaciones generales o sobre una parte específica de ellas. Para obtener más información, consulte Definición de jerarquías de modelos de activos.

Modelo de activos

Cada activo se crea mediante un modelo de activos. Los modelos de activos son estructuras que definen y estandarizan el formato de sus activos. Garantizan la coherencia de la información en varios activos del mismo tipo, lo que permite gestionar los datos de activos que representan grupos de dispositivos. En cada modelo de activos, puede definir atributos, entradas de serie

temporal (medidas), transformaciones de serie temporal (transformaciones), agregaciones de serie temporal (métricas) y jerarquías de activos. Para obtener más información, consulte Crear modelos de activos industriales.

Decida dónde se procesan las propiedades de su modelo de activos configurándolo para la periferia. Utilice esta función para gestionar y supervisar los datos de los activos en sus dispositivos locales.

Propiedad de activo

Las propiedades de los activos son las estructuras dentro de cada activo que contienen datos industriales. Cada propiedad tiene un tipo de datos y también puede tener una unidad. Una propiedad puede ser un atributo, una medida, una transformación o una métrica. Para obtener más información, consulte Definición de las propiedades de datos.

Configure las propiedades de los activos para que se procesen en la periferia. Para obtener más información sobre el procesamiento de datos en la periferia, consulte the section called “Habilitación del procesamiento de datos de la periferia”.

Atributo

Los atributos son propiedades de un activo que normalmente permanecen constantes, como el fabricante del dispositivo o la ubicación del dispositivo. Los atributos pueden tener valores preestablecidos. Cada activo creado a partir de un modelo de activo incluye los valores por defecto de los atributos definidos en ese modelo. Para obtener más información, consulte Definición de datos estáticos (atributos).

Panel de control

Cada proyecto contiene un conjunto de paneles. Los paneles proporcionan un conjunto de visualizaciones para los valores de un conjunto de activos. Los propietarios de proyectos crean los paneles y las visualizaciones que contiene. Cuando un propietario de proyecto está listo para compartir el conjunto de paneles, el propietario puede invitar a observadores al proyecto, lo que les da acceso a todos los paneles del mismo. Si desea un conjunto distinto de observadores para distintos paneles, debe dividir los paneles entre proyectos. Cuando los espectadores miran los paneles, pueden personalizar el intervalo de tiempo para ver datos específicos.

Flujo de datos

Introduce o ingiere datos industriales AWS IoT SiteWise incluso antes de crear modelos y activos. AWS IoT SiteWise genera automáticamente flujos de datos para recopilar flujos de datos sin procesar de su equipo.

Alias de flujo de datos

Los alias de flujo de datos le ayudan a identificar fácilmente un flujo de datos. Por ejemplo, el alias `server1-windfarm/3/turbine/7/temperature` indica los valores de temperatura procedentes de la turbina #7 del parque eólico #3. El término `server1` es el nombre de la fuente de datos que ayuda a identificar el servidor OPC-UA y `server1-` es un prefijo adjunto a todos los flujos de datos notificados desde este servidor OPC-UA.

Asociación de flujos de datos

Después de crear los modelos de activos y los activos, asocie los flujos de datos con las propiedades de los activos definidas en los activos para estructurar los datos. AWS IoT SiteWise a continuación, puede utilizar modelos de activos y activos para gestionar los datos entrantes de sus flujos de datos. También puede disociar los flujos de datos de las propiedades de activo. Para obtener más información, consulte Administración de flujos de datos.

Fórmula

Cada propiedad de transformación y métrica viene con una fórmula que describe cómo la propiedad transforma o agrega los datos. Estas fórmulas incluyen las entradas de propiedades, los operadores y las funciones que ofrece. AWS IoT SiteWise Para obtener más información, consulte Uso de expresiones de fórmula.

Medida

Las mediciones son propiedades de un activo que representan los flujos de datos de series temporales sin procesar del sensor procedentes de un dispositivo o equipo. Para obtener más información, consulte Definición de flujos de datos procedentes del equipo (mediciones).

Métrica

Las métricas son propiedades de un activo que representan datos agregados de series temporales. Cada métrica va acompañada de una expresión matemática (fórmula) que describe cómo agregar puntos de datos y un intervalo de tiempo para calcular esa agregación. Las métricas generan un único punto de datos para cada intervalo de tiempo especificado. Para obtener más información, consulte Agregación de datos de propiedades y otros activos (métricas).

Paquetes

SiteWise Las puertas de enlace perimetrales utilizan paquetes para determinar cómo recopilar, procesar y enrutar los datos. Actualmente, AWS IoT SiteWise es compatible con el paquete de recopilación de datos y el paquete de procesamiento de datos. Para obtener más información

sobre los paquetes disponibles para su puerta de enlace SiteWise Edge, consultethe section called “Uso de los paquetes”.

Paquete de recopilación de datos

Utilice el paquete de recopilación de datos para que su puerta de enlace SiteWise Edge pueda recopilar sus datos industriales y enviarlos al AWS destino que elija. Este paquete se agrega automáticamente a tu puerta de enlace SiteWise Edge y no se puede quitar.

Paquete de procesamiento de datos

Use el paquete de procesamiento de datos para procesar sus datos en la periferia y consérvelos durante 30 días para usarlos en aplicaciones locales.

Portal

Un AWS IoT SiteWise Monitor portal es una aplicación web que puede utilizar para visualizar y compartir sus AWS IoT SiteWise datos. Un portal tiene uno o varios administradores y contiene cero o más proyectos.

Administrador del portal

Cada portal de SiteWise Monitor tiene uno o más administradores de portal. Los administradores del portal utilizan el portal para crear proyectos que contengan recopilaciones de activos y paneles. A continuación, el administrador del portal asigna activos y propietarios a cada proyecto. Al controlar el acceso al proyecto, los administradores del portal especifican los activos que los propietarios y visores de proyectos pueden ver.

Proyecto

Cada portal de SiteWise Monitor contiene un conjunto de proyectos. Cada proyecto tiene un subconjunto de sus activos de AWS IoT SiteWise asociados al mismo. Los propietarios de proyectos crean uno o varios paneles para proporcionar una forma coherente de ver los datos asociados a esos activos. Los propietarios del proyecto pueden invitar a los lectores al proyecto para permitirles ver los activos y paneles del proyecto. El proyecto es la unidad básica para compartir en SiteWise Monitor. Los propietarios del proyecto pueden invitar a los usuarios a los que el AWS administrador les dio acceso al portal. Un usuario debe tener acceso a un portal antes de que un proyecto de ese portal pueda compartirse con ese usuario.

Propietario del proyecto

Cada proyecto de SiteWise Monitor tiene propietarios. Los propietarios de proyectos crean visualizaciones en forma de paneles para representar los datos operativos de manera coherente. Cuando los paneles están listos para compartirse, el propietario del proyecto puede invitar a

lectores al proyecto. Los propietarios de proyectos también pueden asignar otros propietarios al proyecto. Los propietarios del proyecto pueden configurar los umbrales y los ajustes de notificación de las alarmas.

Observador de proyectos

Cada proyecto de SiteWise Monitor tiene visores. Los observadores de proyectos pueden conectarse al portal para ver los paneles creados por los propietarios de proyectos. En cada panel de control, los observadores de proyectos pueden ajustar el intervalo de tiempo para comprender mejor los datos operativos. Los observadores de proyectos solo pueden ver los paneles de los proyectos a los que tienen acceso. Los observadores de proyectos pueden confirmar y posponer alarmas.

Alias de propiedad

Tiene la opción de crear alias en las propiedades de los activos, como la ruta de flujo de datos de un servidor OPC-UA (por ejemplo, /company/windfarm/3/turbine/7/temperature), lo que simplifica la identificación de la propiedad de un activo durante la ingesta o la recuperación de los datos del activo. Cuando utiliza una puerta de enlace SiteWise Edge para ingerir datos de los servidores, los alias de sus propiedades deben coincidir con las rutas de sus flujos de datos sin procesar. Para obtener más información, consulte Asignación de flujos de datos industriales a propiedades de activos.

Notificación de propiedad

Al habilitar las notificaciones de propiedad para una propiedad de un activo, AWS IoT SiteWise publica un mensaje MQTT AWS IoT Core cada vez que esa propiedad recibe un nuevo valor. La carga útil del mensaje incluye detalles sobre la actualización del valor de esa propiedad. Utilice las notificaciones del valor de la propiedad para crear soluciones que conecten sus datos industriales AWS IoT SiteWise con otros AWS servicios. Para obtener más información, consulte Interacción con otros AWS servicios.

SiteWise Puerta de enlace Edge

Una puerta de enlace SiteWise Edge se encuentra en las instalaciones del cliente para recopilar, gestionar y dirigir los datos. Una puerta de enlace SiteWise Edge se conecta a sus fuentes de datos industriales a través del protocolo OPC-UA para recopilar y procesar datos y enviarlos a la AWS nube. SiteWise Las pasarelas perimetrales también se pueden conectar a fuentes de datos asociadas. SiteWise Las pasarelas perimetrales utilizan paquetes para la recopilación de datos, el procesamiento perimetral y mucho más. Para obtener más información sobre los paquetes disponibles, consulte the section called “Uso de los paquetes”.

Tiene la flexibilidad de crear una puerta de enlace SiteWise Edge en cualquier dispositivo o plataforma capaz de funcionar AWS IoT Greengrass. Para obtener más información, consulte Uso de puertas de enlace SiteWise Edge.

Transformación

Las transformaciones son propiedades de un activo que representan datos de series temporales transformadas. Cada transformación va acompañada de una expresión matemática (fórmula) que especifica cómo convertir los puntos de datos de una forma a otra. Los puntos de datos transformados mantienen una one-to-one relación con los puntos de datos de entrada. Para obtener más información, consulte Transformación de datos (transformaciones).

Visualización

En cada panel de control, los propietarios de proyectos deciden cómo mostrar las propiedades y alarmas de los activos asociados al proyecto. La disponibilidad se podría representar como un gráfico de líneas, mientras que otros valores se podrían mostrar como gráficos de barras o indicadores clave de rendimiento (KPI). Las alarmas se visualizan mejor como cuadrículas de estado y líneas temporales de estado. Los propietarios de proyectos personalizan cada visualización para ofrecer la mejor comprensión de los datos de ese activo.

Casos de uso para AWS IoT SiteWise

AWS IoT SiteWise se utiliza en una variedad de industrias para muchas aplicaciones de recopilación y análisis de datos industriales.

Recopile datos de forma coherente de todas sus fuentes para ayudar a resolver los problemas rápidamente. AWS IoT SiteWise ofrece monitoreo remoto para recopilar los datos directamente in situ o recopilarlos de múltiples fuentes en muchas instalaciones. AWS IoT SiteWise proporciona la flexibilidad necesaria para las soluciones de datos de IoT industrial.

Fabricación

AWS IoT SiteWise puede simplificar el proceso de recopilación y utilización de los datos de sus equipos para identificar y minimizar las ineficiencias, lo que mejora las operaciones industriales. AWS IoT SiteWise le ayuda a recopilar datos de las líneas y equipos de fabricación. Con AWS IoT SiteWiseél, puede transferir los datos a la AWS nube y crear métricas de rendimiento para sus equipos y procesos específicos. Puede utilizar las métricas generadas para comprender la eficacia general de sus operaciones e identificar oportunidades de innovación y mejora. También puede ver

su proceso de fabricación e identificar deficiencias en los equipos y procesos, brechas de producción o defectos en los productos.

Alimentos y bebidas

Las instalaciones del sector de alimentos y bebidas manejan una amplia variedad de procesos, que incluyen moler granos para hacer harina, faenar y empacar carne, y preparar, cocinar y congelar alimentos para microondas. Las plantas de procesamiento de alimentos suelen estar ubicadas en varias ubicaciones y los operadores de las plantas y los equipos se encuentran en una ubicación centralizada para monitorear los procesos y los equipos. Por ejemplo, las unidades de refrigeración evalúan la manipulación y la caducidad de los ingredientes. Supervisan la generación de residuos en todas las instalaciones para garantizar la eficiencia operativa. Con ellas AWS IoT SiteWise, puede agrupar los flujos de datos de los sensores procedentes de varios lugares por línea de producción e instalaciones para que sus ingenieros de procesos puedan comprender mejor las instalaciones y realizar mejoras en ellas.

Energía y servicios públicos

Con él AWS IoT SiteWise, puede resolver los problemas de los equipos de forma más fácil y eficiente. Puede supervisar el rendimiento de los activos de forma remota y en tiempo real. Acceda a los datos históricos del equipo desde cualquier lugar para identificar posibles problemas, enviar recursos precisos y prevenir y solucionar problemas con mayor rapidez.

Empezar con AWS IoT SiteWise

Con AWS IoT SiteWiseél, puede recopilar, organizar, analizar y visualizar sus datos.

AWS IoT SiteWise proporciona una demostración que puede utilizar para explorar el servicio sin configurar una fuente de datos real. Para obtener más información, consulte Uso de la AWS IoT SiteWise demostración.

Puede completar los siguientes tutoriales para explorar determinadas funciones de AWS IoT SiteWise:

- Ingerir datos de cosas AWS IoT
- Visualización y uso compartido de datos de parques eólicos en Monitor SiteWise
- Publicar actualizaciones de valor de propiedad en Amazon DynamoDB

Consulte los siguientes temas para obtener más información sobre AWS IoT SiteWise:

- Ingerir datos para AWS IoT SiteWise
- Crear modelos de activos industriales
- Habilitación del procesamiento de datos de la periferia
- Monitorización de datos con AWS IoT SiteWise Monitor
- Consulta datos de AWS IoT SiteWise
- Interacción con otros AWS servicios

Temas

Requisitos

Para empezar, debe Cuenta de AWS tener uno AWS IoT SiteWise. Si no dispone de una, consulte Configuración de una Cuenta de AWS.

Utilice una región donde AWS IoT SiteWise esté disponible. Para obtener más información, consulte Puntos de conexión y cuotas de AWS IoT SiteWise. Puede utilizar el selector de regiones de la AWS Management Console para cambiar a una de estas regiones.

Configuración de una Cuenta de AWS

Temas

- Inscríbase en un Cuenta de AWS
- Cómo crear un usuario administrativo

Inscríbase en un Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirse a una Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en una Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea una. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario administrativo y utilice únicamente el usuario raíz para ejecutar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Cómo crear un usuario administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In .
2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Crear un usuario administrativo

1. Activar IAM Identity Center

   Consulte las instrucciones en Enabling AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .
2. En el Centro de identidades de IAM, conceda acceso administrativo a un usuario administrativo.

   Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Inicio de sesión como usuario administrativo

- Para iniciar sesión con el usuario de IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Uso de la AWS IoT SiteWise demostración

Puede explorarlo fácilmente AWS IoT SiteWise utilizando la AWS IoT SiteWise demostración. AWS IoT SiteWise incluye la demostración en forma de AWS CloudFormation plantilla que puede utilizar

para crear modelos de activos, activos y un portal de SiteWise monitorización, además de generar datos de muestra para un máximo de una semana.

> **Important**
>
> Una vez que cree la demostración, se le empezará a cobrar por los recursos que cree y consuma esta demostración.

Temas

Creando la AWS IoT SiteWise demostración

Puede crear la AWS IoT SiteWise demostración desde la AWS IoT SiteWise consola.

> **Note**
>
> La demostración crea las funciones Lambda, una regla de CloudWatch eventos y las funciones AWS Identity and Access Management (de IAM) necesarias para la demostración. Es posible que vea estos recursos en su. Cuenta de AWS Recomendamos que conserve estos recursos hasta que termine con la demostración. Si elimina los recursos, la demostración podría dejar de funcionar correctamente.

Para crear la demostración en la AWS IoT SiteWise consola

1. Ve a la AWS IoT SiteWise consola y busca la SiteWise demostración en la esquina superior derecha de la página.
2. (Opcional) En la sección de SiteWise demostración, cambia el campo Días para conservar los activos de la demostración para especificar cuántos días se conservará la demostración antes de eliminarla.
3. (Opcional) Para crear un portal de SiteWise monitoreo para monitorear los datos de muestra, haga lo siguiente.

> **Note**
>
> Se le cobrará por los recursos de SiteWise Monitor que cree y consuma esta demostración. Para obtener más información, consulte SiteWise Monitorear en los AWS IoT SiteWise precios.

a. Seleccione Recursos de monitorización.

b. Seleccione Permiso.

c. Elija un rol de IAM existente que conceda a sus usuarios de IAM federados acceso al portal.

> **Important**
>
> Su rol de IAM debe tener los siguientes permisos.

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

Para obtener más información sobre cómo trabajar con SiteWise Monitor, consulte ¿Qué es AWS IoT SiteWise Monitor? en la Guía AWS IoT SiteWise Monitor de aplicación.

4. Seleccione Crear demostración.

   Se tarda unos 3 minutos en crear la demostración. Si no se puede crear la demostración, es posible que su cuenta no tenga permisos suficientes. Cambie a una cuenta que tenga permisos administrativos o use los siguientes pasos para eliminar la demostración e inténtelo de nuevo:

   a. Seleccione Eliminar demostración.

      La demostración tarda unos 15 minutos en borrarse.

   b. Si la demostración no elimina, abre la AWS CloudFormation consola, elige la pila llamada IoT SiteWiseDemoAssets y selecciona Eliminar en la esquina superior derecha.

   c. Si la demostración no se puede eliminar de nuevo, sigue los pasos de la AWS CloudFormation consola para omitir los recursos que no se pudieron eliminar e inténtalo de nuevo.

5. Una vez que la demostración se haya creado correctamente, podrá explorar los activos y datos de la demostración en la consola de AWS IoT SiteWise.

Eliminar la AWS IoT SiteWise demostración

La AWS IoT SiteWise demo se borra automáticamente al cabo de una semana, o el número de días que hayas elegido si creaste la versión de demostración desde la AWS CloudFormation consola. Puede eliminar la demostración si ha terminado de usar los recursos de demostración. También puede eliminar la demostración si no se puede crear. Siga los pasos siguientes para eliminar la demostración manualmente.

Para eliminar la demostración AWS IoT SiteWise

1. Vaya a la consola de AWS CloudFormation.
2. Seleccione IoTSiteWiseDemoAssets de la lista de Stacks (Pilas).
3. Seleccione Eliminar (Delete).

   Al eliminar la pila, se eliminan todos los recursos creados para la demostración.

4. En el cuadro de diálogo de confirmación, elija Delete stack (Eliminar pila).

   La pila tarda unos 15 minutos en borrarse. Si la demostración no se elimina, vuelva a seleccionar Delete (Eliminar) en la esquina superior derecha. Si la demostración no se puede

eliminar de nuevo, siga los pasos de la AWS CloudFormation consola para omitir los recursos que no se pudieron eliminar e inténtelo de nuevo.

AWS IoT SiteWise tutoriales

Bienvenido a la página de AWS IoT SiteWise tutoriales. Esta creciente colección de tutoriales le brinda los conocimientos y las habilidades necesarios para navegar por las complejidades de. AWS IoT SiteWise Estos tutoriales ofrecen una amplia gama de temas básicos para satisfacer sus necesidades. A medida que profundice en los tutoriales, descubra información inestimable sobre varios aspectos de. AWS IoT SiteWise

Cada tutorial utiliza un ejemplo de equipo específico. Estos tutoriales están pensados para entornos de prueba y utilizan nombres de empresas, modelos, activos, propiedades, etc. ficticios. Su finalidad es proporcionar orientación general. Los tutoriales no están diseñados para su uso directo en un entorno de producción sin una revisión y adaptación cuidadosas para satisfacer las necesidades únicas de su organización.

Temas

- Calcular el OEE en AWS IoT SiteWise
- Ingerir datos de cosas AWS IoT
- Visualización y uso compartido de datos de parques eólicos en Monitor SiteWise
- Publicar actualizaciones de valor de propiedad en Amazon DynamoDB

Calcular el OEE en AWS IoT SiteWise

En este tutorial se proporciona un ejemplo de cómo calcular la eficacia general de los equipos (OEE) de un proceso de producción. Como resultado, los cálculos o fórmulas de su OEE podrían diferir de los que se muestran aquí. En general, OEE se define como `Availability * Quality * Performance`. Para obtener más información sobre el cálculo de la OEE, consulte Eficacia general de los equipos en Wikipedia.

Requisitos previos

Para completar este tutorial, debe configurar la ingesta de datos para un dispositivo que tenga los tres flujos de datos siguientes:

- `Equipment_State`: un código numérico que representa el estado de la máquina como inactiva, averiada, parada planificada o funcionamiento normal.

- `Good_Count`: un flujo de datos donde cada punto de datos contiene el número de operaciones exitosas desde el último punto de datos.
- `Bad_Count`: un flujo de datos donde cada punto de datos contiene el número de operaciones fallidas desde el último punto de datos.

Para configurar la ingesta de datos, consulte Ingerir datos para AWS IoT SiteWise. Si no tiene una operación industrial disponible, puede escribir un script que genere y cargue datos de muestra a través de la API de AWS IoT SiteWise .

Cómo calcular la OEE

En este aprendizaje, creará un modelo de activos que calcula la OEE a partir de tres flujos de entrada de datos: `Equipment_State`, `Good_Count` y `Bad_Count`. En este ejemplo, considere una máquina de envasado genérica, como una que se utiliza para empaquetar azúcar, patatas fritas o pintura. En la AWS IoT SiteWise consola, cree un modelo de AWS IoT SiteWise activos con las siguientes medidas, transformaciones y métricas. A continuación, puede crear un activo para representar la máquina de embalaje y observar cómo AWS IoT SiteWise calcula la OEE.

Defina las siguientes mediciones para representar los flujos de datos sin formato de la máquina de envasado.

Mediciones

- `Equipment_State`: un flujo de datos (o medición) que proporciona el estado actual de la máquina de envasado en códigos numéricos:
  - `1024`: la máquina está inactiva.
  - `1020`: un fallo, como un error o un retraso.
  - `1000`: una parada planificada.
  - `1111`: funcionamiento normal.
- `Good_Count`: un flujo de datos donde cada punto de datos contiene el número de operaciones exitosas desde el último punto de datos.
- `Bad_Count`: un flujo de datos donde cada punto de datos contiene el número de operaciones fallidas desde el último punto de datos.

Con el flujo de datos de medida `Equipment_State` y los códigos que contiene, defina las siguientes transformaciones (o medidas derivadas). Las transformaciones tienen una one-to-one relación con las medidas sin procesar.

Transformaciones

- `Idle = eq(Equipment_State, 1024)`: un flujo de datos transformado que contiene el estado de inactividad de la máquina.
- `Fault = eq(Equipment_State, 1020)`: un flujo de datos transformado que contiene el estado de fallo de la máquina.
- `Stop = eq(Equipment_State, 1000)`: un flujo de datos transformado que contiene el estado de parada planificada de la máquina.
- `Running = eq(Equipment_State, 1111)`: un flujo de datos transformado que contiene el estado de funcionamiento normal de la máquina.

Utilizando las medidas sin formato y las medidas transformadas, defina las siguientes métricas que agreguen los datos de la máquina a lo largo de los intervalos de tiempo especificados. Seleccione el mismo intervalo de tiempo para cada métrica cuando defina las métricas en esta sección.

Métricas

- `Successes = sum(Good_Count)`: el número de envases llenados con éxito durante el intervalo de tiempo especificado.
- `Failures = sum(Bad_Count)`: el número de envases llenados sin éxito durante el intervalo de tiempo especificado.
- `Idle_Time = statetime(Idle)`: el tiempo total de inactividad de la máquina (en segundos) por intervalo de tiempo especificado.
- `Fault_Time = statetime(Fault)`: el tiempo total de fallo de la máquina (en segundos) por intervalo de tiempo especificado.
- `Stop_Time = statetime(Stop)`: el tiempo total de parada planificada de la máquina (en segundos) por intervalo de tiempo especificado.
- `Run_Time = statetime(Running)`: el tiempo total de la máquina (en segundos) funcionando sin problemas por intervalo de tiempo especificado.
- `Down_Time = Idle_Time + Fault_Time + Stop_Time`: el tiempo total de inactividad de la máquina (en segundos) durante el intervalo de tiempo especificado, calculado como la suma de los estados de la máquina distintos de `Run_Time`.

- `Availability = Run_Time / (Run_Time + Down_Time)`: el tiempo de actividad de la máquina o el porcentaje de tiempo programado que la máquina está disponible para funcionar durante el intervalo de tiempo especificado.
- `Quality = Successes / (Successes + Failures)`: el porcentaje de envases llenados con éxito de la máquina durante los intervalos de tiempo especificados.
- `Performance = ((Successes + Failures) / Run_Time) / Ideal_Run_Rate`: el rendimiento de la máquina a lo largo del intervalo de tiempo especificado como porcentaje de la tasa de ejecución ideal (en segundos) de su proceso.

  Por ejemplo, su `Ideal_Run_Rate` podría ser de 60 envases por minuto (1 envase por segundo). Si su `Ideal_Run_Rate` es por minuto o por hora, deberá dividirlo por el factor de conversión de unidades apropiado porque `Run_Time` es en segundos.
- `OEE = Availability * Quality * Performance`: la eficacia general de los equipos de la máquina a lo largo del intervalo de tiempo especificado. Esta fórmula calcula la OEE como fracción de 1.

Ingerir datos de cosas AWS IoT

En este tutorial, aprenda a ingerir datos AWS IoT SiteWise de una flota de AWS IoT cosas mediante el uso de sombras de dispositivos. Las sombras de los dispositivos son objetos JSON que almacenan información sobre el estado actual de un AWS IoT dispositivo. Para obtener más información, consulte Servicio sombra de dispositivo en la Guía para desarrolladores de AWS IoT .

Después de completar este tutorial, puede configurar una operación en AWS IoT SiteWise función de los AWS IoT elementos. Al usar AWS IoT cosas, puede integrar su operación con otras funciones útiles de AWS IoT. Por ejemplo, puede configurar AWS IoT funciones para realizar las siguientes tareas:

- Configure reglas adicionales para transmitir datos a AWS IoT EventsAmazon DynamoDB y otros. Servicios de AWS Para obtener más información, consulte Reglas en la Guía para desarrolladores de AWS IoT .
- Indexe, busque y agregue los datos de sus dispositivos con el servicio de indexación de AWS IoT flotas. Para obtener más información, consulte Servicio de indexación de flotas en la Guía para desarrolladores de AWS IoT .
- Audite y proteja sus dispositivos con AWS IoT Device Defender. Para obtener más información, consulte AWS IoT Device Defender en la Guía para desarrolladores de AWS IoT .

En este tutorial, aprenderás a transferir datos desde dispositivos AWS IoT ocultos hasta activos internos. AWS IoT SiteWise Para ello, debe crear una o más AWS IoT cosas y ejecutar un script que actualice la sombra del dispositivo de cada una de ellas con los datos de uso de la CPU y la memoria. Utilice los datos de uso de CPU y memoria en este tutorial para imitar datos realistas del sensor. A continuación, se crea una regla con una AWS IoT SiteWise acción que envía estos datos a un activo AWS IoT SiteWise cada vez que se actualiza la sombra del dispositivo de una cosa. Para obtener más información, consulte Ingerir datos mediante reglas AWS IoT Core.

Temas

Requisitos previos

Necesitará lo siguiente para completar este tutorial:

- Y Cuenta de AWS. Si no dispone de una, consulte Configuración de una Cuenta de AWS.
- Un ordenador de desarrollo en ejecución WindowsmacOS,Linux, o Unix para acceder al AWS Management Console. Para obtener más información, consulte Introducción a AWS Management Console.
- Un usuario AWS Identity and Access Management (IAM) con permisos de administrador.
- Python3 instalado en tu ordenador de desarrollo o instalado en el dispositivo que quieres registrar como AWS IoT cosa.

Paso 1: Crear una AWS IoT política

En este procedimiento, cree una AWS IoT política que permita que sus AWS IoT cosas accedan a los recursos utilizados en este tutorial.

Para crear una AWS IoT política

1. Inicie sesión en la AWS Management Console.
2. Revise las AWS regiones en las que AWS IoT SiteWise está disponible. Cambie a una de estas regiones compatibles, si es necesario.
3. Vaya a la consola de AWS IoT. Si aparece el botón Conectar dispositivo, elíjalo.
4. En el panel de navegación de la izquierda, elija Seguridad y, a continuación, elija Políticas.
5. Seleccione Crear.
6. Introduzca un nombre para la AWS IoT política (por ejemplo,**`SiteWiseTutorialDevicePolicy`**).
7. En Documento de política, elija JSON para introducir la siguiente política en formato JSON. Reemplace *`region`* y *`account-id`* por su región e ID de cuenta, como **`us-east-1`** y **`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*"
    }
  ]
}
```

Esta política permite a sus AWS IoT dispositivos establecer conexiones y comunicarse con dispositivos ocultos mediante mensajes MQTT. Para obtener más información sobre los mensajes MQTT, consulte ¿Qué es MQTT? . Para interactuar con las sombras de los dispositivos, tus AWS IoT cosas publican y reciben mensajes MQTT sobre temas que comienzan con`$aws/things/thing-name/shadow/`. Esta política incorpora una variable de política denominada`${iot:Connection.Thing.ThingName}`. Esta variable sustituye el nombre de la cosa conectada en cada tema. La `iot:Connect` declaración establece limitaciones sobre los dispositivos que pueden establecer conexiones, lo que garantiza que la variable de política del objeto solo pueda sustituir los nombres que comiencen por. `SiteWiseTutorialDevice`

Para obtener más información, consulte Variables de objetos de políticas en la Guía para desarrolladores de AWS IoT .

> **Note**
>
> Esta política se aplica a objetos cuyos nombres comienzan por `SiteWiseTutorialDevice`. Para usar un nombre diferente para sus objetos, debe actualizar la política según corresponda.

8. Seleccione Crear.

Paso 2: Creación y configuración de un objeto de AWS IoT

En este procedimiento, se crea y configura cualquier AWS IoT cosa. Puede designar su ordenador de desarrollo como cualquier AWS IoT cosa. A medida que avances, recuerda que los principios que estás aprendiendo aquí se pueden aplicar a proyectos reales. Tiene la flexibilidad de crear y configurar AWS IoT cosas en cualquier dispositivo capaz de ejecutar un AWS IoT SDK, incluido AWS IoT Greengrass FreeRTOS. Para obtener más información, consulte SDK de AWS IoT en la Guía para desarrolladores de AWS IoT .

Para crear y configurar cualquier cosa AWS IoT

1. Abra una línea de comandos y ejecute el siguiente comando para crear un directorio para este tutorial.

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

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

2. Ejecute el siguiente comando para crear un directorio para los certificados de su objeto.

```
mkdir device1
```

Si está creando objetos adicionales, incremente el número en el nombre del directorio según corresponda para realizar un seguimiento de cuáles son los certificados que pertenecen a cada objeto.

3. Vaya a la consola de AWS IoT.
4. En el panel de navegación izquierdo, selecciona Todos los dispositivos en la sección Administrar. A continuación, elija Objetos.
5. Si aparece un cuadro de diálogo You don't have any things yet (Aún no tiene ningún objeto), elija Create a thing (Crear un objeto). De lo contrario, seleccione Crear objetos.
6. En la página Creación de objetos, elija Crear un solo objeto y luego elija Siguiente.
7. En la página Especificar propiedades de objeto, introduzca un nombre para el objeto AWS IoT (por ejemplo, **`SiteWiseTutorialDevice1`**) y, a continuación, seleccione Siguiente. Si está creando objetos adicionales, incremente el número en el nombre del objeto según corresponda.

> **Important**
>
> El nombre del elemento debe coincidir con el nombre utilizado en la política que creó en el paso 1: Creación de una AWS IoT política. De lo contrario, el dispositivo no podrá conectarse a AWS IoT.

8. En la página Configurar el certificado del dispositivo: opcional, seleccione Generar automáticamente un nuevo certificado (opción recomendada) y, a continuación, seleccione Siguiente. Los certificados permiten AWS IoT identificar tus dispositivos de forma segura.
9. En la página Adjuntar políticas al certificado (opcional), seleccione la política que creó en el paso 1: Crear una AWS IoT política y elija Crear cosa.
10. En el cuadro de diálogo Descargar certificados y claves, haga lo siguiente:

    a. Elija los enlaces de Download (Descarga) para descargar el certificado, la clave pública y la clave privada de su objeto. Guarde los tres archivos en el directorio que creó para los certificados de su objeto (por ejemplo, `iot-sitewise-rule-tutorial/device1`).

> **Important**
>
> Esta es la única vez que puede descargar el certificado y las claves de su certificado, que necesita para que su dispositivo se conecte correctamente a AWS IoT.

b. Seleccione el enlace Descargar para descargar un certificado de CA raíz. Guarde el certificado de entidad de certificación raíz en `iot-sitewise-rule-tutorial`. Recomendamos descargar Amazon Root CA 1.

11. Seleccione Listo.

Ya ha registrado AWS IoT algo en su ordenador. Realice uno de los siguientes pasos:

- Continúe con el paso 3: Crear un modelo de activos de dispositivo sin crear AWS IoT elementos adicionales. Puede completar este tutorial con un solo objeto.
- Repita los pasos de esta sección en otro equipo o dispositivo para crear más objetos de AWS IoT . Para este tutorial, le recomendamos que siga esta opción para que pueda ingerir datos únicos de uso de memoria y CPU desde varios dispositivos.
- Repita los pasos de esta sección en el mismo dispositivo (su equipo) para crear más objetos de AWS IoT . Cada AWS IoT dispositivo recibe datos de uso de CPU y memoria similares de su ordenador, así que utilice este enfoque para demostrar la ingesta de datos no exclusivos de varios dispositivos.

Paso 3: Creación de un modelo de activos de dispositivo

En este procedimiento, se crea un modelo de activos AWS IoT SiteWise para representar los dispositivos que transmiten datos de uso de la CPU y la memoria. Para procesar los datos de los activos que representan grupos de dispositivos, los modelos de activos exigen información coherente en varios activos del mismo tipo. Para obtener más información, consulte Crear modelos de activos industriales.

Para crear un modelo de activos que represente un dispositivo

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación izquierdo, elija Models (Modelos).

3. Seleccione Crear modelo.
4. En Detalles del modelo, escriba un nombre para el modelo. Por ejemplo, **`SiteWise Tutorial Device Model`**.
5. En Measurement definitions (Definiciones de medida), haga lo siguiente:

   a. En Name (Nombre), escriba **`CPU Usage`**.

   b. En Unit (Unidad), escriba **`%`**.

   c. Deje Data type (Tipo de datos) como Double (Doble).

   Las propiedades de medición representan los flujos de datos sin procesar de un dispositivo. Para obtener más información, consulte Definición de flujos de datos procedentes del equipo (mediciones).
6. Elija Agregar nueva medida para agregar una segunda propiedad de medida.
7. En la segunda fila, en Measurement definitions (Definiciones de medida), haga lo siguiente:

   a. En Name (Nombre), escriba **`Memory Usage`**.

   b. En Unit (Unidad), escriba **`%`**.

   c. Deje Data type (Tipo de datos) como Double (Doble).
8. En Metric definitions (Definiciones de métricas), haga lo siguiente:

   a. En Name (Nombre), escriba **`Average CPU Usage`**.

   b. En Formula (Fórmula), escriba **`avg(CPU Usage)`**. Elija CPU Usage en la lista de autocompletar cuando aparezca.

   c. En Time interval (Intervalo de tiempo), escriba **`5 minutes`**.

   Las propiedades de métrica definen cálculos de agregación que procesan todos los puntos de datos de entrada a lo largo de un intervalo y generan un único punto de datos por intervalo. Esta propiedad de métrica calcula el uso promedio de CPU de cada dispositivo cada 5 minutos. Para obtener más información, consulte Agregación de datos de propiedades y otros activos (métricas).
9. Elija Agregar nueva métrica para agregar una segunda propiedad de métrica.
10. En la segunda fila en Metric definitions (Definiciones de métricas), haga lo siguiente:

    a. En Name (Nombre), escriba **`Average Memory Usage`**.

b. En Formula (Fórmula), escriba **`avg(Memory Usage)`**. Elija Memory Usage en la lista de autocompletar cuando aparezca.

c. En Time interval (Intervalo de tiempo), escriba **`5 minutes`**.

Esta propiedad de métrica calcula el uso medio de memoria de cada dispositivo cada 5 minutos.

11. (Opcional) Agregue otras métricas adicionales que le interese calcular por dispositivo. Algunas funciones interesantes incluyen `min` y `max`. Para obtener más información, consulte Uso de expresiones de fórmula. En el paso 4: crear un modelo de activos de flota de dispositivos, usted crea un activo principal que pueda calcular métricas utilizando datos de toda la flota de dispositivos.
12. Seleccione Crear modelo.

Paso 4: Creación de un modelo de activos de flota de dispositivos

En este procedimiento, se crea un modelo de activos AWS IoT SiteWise para simbolizar el conjunto de dispositivos. En este modelo de activos, se establece una estructura que permite vincular varios activos de dispositivos a un activo general de la flota. A continuación, describe las métricas del modelo de activos de la flota para consolidar los datos de todos los activos de dispositivos conectados. Este enfoque le proporciona información exhaustiva sobre el rendimiento colectivo de toda su flota.

Para crear un modelo de activos que represente una flota de dispositivos

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación izquierdo, elija Models (Modelos).
3. Seleccione Crear modelo.
4. En Detalles del modelo, escriba un nombre para el modelo. Por ejemplo, **`SiteWise Tutorial Device Fleet Model`**.
5. En Hierarchy definitions (Definiciones de jerarquía), haga lo siguiente:

   a. En Hierarchy name (Nombre de jerarquía), escriba **`Device`**.

   b. En Hierarchy model (Modelo de jerarquía), elija su modelo de activos de dispositivo (**`SiteWise Tutorial Device Model`**).

Una jerarquía define una relación entre un modelo de activo principal (flota) y un modelo de activo secundario (dispositivo). Los activos principales pueden acceder a los datos de propiedades de los activos secundarios. Cuando cree activos más adelante, tiene que asociar los activos secundarios a activos principales según una definición de jerarquía en el modelo de activos principales. Para obtener más información, consulte Definición de jerarquías de modelos de activos.

6. En Metric definitions (Definiciones de métricas), haga lo siguiente:

   a. En Name (Nombre), escriba **`Average CPU Usage`**.

   b. En Formula (Fórmula), escriba **`avg(Device | Average CPU Usage)`**. Cuando aparezca la lista de autocompletar, elija Device para elegir una jerarquía y, a continuación, elija Average CPU Usage para elegir la métrica del activo de dispositivo que creó anteriormente.

   c. En Time interval (Intervalo de tiempo), escriba **`5 minutes`**.

   Esta propiedad de métrica calcula el uso medio de CPU de todos los activos de dispositivo asociados a un activo de flota a través de la jerarquía de **`Device`**.

7. Elija Agregar nueva métrica para agregar una segunda propiedad de métrica.

8. En la segunda fila en Metric definitions (Definiciones de métricas), haga lo siguiente:

   a. En Name (Nombre), escriba **`Average Memory Usage`**.

   b. En Formula (Fórmula), escriba **`avg(Device | Average Memory Usage)`**. Cuando aparezca la lista de autocompletar, elija Device para elegir una jerarquía y, a continuación, elija Average Memory Usage para elegir la métrica del activo de dispositivo que creó anteriormente.

   c. En Time interval (Intervalo de tiempo), escriba **`5 minutes`**.

   Esta propiedad de métrica calcula el uso medio de memoria de todos los activos de dispositivo asociados a un activo de flota a través de la jerarquía de **`Device`**.

9. (Opcional) Agregue otras métricas adicionales que le interese calcular en su flota de dispositivos.

10. Seleccione Crear modelo.

Paso 5: Creación y configuración de un activo de dispositivo

En este procedimiento, generas un activo de dispositivo que se basa en el modelo de activos de tu dispositivo. A continuación, se definen los alias de propiedad para cada propiedad de medida. El alias de una propiedad es una cadena única que identifica la propiedad de un activo. Más adelante, podrá identificar una propiedad para la carga de datos utilizando los alias en lugar del identificador del activo y el identificador de la propiedad. Para obtener más información, consulte Asignación de flujos de datos industriales a propiedades de activos.

Para crear un activo de dispositivo y definir alias de propiedad

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación izquierdo, elija Assets (activos).
3. Elija Create asset (Crear activo).
4. En Información del modelo, seleccione el modelo de activo de su dispositivo, **`SiteWise Tutorial Device Model`**.
5. En Información del activo, introduzca un nombre para su activo. Por ejemplo, **`SiteWise Tutorial Device 1`**.
6. Elija Create asset (Crear activo).
7. Para el nuevo activo de dispositivo, elija Edit (Editar).
8. En CPU Usage, escriba **`/tutorial/device/SiteWiseTutorialDevice1/cpu`** como alias de propiedad. El nombre de la AWS IoT cosa se incluye en el alias de la propiedad para poder ingerir datos de todos los dispositivos con una sola AWS IoT regla.
9. En Memory Usage, escriba **`/tutorial/device/SiteWiseTutorialDevice1/memory`** como alias de propiedad.
10. Seleccione Guardar.

Si has creado varios AWS IoT elementos anteriormente, repite los pasos 3 a 10 para cada dispositivo e incrementa el número en el nombre del activo y en los alias de propiedad según corresponda. Por ejemplo, el nombre del segundo activo del dispositivo debe ser **`SiteWise Tutorial Device 2`** y sus alias de propiedad deben ser **`/tutorial/device/SiteWiseTutorialDevice2/cpu`** y **`/tutorial/device/SiteWiseTutorialDevice2/memory`**.

Paso 6: Creación y configuración de un activo de flota de dispositivos

En este procedimiento, se forma un activo de flota de dispositivos derivado del modelo de activos de su flota de dispositivos. A continuación, vincula los activos de sus dispositivos individuales al activo de la flota. Esta asociación permite que las propiedades métricas del activo de la flota recopilen y analicen datos de varios dispositivos. Estos datos le proporcionan una visión consolidada del rendimiento colectivo de toda la flota.

Para crear un activo de flota de dispositivos y asociar activos de dispositivo

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación izquierdo, elija Assets (activos).
3. Elija Create asset (Crear activo).
4. En Información de modelo, elija su modelo de activos de flota de dispositivos, **`SiteWise Tutorial Device Fleet Model`**.
5. En Información del activo, introduzca un nombre para su activo. Por ejemplo, **`SiteWise Tutorial Device Fleet 1`**.
6. Elija Create asset (Crear activo).
7. Para el nuevo activo de flota de dispositivos, elija Edit (Editar).
8. En Activos asociados a este activo, elija Añadir activo asociado y haga lo siguiente:
   a. En Hierarchy (Jerarquía), elija Device. Esta jerarquía identifica la relación jerárquica entre el dispositivo y los activos de la flota de dispositivos. Ha definido esta jerarquía en el modelo de activos de flota de dispositivos anteriormente en este tutorial.
   b. En Asset (activo), elija el activo del dispositivo, SiteWise Tutorial Device 1.
9. (Opcional) Si ha creado varios activos de dispositivo anteriormente, repita los pasos 8 a 10 para cada activo de dispositivo que haya creado.
10. Seleccione Guardar.

    Ahora debería ver los activos de su dispositivo organizados como una jerarquía.

Paso 7: Crear una regla en AWS IoT Core para enviar datos a los activos del dispositivo

En este procedimiento, se establece una regla en AWS IoT Core. La regla está diseñada para interpretar los mensajes de notificación de los dispositivos ocultos y transmitir los datos a los activos del dispositivo AWS IoT SiteWise. Cada vez que la pantalla oculta del dispositivo se actualice, AWS IoT envía un mensaje MQTT. Puede crear una regla que actúe cuando cambien las sombras del dispositivo según el mensaje MQTT. En este caso, el objetivo es gestionar el mensaje de actualización, extraer los valores de las propiedades y transmitirlos a los activos del dispositivo. AWS IoT SiteWise

Para crear una regla con una AWS IoT SiteWise acción

1. Vaya a la consola de AWS IoT.
2. En el panel de navegación de la izquierda, elija Redirección de mensajes y, a continuación, seleccione Reglas.
3. Seleccione Crear regla.
4. Ingrese un nombre y una descripción para su regla y, a continuación, elija Siguiente.
5. Introduzca la siguiente instrucción SQL y, a continuación, seleccione Siguiente.

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

   Esta instrucción de consulta de regla funciona porque el servicio de sombras de dispositivo publica actualizaciones de sombras en `$aws/things/thingName/shadow/update/accepted`. Para obtener más información acerca de las sombras de dispositivos, consulte Servicio de sombras de dispositivos en la Guía de desarrolladores de AWS IoT .

   En la cláusula `WHERE`, esta declaración de consulta de regla utiliza la función `topic(3)` para obtener el nombre de objeto del tercer segmento del tema. A continuación, la instrucción filtra los dispositivos que tienen nombres que no coinciden con los de los dispositivos del tutorial. Para obtener más información sobre AWS IoT SQL, consulte la referencia de AWS IoT SQL en la Guía para AWS IoT desarrolladores.

6. En Acciones de la regla, seleccione Enviar los datos del mensaje a las propiedades de activos en AWS IoT SiteWise y haga lo siguiente:

   a. Elija By property alias (Por alias de propiedad).

   b. En Property alias (Alias de propiedad), escriba **`/tutorial/device/${topic(3)}/cpu`**.

      La `${...}` sintaxis es una plantilla de sustitución. AWS IoT evalúa el contenido de las llaves. Esta plantilla de sustitución extrae el nombre del objeto del tema para crear un alias único para cada objeto. Para obtener más información, consulte Plantillas de sustitución en la Guía para desarrolladores de AWS IoT .

      > **Note**
      >
      > Dado que una expresión de una plantilla de sustitución se evalúa por separado de la instrucción `SELECT`, no se puede utilizar una plantilla de sustitución para hacer referencia a un alias creado mediante una cláusula `AS`. Solo puede hacer referencia a la información presente en la carga original, además de a las funciones y operadores compatibles.

   c. En ID de entrada: opcional, introduzca **`${concat(topic(3), "-cpu-", floor(state.reported.timestamp))}`**.

      Los ID de entrada identifican de forma única cada intento de entrada de valor. Si una entrada devuelve un error, puede encontrar el ID de entrada en la salida de error para solucionar el problema. La plantilla de sustitución en este ID de entrada combina el nombre del objeto y la marca temporal notificada por el dispositivo. Por ejemplo, el ID de entrada resultante podría tener un aspecto similar a `SiteWiseTutorialDevice1-cpu-1579808494`.

   d. En Time in seconds (Tiempo en segundos), escriba **`${floor(state.reported.timestamp)}`**.

      Esta plantilla de sustitución calcula el tiempo en segundos a partir de la marca temporal notificada por el dispositivo. En este tutorial, los dispositivos notifican la marca temporal en segundos en formato de tiempo Unix como un número de punto flotante.

   e. En Desfase en nanosegundos opcional, escriba **`${floor((state.reported.timestamp % 1) * 1E9)}`**.

Esta plantilla de sustitución calcula el desfase en nanosegundos a partir de la hora en segundos convirtiendo la parte decimal de la marca temporal notificada por el dispositivo.

> **Note**
>
> AWS IoT SiteWise requiere que sus datos tengan una marca de tiempo actual en Unix. Si los dispositivos no notifican la hora con precisión, puede obtener la hora actual del motor de reglas de AWS IoT con timestamp(). Esta función notifica el tiempo en milisegundos, por lo que debe actualizar los parámetros de tiempo de la acción de regla a los siguientes valores:
>
> - En Time in seconds (Tiempo en segundos), escriba **`${floor(timestamp() / 1E3)}`**.
> - En Offset in nanos (Desfase en nanosegundos), escriba **`${(timestamp() % 1E3) * 1E6}`**.

f. En Data type (Tipo de datos), elija Double (Doble).

   Este tipo de datos debe coincidir con el tipo de datos de la propiedad de activo definida en el modelo de activos.

g. En Valor, escriba **`${state.reported.cpu}`**. En las plantillas de sustitución, se utiliza el operador **`.`** para recuperar un valor desde una estructura JSON.

h. Elija Add entry (Agregar entrada) para agregar una nueva entrada para la propiedad de uso de memoria y lleve a cabo los pasos siguientes para esa propiedad:

   i. Elija By property alias (Por alias de propiedad).

   ii. En Property alias (Alias de propiedad), escriba **`/tutorial/device/${topic(3)}/memory`**.

   iii. En ID de entrada: opcional, introduzca **`${concat(topic(3), "-memory-", floor(state.reported.timestamp))}`**.

   iv. En Time in seconds (Tiempo en segundos), escriba **`${floor(state.reported.timestamp)}`**.

   v. En Desfase en nanosegundos opcional, escriba **`${floor((state.reported.timestamp % 1) * 1E9)}`**.

   vi. En Data type (Tipo de datos), elija Double (Doble).

vii. En Valor, escriba **`${state.reported.memory}`**.

i. En Rol de IAM, elija Crear rol para crear un rol de IAM para esta acción de regla. Esta función le permite enviar datos AWS IoT a las propiedades del activo de su flota de dispositivos y a su jerarquía de activos.

j. Introduzca un nombre de rol y elija Crear.

7. (Opcional) Configure una acción de error que pueda utilizar para solucionar problemas de la regla. Para obtener más información, consulte Solución de problemas de las reglas.
8. Seleccione Siguiente.
9. Revise la configuración y seleccione Crear.

Paso 8: Ejecución del script del cliente de dispositivo

En este tutorial, no vas a utilizar un dispositivo real para generar informes de datos. En su lugar, ejecutas un script para actualizar la sombra AWS IoT del dispositivo con el uso de la CPU y la memoria para imitar los datos reales de los sensores. Para ejecutar el script, primero debes instalar Python los paquetes necesarios. En este procedimiento, instale los Python paquetes necesarios y, a continuación, ejecute el script del cliente del dispositivo.

Para configurar y ejecutar el script del cliente del dispositivo

1. Vaya a la consola de AWS IoT.
2. En la parte inferior del panel de navegación izquierdo, elija Settings (Configuración).
3. Guarde el punto de enlace personalizado para usarlo con el script del cliente del dispositivo. Utiliza este punto de enlace para interactuar con las sombras de su objeto. Este punto de enlace es exclusivo de su cuenta en la región actual.

   El punto de enlace personalizado debe ser similar al siguiente ejemplo.

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

4. Abra una línea de comandos y ejecute el siguiente comando para acceder al directorio del tutorial que creó anteriormente.

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

5. Ejecute el siguiente comando para instalar AWS IoT Device SDK para Python.

```
pip3 install AWSIoTPythonSDK
```

Para obtener más información, consulte AWS IoT Device SDK para Python en la Guía para desarrolladores de AWS IoT

6. Ejecute el siguiente comando para instalar psutil, un proceso multiplataforma y una biblioteca de utilidades del sistema.

```
pip3 install psutil
```

Para obtener más información, consulte psutil en el Python Package Index.

7. Cree un archivo denominado `thing_performance.py` en el directorio `iot-sitewise-rule-tutorial` y, a continuación, copie el siguiente código Python en el archivo.

```
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. Ejecute `thing_performance.py` desde la línea de comandos con los siguientes parámetros:

   - `-n`, `--thingName`: su nombre del objeto, como **`SiteWiseTutorialDevice1`**.
   - `-e`, `--endpoint` — El AWS IoT punto final personalizado que guardó anteriormente en este procedimiento.
   - `-r`, `--rootCA` — La ruta a su certificado de CA AWS IoT raíz.
   - `-c`, `--cert` — La ruta a su certificado de AWS IoT cosas.
   - `-k`, `--key` — La ruta a la clave privada de su certificado de AWS IoT cosas.
   - `-d`, `--requestDelay`: (opcional) el tiempo de espera en segundos entre cada actualización de la sombra de dispositivo. El valor predeterminado es 1 segundo.
   - `-v`, `--enableLogging`: (opcional) si este parámetro está presente, el script imprime los mensajes de depuración desde el AWS IoT Device SDK para Python.

   El comando debería ser similar al siguiente ejemplo.

```
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
```

Si está ejecutando el script para otras AWS IoT cosas, actualice el nombre de la cosa y el directorio del certificado en consecuencia.

9. Intente abrir y cerrar programas en su dispositivo para ver cómo cambian los usos de la CPU y la memoria. El script imprime cada lectura de uso de CPU y memoria. Si el script carga datos en el servicio de sombra del dispositivo correctamente, el resultado del script debe ser similar al siguiente ejemplo.

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

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

10. Siga estos pasos para comprobar que el script está actualizando la sombra del dispositivo:

    a. Vaya a la consola de AWS IoT.

    b. En el panel de navegación de la izquierda, elija Todos los dispositivos y, a continuación, Objetos.

    c. Elige lo tuyo, SiteWiseTutorialDevice.

    d. Seleccione la pestaña Sombras de dispositivo, seleccione Sombra clásica y compruebe que el Estado de la sombra es similar al del siguiente ejemplo.

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

    Si el estado de sombra de tu objeto está vacío o no tiene el mismo aspecto que en el ejemplo anterior, comprueba que el script se esté ejecutando y se haya conectado correctamente AWS IoT. Si el script sigue agotándose al conectarse AWS IoT, compruebe que su política de cosas esté configurada de acuerdo con este tutorial.

11. Siga estos pasos para comprobar que la acción de regla está enviando datos a AWS IoT SiteWise:

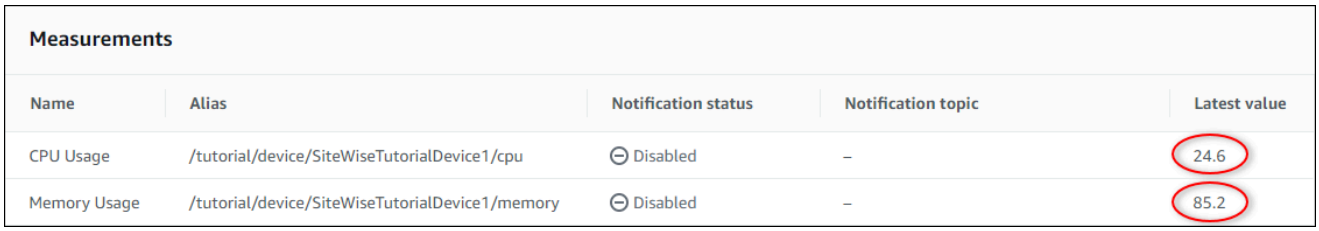
    a. Vaya a la consola de AWS IoT SiteWise.

    b. En el panel de navegación izquierdo, elija Assets (activos).

    c. Elija la flecha situada junto a su activo de flota de dispositivos (SiteWise Tutorial Device Fleet 1 1) para expandir su jerarquía de activos y, a continuación, elija su activo de dispositivo (SiteWise Tutorial Device 1).

    d. Elija Measurements (Medidas).

    e. Compruebe que las celdas Latest value (Valor más reciente) tengan valores para las propiedades CPU Usage y Memory Usage.



Measurements

Name	Alias	Notification status	Notification topic	Latest value
CPU Usage	/tutorial/device/SiteWiseTutorialDevice1/cpu	Disabled	–	24.6
Memory Usage	/tutorial/device/SiteWiseTutorialDevice1/memory	Disabled	–	85.2

    f. Si las propiedades CPU Usage y Memory Usage no tienen los valores más recientes, actualice la página. Si los valores no aparecen después de unos minutos, consulte Solución de problemas de las reglas.

12. Ha completado este tutorial. Si desea explorar visualizaciones en directo de sus datos, puede configurar un portal en AWS IoT SiteWise Monitor. Para obtener más información, consulte Monitorización de datos con AWS IoT SiteWise Monitor. De lo contrario, puede pulsar CTRL +C en el símbolo del sistema para detener el script del cliente del dispositivo. Es poco probable que el programa Python envíe suficientes mensajes para incurrir en gastos, pero se recomienda detener el programa cuando haya terminado.

Paso 9: Limpieza de los recursos después del tutorial

Después de completar el tutorial sobre la ingesta de datos de AWS IoT las cosas, limpia tus recursos para evitar incurrir en cargos adicionales.

Para eliminar activos jerárquicos en AWS IoT SiteWise

1. Vaya a la consola AWS IoT SiteWise.
2. En el panel de navegación izquierdo, elija Assets (activos).
3. Al eliminar activos AWS IoT SiteWise, primero debe desasociarlos.

Complete los siguientes pasos para anular la asociación de los activos de su dispositivo de su activo de flota de dispositivos:

a. Elija su activo de flota de dispositivos (SiteWise Tutorial Device Fleet 1).

b. Elija Editar.

c. En Assets associated to this asset (activos asociados a este activo), elija Disassociate (Anular asociación) para cada activo de dispositivo asociado a este activo de flota de dispositivo.

d. Seleccione Guardar.

Ahora ya no debería ver los activos de su dispositivo organizados como jerarquía.

4. Elija el activo de dispositivo (SiteWise Tutorial Device 1).
5. Elija Eliminar.
6. En el cuadro de diálogo de confirmación, escriba **`Delete`** y, a continuación, elija Delete (Eliminar).
7. Repita los pasos 4 a 6 para cada activo de dispositivo y el activo de flota de dispositivos (SiteWise Tutorial Device Fleet 1).

Para eliminar modelos de activos jerárquicos en AWS IoT SiteWise

1. Vaya a la consola de AWS IoT SiteWise.
2. Si aún no lo ha hecho, elimine el dispositivo y los activos de la flota de dispositivos. Para obtener más información, consulte el procedimiento anterior. No puede eliminar un modelo si tiene activos creados a partir de ese modelo.
3. En el panel de navegación izquierdo, elija Models (Modelos).
4. Elija su modelo de activos de flota de dispositivos (SiteWise Tutorial Device Fleet Model).

   Al eliminar modelos de activos jerárquicos, comience por eliminar primero el modelo de activos principal.
5. Elija Eliminar.
6. En el cuadro de diálogo de confirmación, escriba **`Delete`** y, a continuación, elija Delete (Eliminar).
7. Repita los pasos 4 a 6 para el modelo de activos del dispositivo (SiteWise Tutorial Device Model).

Para deshabilitar o eliminar una regla en AWS IoT Core

1. Vaya a la consola de AWS IoT.
2. En el panel de navegación de la izquierda, elija Redirección de mensajes y, a continuación, seleccione Reglas.
3. Seleccione su regla y seleccione Eliminar.
4. En el cuadro de diálogo de confirmación, ingrese el nombre de la regla y, a continuación, elija Eliminar.

Visualización y uso compartido de datos de parques eólicos en Monitor SiteWise

En este tutorial se explica cómo visualizar AWS IoT SiteWise Monitor y compartir datos industriales a través de aplicaciones web gestionadas, conocidas como portales. Cada portal abarca proyectos, lo que le proporciona la flexibilidad de elegir los datos a los que se puede acceder en cada proyecto. A continuación, especifique las personas de su organización que pueden acceder a cada portal. Sus usuarios inician sesión en los portales mediante AWS IAM Identity Center cuentas, por lo que puede utilizar su almacén de identidades existente o un almacén gestionado por él AWS.

Usted y sus usuarios con permisos suficientes pueden crear paneles en cada proyecto para visualizar sus datos industriales de manera significativa. A continuación, los usuarios pueden ver estos paneles para obtener rápidamente información sobre sus datos y monitorizar su operación. Puede configurar permisos administrativos o de solo lectura para cada proyecto para cada usuario de su empresa. Para obtener más información, consulte Monitorización de datos con AWS IoT SiteWise Monitor.

A lo largo del tutorial, mejorarás la AWS IoT SiteWise demostración y proporcionarás un conjunto de datos de muestra para un parque eólico. Configura un portal en SiteWise Monitor, crea un proyecto y paneles para visualizar los datos del parque eólico. El tutorial también incluye la creación de usuarios adicionales, junto con la asignación de permisos para ser propietario o ver el proyecto y sus paneles asociados.

> **Note**
>
> Al usar SiteWise Monitor, se le cobra por cada usuario que inicie sesión en un portal (por mes). En este tutorial, crea tres usuarios, pero solo tiene que iniciar sesión con uno. Después

de completar este tutorial, generará cargos por un usuario. Para obtener más información, consulte AWS IoT SiteWise Precios.

Temas

Requisitos previos

Necesitará lo siguiente para completar este tutorial:

- Un Cuenta de AWS. Si no dispone de una, consulte Configuración de una Cuenta de AWS.
- Un ordenador de desarrollo en ejecución WindowsmacOS,Linux, o Unix para acceder al AWS Management Console. Para obtener más información, consulte Introducción a AWS Management Console.
- Un usuario AWS Identity and Access Management (IAM) con permisos de administrador.
- Una demostración de un AWS IoT SiteWise parque eólico en funcionamiento. Al configurar la demostración, esta define los modelos y los activos AWS IoT SiteWise y les transmite datos para representar un parque eólico. Para obtener más información, consulte Uso de la AWS IoT SiteWise demostración.
- Si ha activado el Centro de identidad de IAM en su cuenta, inicie sesión en su cuenta AWS Organizations de gestión. Para obtener más información, consulte Terminología y conceptos de AWS Organizations. Si no ha habilitado el Centro de identidades de IAM, lo habilitará en este tutorial y configurará su cuenta como cuenta de administración.

  Si no puede iniciar sesión en su cuenta AWS Organizations de administración, puede completar parcialmente el tutorial siempre que tenga un usuario del IAM Identity Center en su organización. En este caso, podrá crear el portal y los paneles de control, pero no podrá crear nuevos usuarios del Centro de identidades de IAM para asignarlos a los proyectos.

Paso 1: Crear un portal en Monitor SiteWise

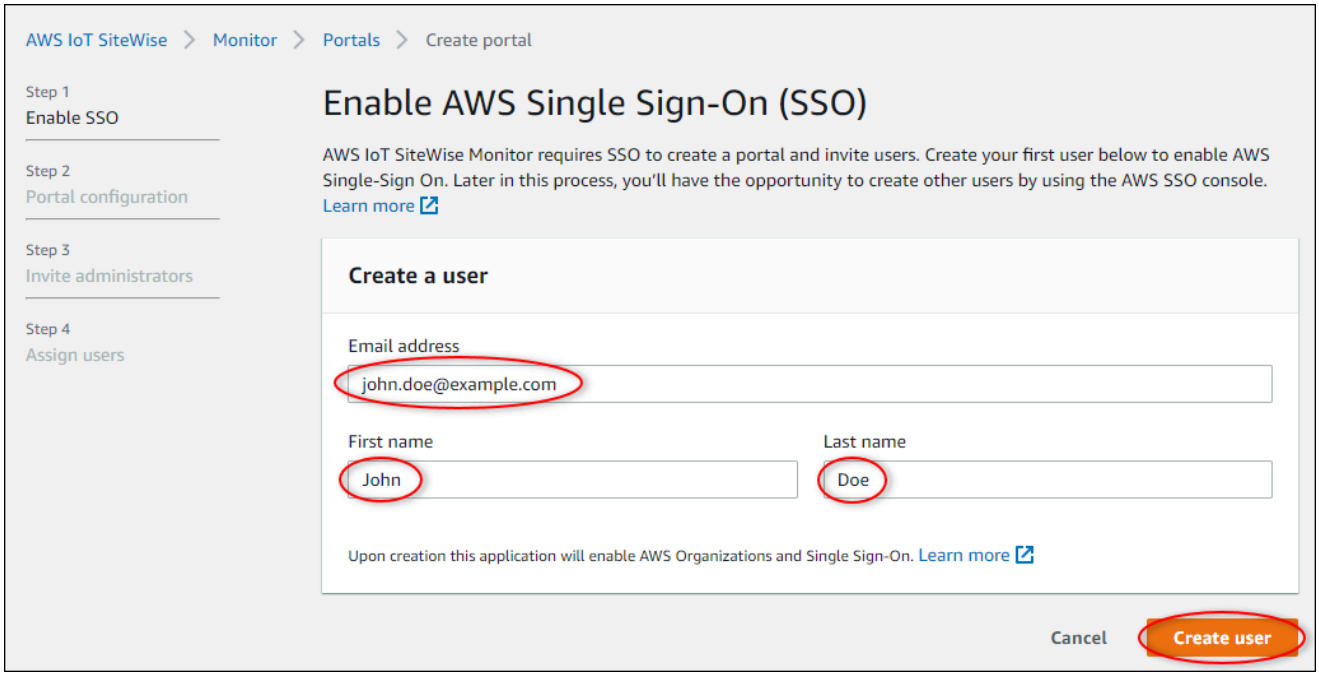
En este procedimiento, crea un portal en AWS IoT SiteWise Monitor. Cada portal es una aplicación web gestionada en la que usted y sus usuarios pueden iniciar sesión con AWS IAM Identity Center cuentas. Con el Centro de identidades de IAM, puede utilizar el almacén de identidades existente de su empresa o crear uno gestionado por AWSél. Los empleados de su empresa pueden iniciar sesión sin tener que crear un registro independiente Cuentas de AWS.

Para crear un portal

1. Inicie sesión en la consola de AWS IoT SiteWise.
2. Revisa los AWS IoT SiteWise puntos finales y las cuotas compatibles y cambia de región si AWS IoT SiteWise es necesario. Debe ejecutar la AWS IoT SiteWise demostración en la misma región.
3. En el panel de navegación izquierdo, elija Portales.
4. Elija Create portal (Crear portal).
5. Si ya ha habilitado el Centro de identidades de IAM, vaya al paso 6. Caso contrario, complete los siguientes pasos para habilitar el Centro de identidades de IAM:

    a. En la página Habilitar AWS IAM Identity Center (SSO), introduzca su dirección de correo electrónico, nombre y apellidos para crear un usuario del IAM Identity Center que será el administrador del portal. Utilice una dirección de correo electrónico a la que pueda acceder para recibir un mensaje con el fin de establecer una contraseña para su nuevo usuario del Centro de identidades de IAM.

    En un portal, el administrador del portal crea proyectos y asigna usuarios a proyectos. Puede crear más usuarios más adelante.



b. Seleccione la opción Crear un usuario.

6. En la página Configuración del portal, siga los pasos que se describen a continuación:

   a. Escriba un nombre para el portal, como **`WindFarmPortal`**.

   b. (Opcional) Escriba una descripción para el portal. Si tiene varios portales, utilice descripciones significativas para realizar un seguimiento de lo que contiene cada portal.

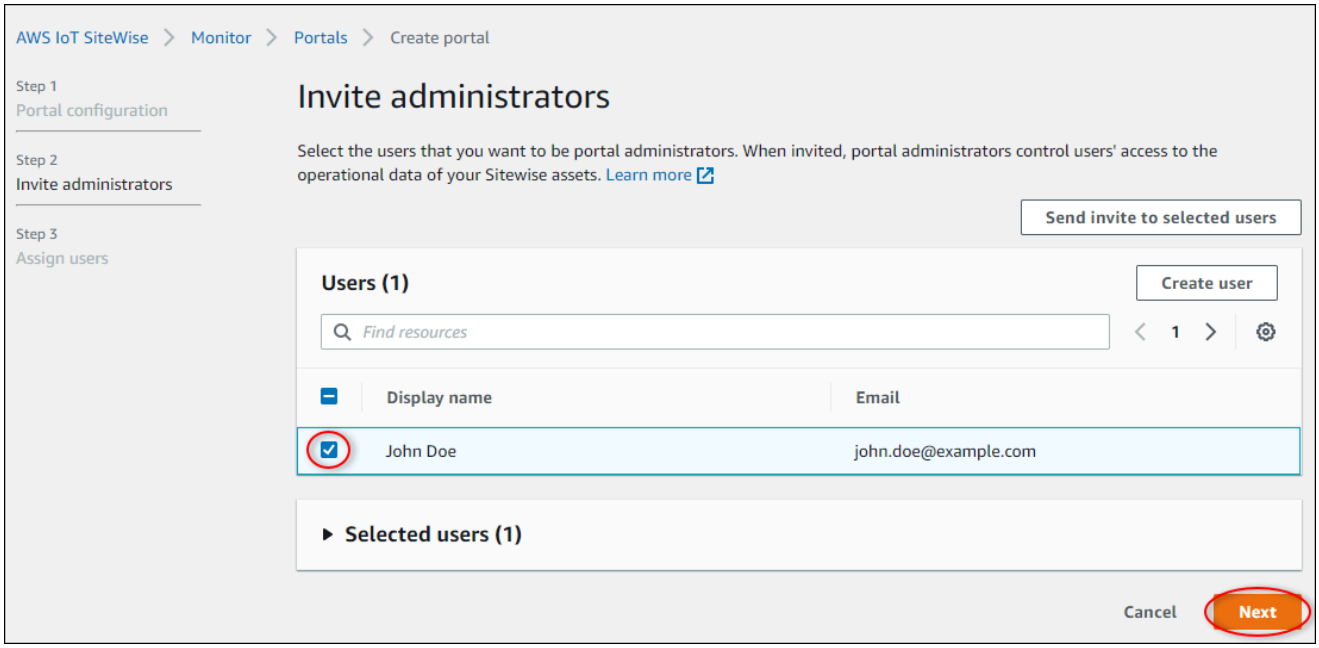
   c. (Opcional) Cargue una imagen para mostrarla en el portal.

   d. Introduzca una dirección de correo electrónico con la que los usuarios del portal puedan ponerse en contacto cuando tengan un problema con el portal y necesiten la ayuda del AWS administrador de la empresa para resolverlo.

   e. Elija Create portal (Crear portal).

7. En la página Invitar administradores, puede asignar usuarios del Centro de identidades de IAM al portal como administradores. Los administradores del portal administran los permisos y los proyectos dentro de un portal. En esta página, haga lo siguiente:

   a. Seleccione un usuario que vaya a ser el administrador del portal. Si habilitó el Centro de identidades de IAM anteriormente en este tutorial, seleccione el usuario que creó.



b. (Opcional) Elija Enviar invitación a los usuarios seleccionados. Se abrirá su cliente de correo electrónico y aparecerá una invitación en el cuerpo del mensaje. Puede personalizar el correo electrónico antes de enviarlo a los administradores del portal. También puede enviar el correo electrónico a los administradores de su portal más tarde. Si es la primera vez que prueba SiteWise Monitor y va a ser el administrador del portal, no es necesario que se envíe un correo electrónico.

c. Elija Siguiente.

8. En la página Asignar usuarios, puede asignar usuarios del Centro de identidades de IAM al portal. Posteriormente, los administradores del portal podrán asignar a estos usuarios como propietarios u observadores de proyectos. Los propietarios de proyectos pueden crear paneles de control en los proyectos. Los observadores de proyectos tienen acceso de solo lectura a los proyectos que tengan asignados. En esta página puede crear usuarios del Centro de identidades de IAM para añadirlos al portal.

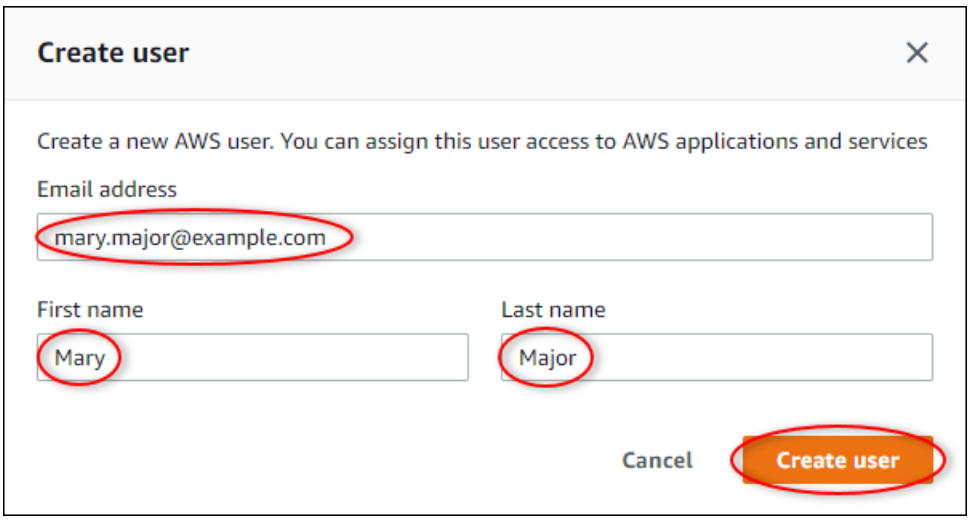
> **Note**
>
> Si no ha iniciado sesión en su cuenta AWS Organizations de administración, no podrá crear usuarios del IAM Identity Center. Seleccione Asignar usuarios para crear el portal sin usuarios del portal y, a continuación, omita este paso.

En esta página, haga lo siguiente:

a. Complete los siguientes pasos dos veces para crear dos usuarios del Centro de identidades de IAM:

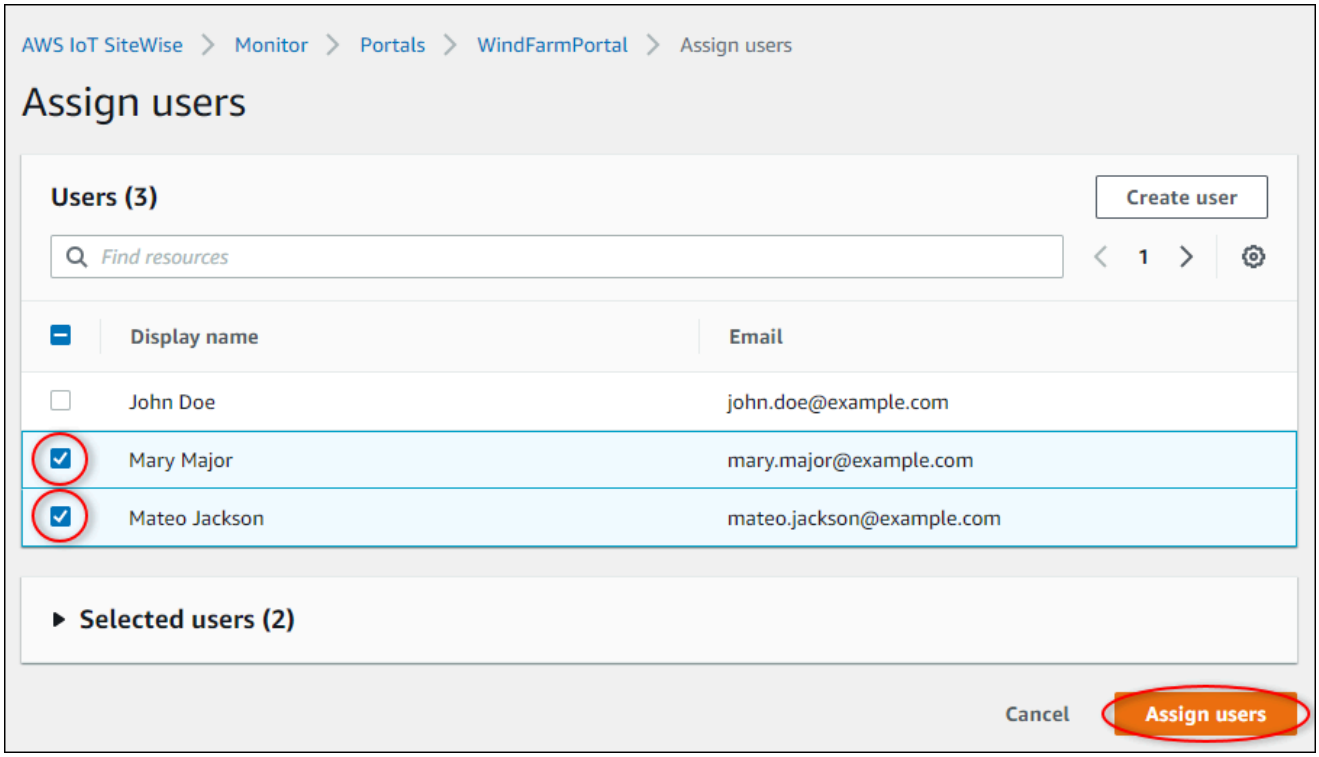
   i. Seleccione Crear usuario para abrir un cuadro de diálogo en el que introducirá los detalles del nuevo usuario.

   ii. Introduzca Dirección de correo electrónico, Nombre y Apellido para el nuevo usuario. El Centro de identidades de IAM enviará al usuario un correo electrónico para que establezca su contraseña. Si desea iniciar sesión en el portal como estos usuarios, elija una dirección de correo electrónico a la que pueda acceder. Cada dirección de correo electrónico debe ser única. Sus usuarios inician sesión en el portal utilizando su dirección de correo electrónico como nombre de usuario.



   iii. Seleccione la opción Crear un usuario.

b. Seleccione los dos usuarios del Centro de identidades de IAM que creó en el paso anterior.



c. Seleccione Asignar usuarios para añadir estos usuarios al portal.

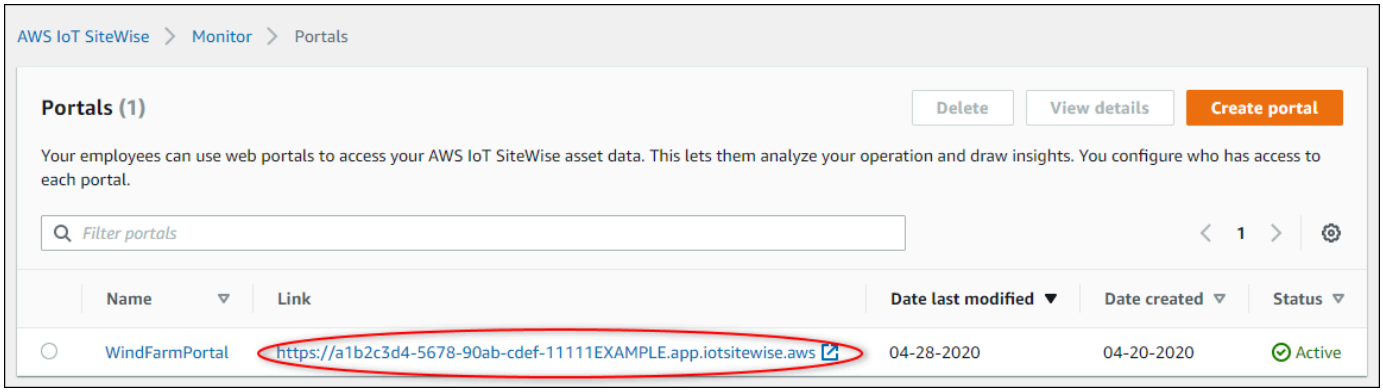
La página de portales se abre con su nuevo portal mostrado.

Paso 2: inicie sesión en un portal

En este procedimiento, inicie sesión en el nuevo portal con el AWS IAM Identity Center usuario que agregó al portal.

Para iniciar sesión en un portal

1. En la página Portals (Portales), elija el Link (Enlace) del nuevo portal para abrirlo en una nueva pestaña.



2. Si ha creado su primer usuario del Centro de identidades de IAM anteriormente en el tutorial, realice los pasos siguientes para crear una contraseña para su usuario:

   a. Revise su correo electrónico para ver el asunto Invitation to join AWS IAM Identity Center.

   b. Abra ese correo electrónico de invitación y elija Accept invitation.

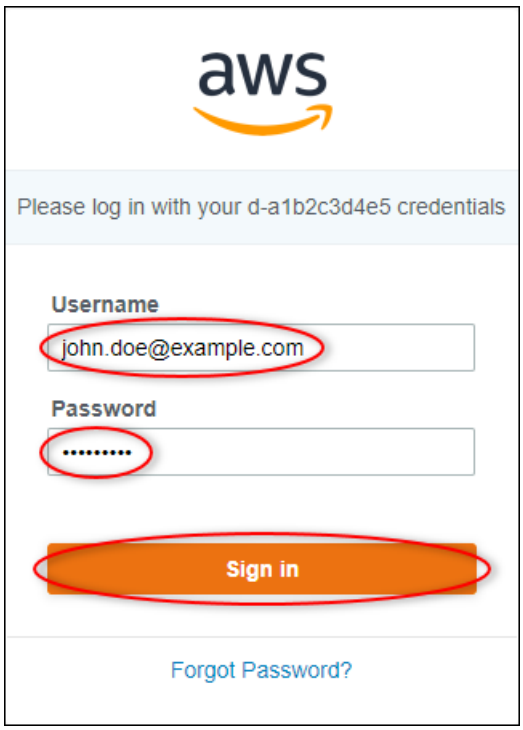
   c. En la nueva ventana, establezca una contraseña para su usuario del Centro de identidades de IAM.

   Si desea iniciar sesión más adelante en el portal como el segundo y tercer usuario del Centro de identidades de IAM que creó anteriormente, también puede completar estos pasos para establecer las contraseñas de dichos usuarios.

   > **Note**
   >
   > Si no ha recibido un correo electrónico, puede generar una contraseña para su usuario en la consola del Centro de identidades de IAM. Para obtener más información, consulte Restablecimiento de una contraseña de usuario en la Guía del usuario de AWS IAM Identity Center .

3. Introduzca su Username y Password del Centro de identidades de IAM. Si creó su usuario del Centro de identidades de IAM anteriormente en este tutorial, su Username es la dirección de correo electrónico del usuario administrador del portal que creó.

   Todos los usuarios del portal, incluyendo el administrador del portal, deben iniciar sesión con sus credenciales de usuario del Centro de identidades de IAM. Normalmente, estas credenciales no son las mismas que se utilizan para iniciar sesión en la AWS Management Console.



4. Elija Sign in.

   Se abrirá su portal.

Paso 3: Cree un proyecto de parque eólico

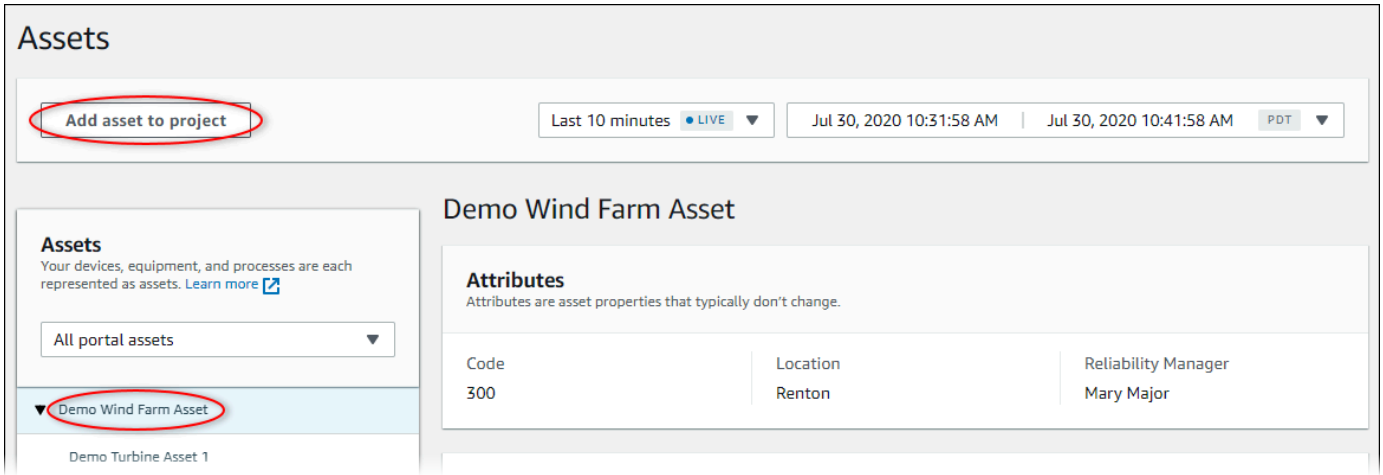
En este procedimiento, crea un proyecto en el portal. Los proyectos son recursos que definen un conjunto de permisos, activos y paneles, que puede configurar para visualizar los datos de los activos de ese proyecto. Con los proyectos, define quién tiene acceso a qué subconjuntos de su operación y cómo se visualizan los datos de esos subconjuntos. Puede asignar a los usuarios del portal como propietarios u observadores de cada proyecto. Los propietarios de proyectos pueden crear paneles de control para visualizar datos y compartir el proyecto con otros usuarios. Los observadores de proyectos pueden ver los paneles de control, pero no editarlos. Para obtener más información sobre las funciones en SiteWise Monitor, consulteSiteWise Supervise las funciones.

Para crear un proyecto de parque eólico

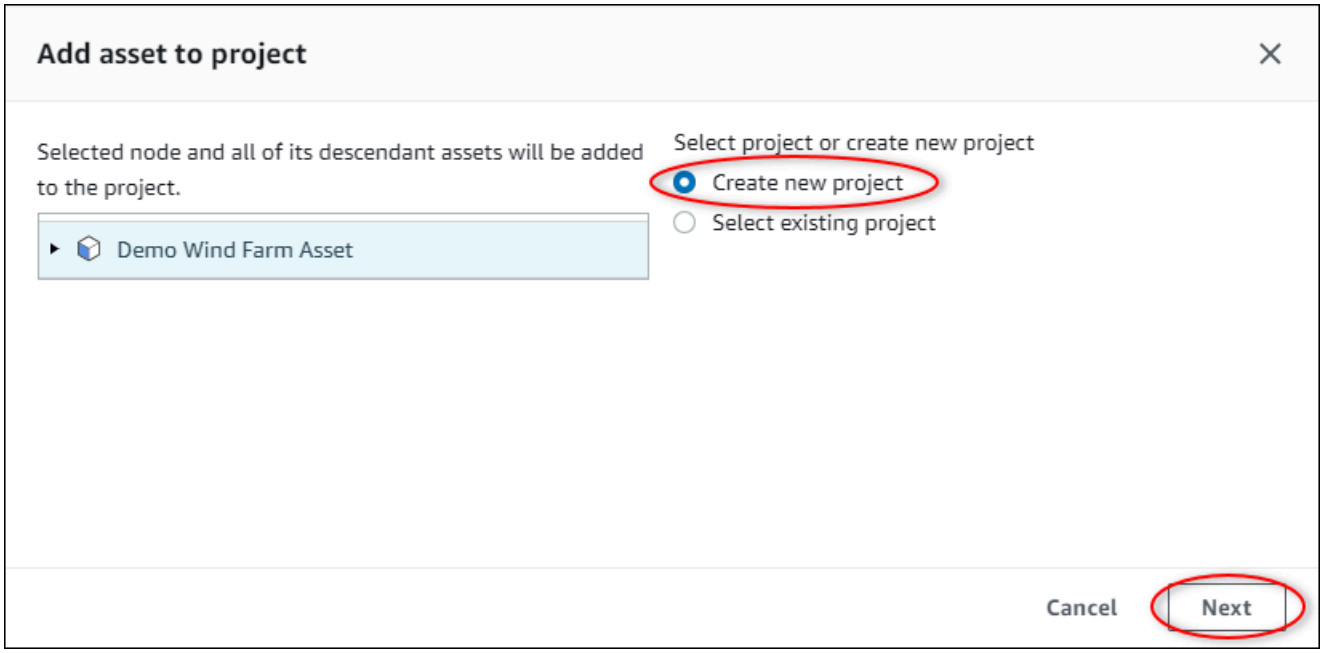
1. En el panel de navegación izquierdo de su portal, seleccione la pestaña Activos. En la página Activos, puede explorar todos los activos disponibles en el portal y añadirlos a proyectos.

2. En el navegador de activos, elija Demo Wind Farm Asset. Al elegir un activo, puede explorar los datos históricos y en directo del mismo. También puede presionar Shift para seleccionar varios activos y comparar sus datos side-by-side.

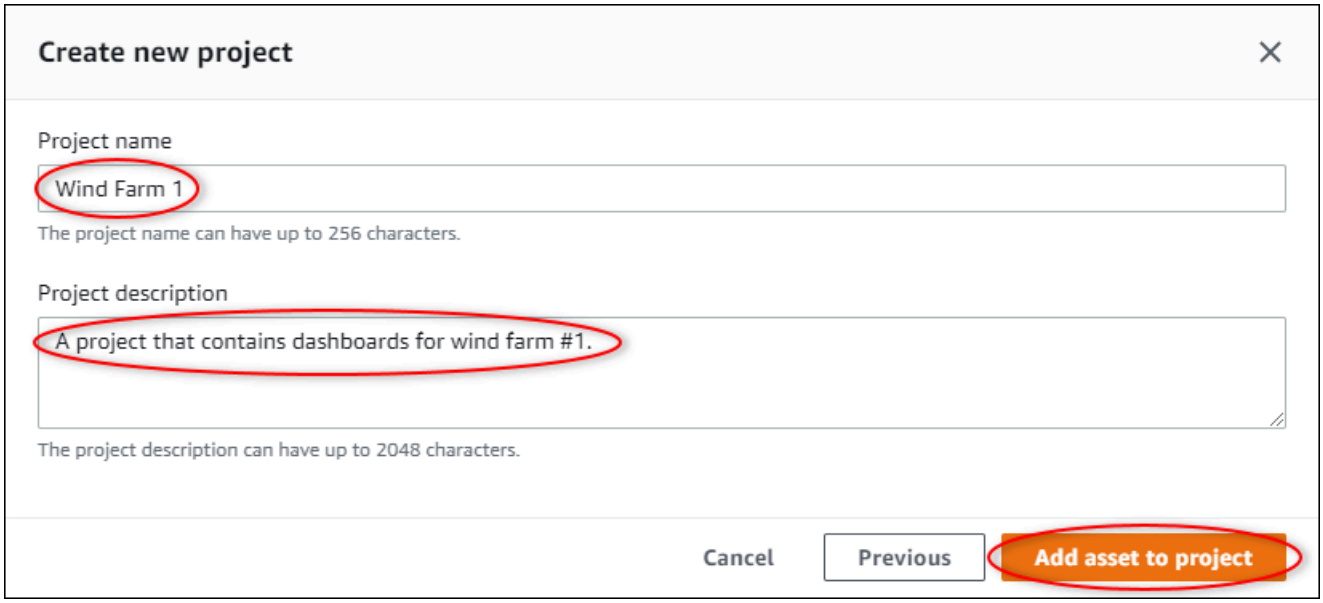
3. Seleccione Añadir activo a proyecto en la parte superior izquierda. Los proyectos contienen paneles que pueden ver los usuarios del portal para explorar los datos. Cada proyecto tiene acceso a un subconjunto de tus activos en AWS IoT SiteWise. Cuando añade un activo a un proyecto, todos los usuarios con acceso a ese proyecto también pueden acceder a los datos de ese activo y sus elementos secundarios.



4. En el cuadro de diálogo Añadir activo al proyecto, seleccione Crear nuevo proyecto y, a continuación, Siguiente.



5. En el cuadro de diálogo Crear nuevo proyecto, introduzca el Nombre del proyecto y una Descripción del proyecto para su proyecto y, a continuación, seleccione Añadir activo al proyecto.



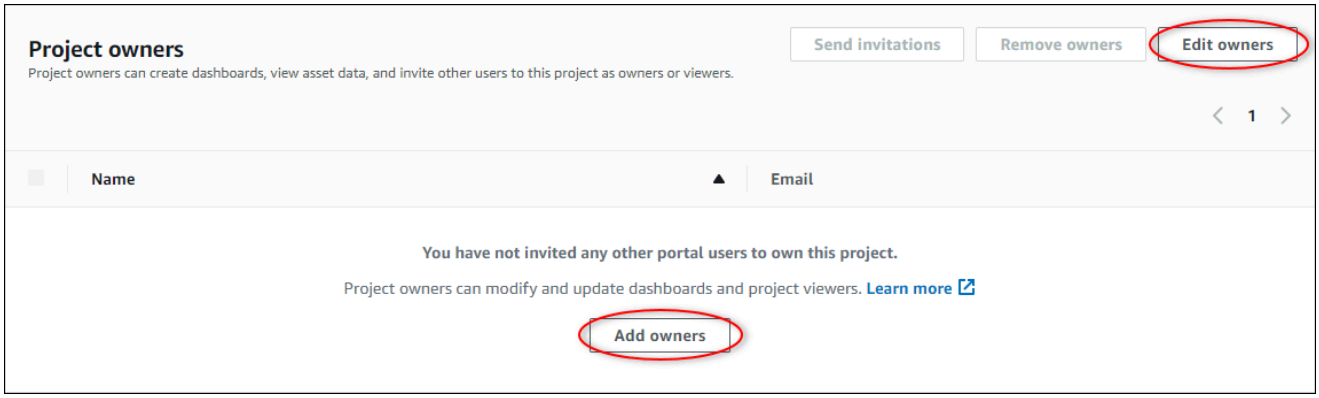
   Se abrirá la página de su nuevo proyecto.

6. En la página del proyecto, puede añadir usuarios del portal como propietarios u observadores de este proyecto.

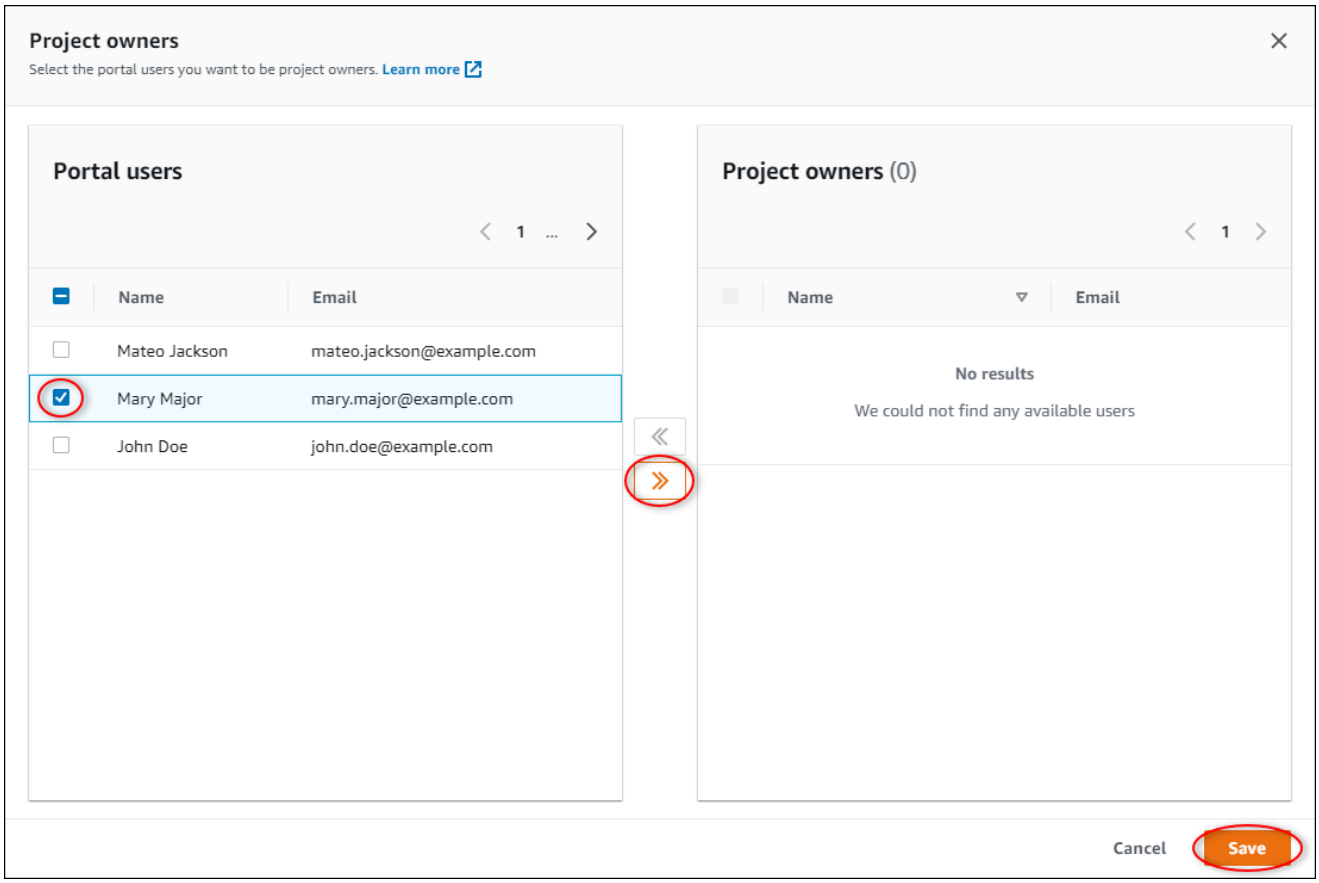
   > **Note**
   >
   > Si no ha iniciado sesión en su cuenta de AWS Organizations administración, es posible que no tenga usuarios del portal para asignar a este proyecto, por lo que puede omitir este paso.

   En esta página, haga lo siguiente:

   a. En Propietarios del proyecto, elija Añadir propietarios o Editar usuarios.



b. Elija el usuario que se va a añadir como propietario del proyecto (por ejemplo, Mary Major) y, a continuación, elija el icono >>.



c. Seleccione Guardar.

Su usuario Mary Major del Centro de identidades de IAM puede iniciar sesión en este portal para editar los paneles de control de este proyecto y compartirlo con otros usuarios de este portal.

d. En Observadores del proyecto, elija Añadir observadores o Editar usuarios.

e. Elija el usuario que desee añadir como observador del proyecto (por ejemplo, Mateo Jackson) y, a continuación, seleccione el icono **>>**.

f. Seleccione Guardar.

Su usuario Mateo Jackson del Centro de identidades de IAM puede acceder a este portal para ver, pero no editar, los paneles de control del proyecto del parque eólico.

Paso 4: Crea un panel para visualizar los datos del parque eólico

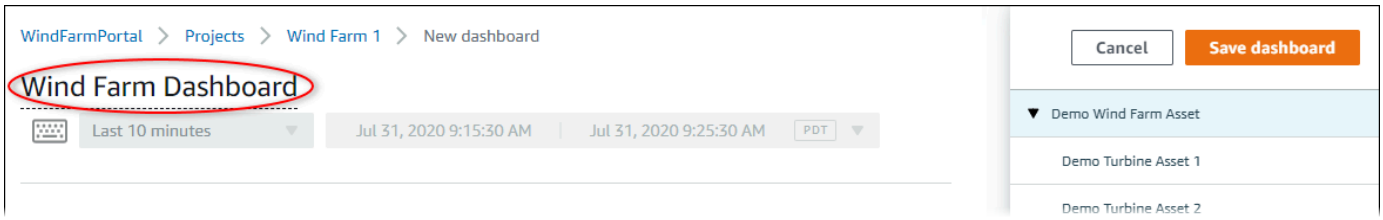
En este procedimiento, creará paneles para visualizar los datos de parques eólicos de demostración. Los paneles contienen visualizaciones personalizables de los datos de activos del proyecto. Cada visualización puede tener un tipo diferente, como un gráfico de líneas, un gráfico de barras o una pantalla de indicadores clave de rendimiento (KPI). Puede elegir el tipo de visualización que mejor se adapte a sus datos. Los propietarios de los proyectos pueden editar los paneles, mientras que los espectadores de los proyectos solo pueden verlos para obtener información.

Para crear un panel con visualizaciones

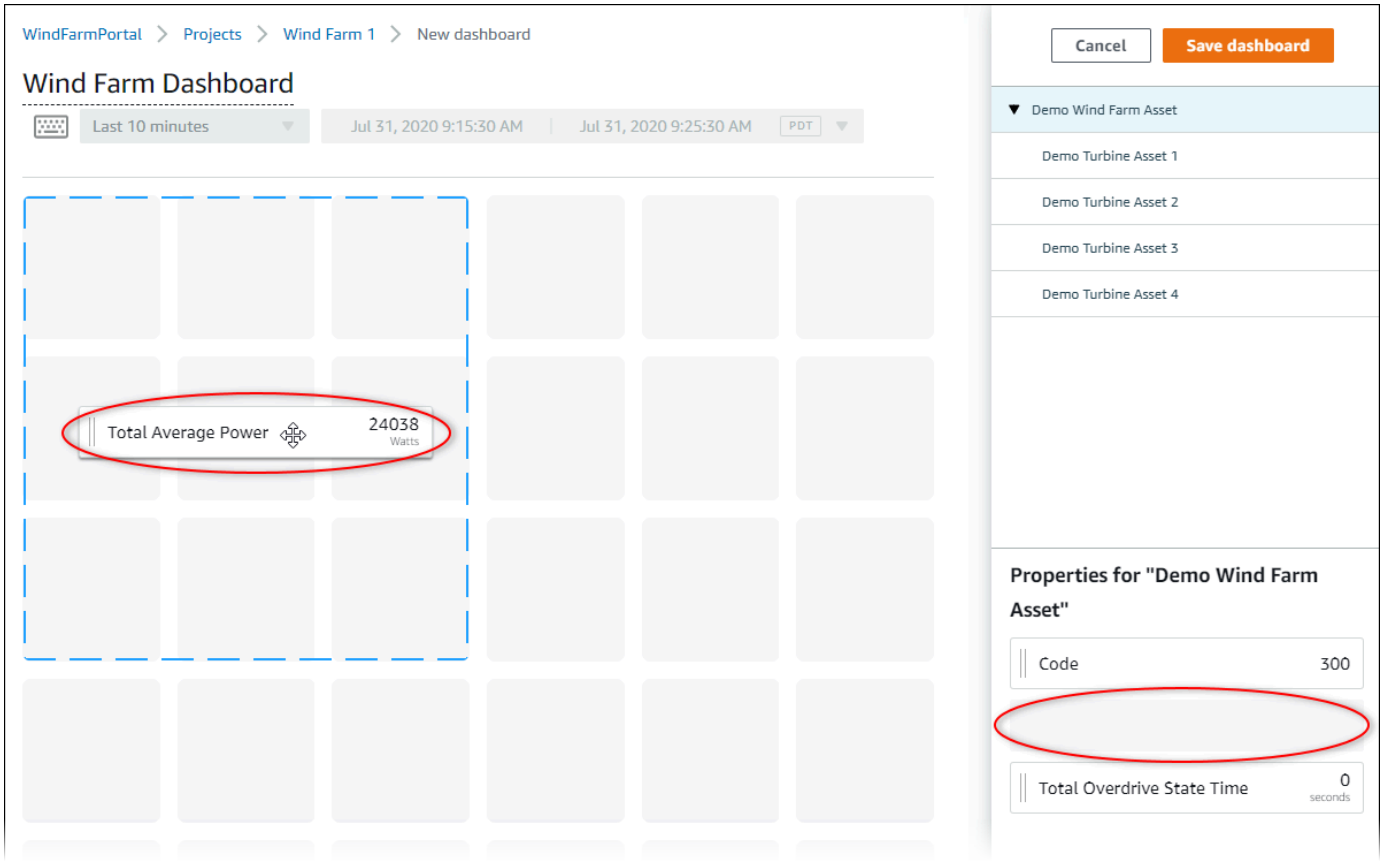
1. En la página de su nuevo proyecto, seleccione Crear panel de control para crear un panel de control y abrir su página de edición.

   En la página de edición de un panel, puede arrastrar las propiedades de los activos desde la jerarquía de activos hasta el panel para crear visualizaciones. A continuación, puede editar el título, los títulos de leyenda, el tipo, el tamaño y la ubicación de cada visualización en el panel.

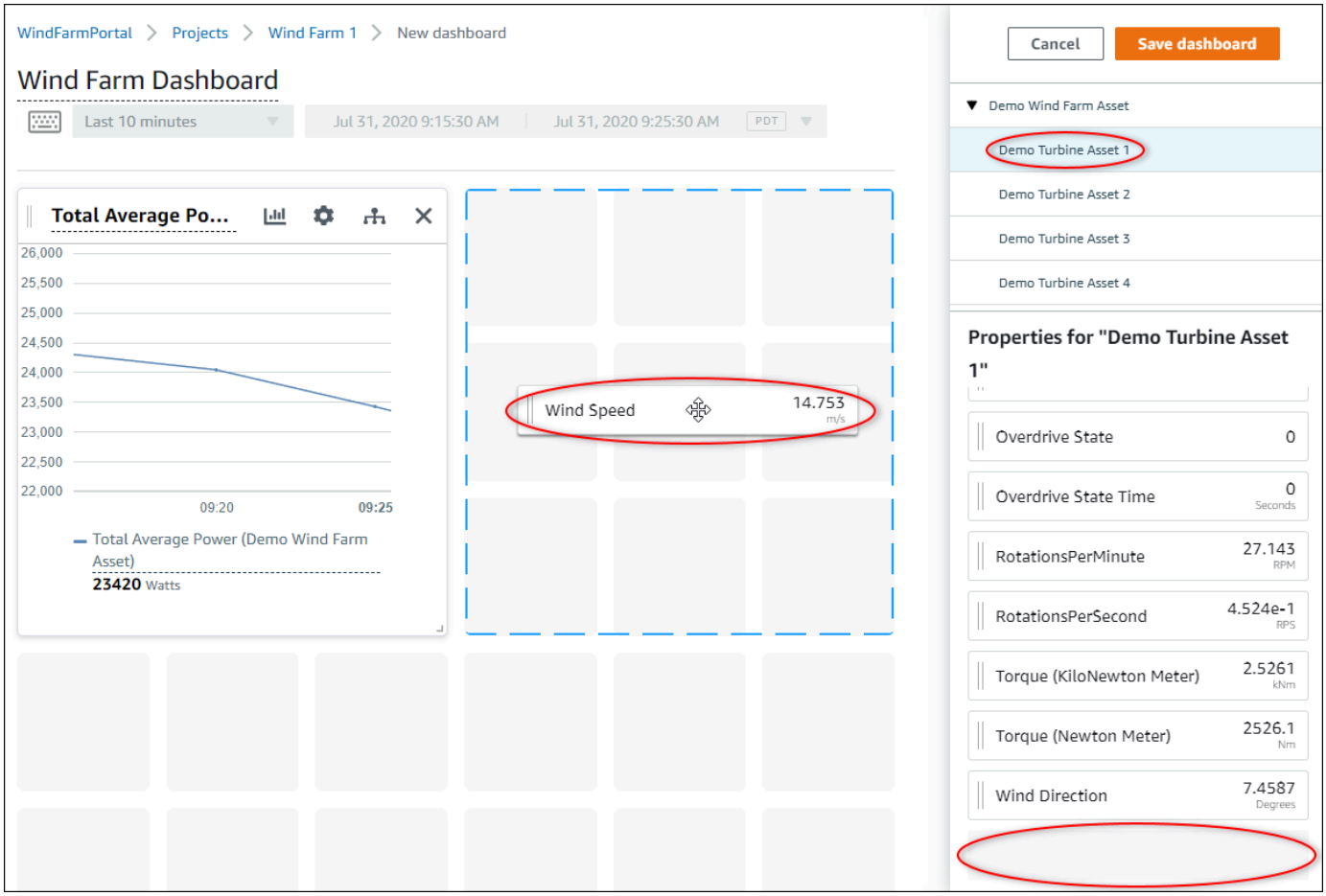
2. Introduzca un nombre para su panel de control.



3. Arrastre Total Average Power desde el Demo Wind Farm Asset hasta el panel para crear una visualización.

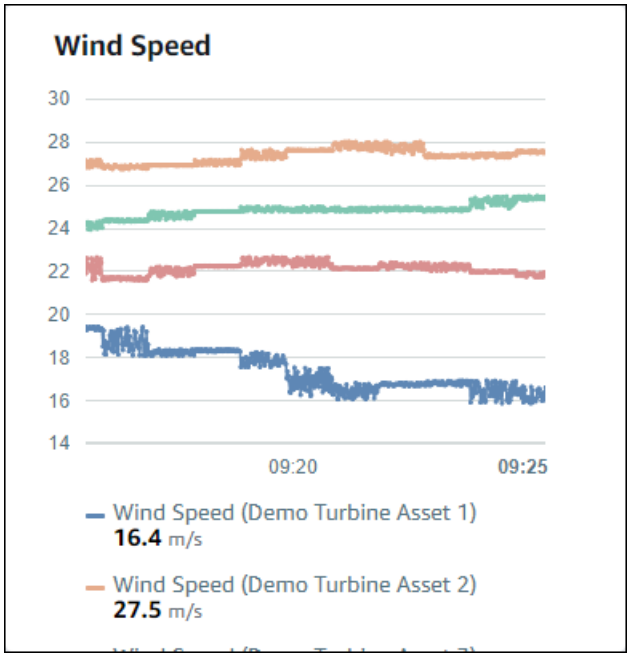


4. Seleccione Demo Turbine Asset 1 para mostrar las propiedades de ese activo y, a continuación, arrastre Wind Speed al panel de control para crear una visualización de velocidad del viento.

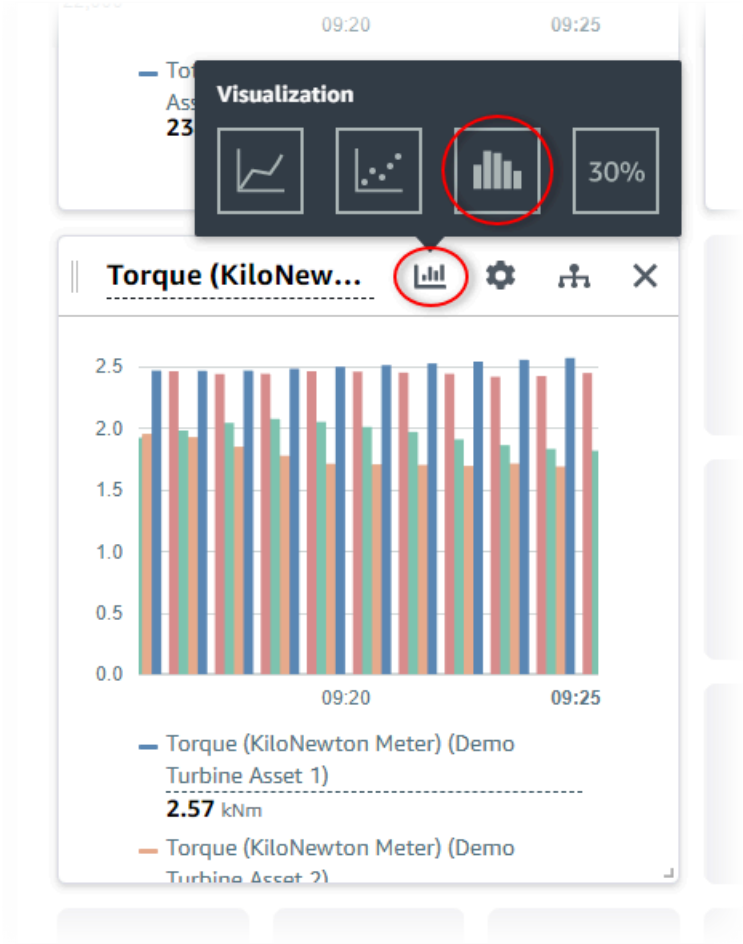


5. Añada Wind Speed a la nueva visualización de la velocidad del viento para cada Demo Turbine Asset 2, 3 y 4 (en ese orden).

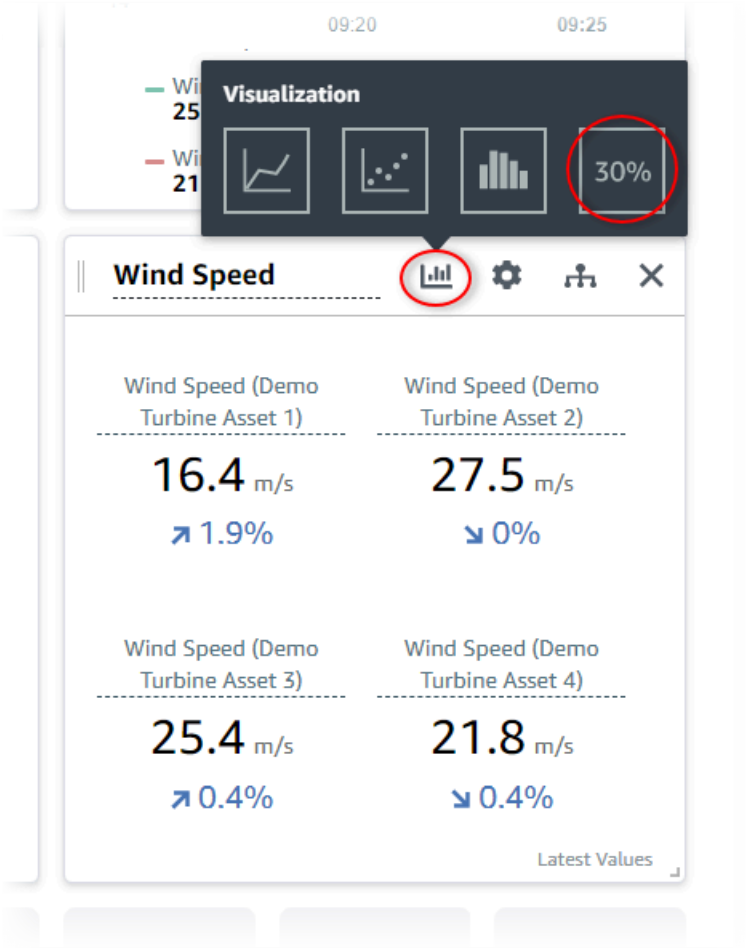
   Su visualización Wind Speed debería ser similar a la siguiente captura de pantalla.



6. Repita los pasos 4 y 5 para las propiedades de Torque (KiloNewton Meter) de las turbinas eólicas a fin de crear una visualización de par de las turbinas eólicas.
7. Seleccione el icono de tipo de visualización para la visualización de Torque (KiloNewton Meter) y, a continuación, el icono de gráfico de barras.

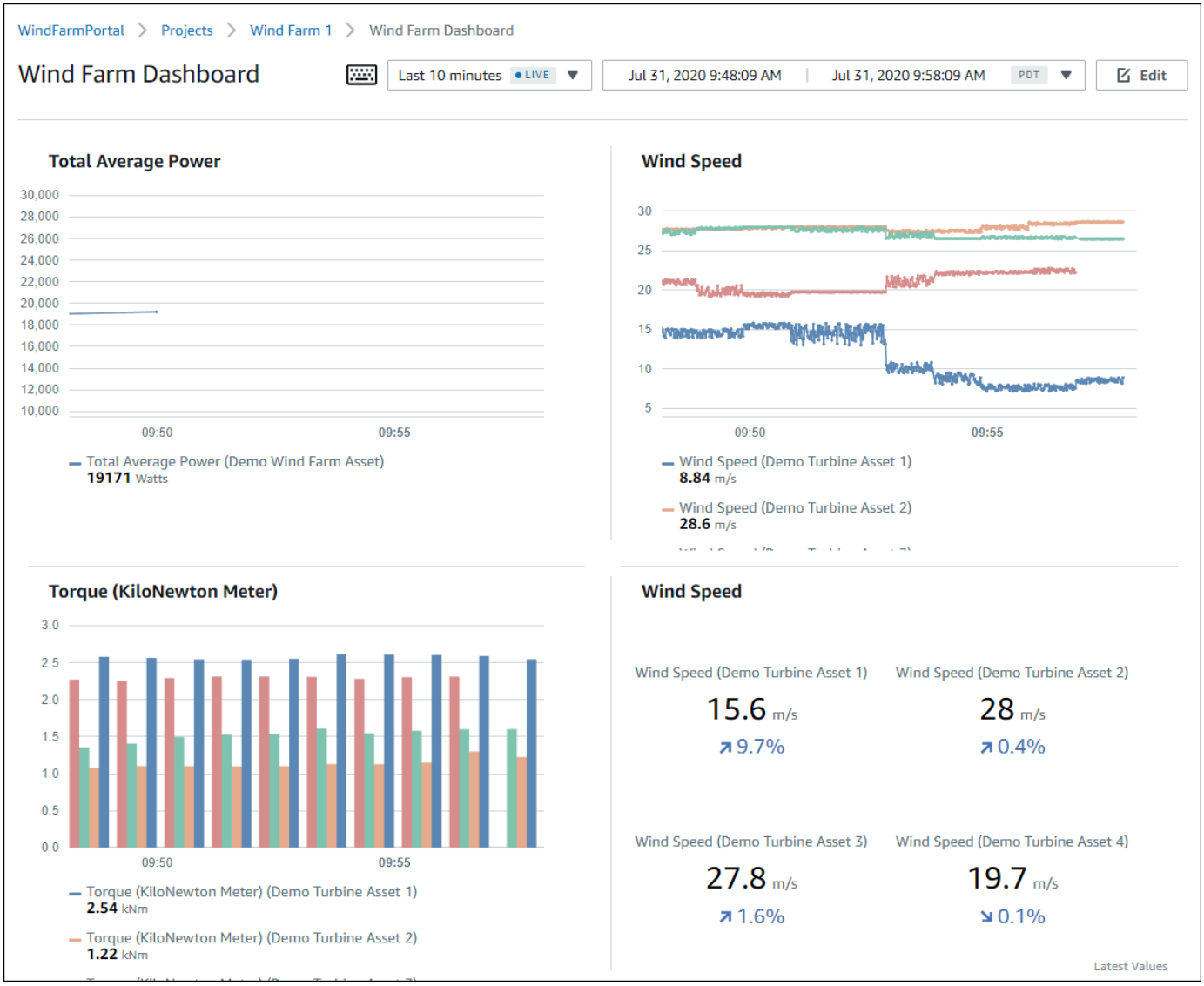


8. Repita los pasos 4 y 5 para las propiedades de Wind Direction de las turbinas eólicas a fin de crear una visualización de dirección del viento.
9. Seleccione el icono de tipo de visualización para la visualización de Wind Direction y, a continuación, el icono de gráfico de KPI (30%).



10. (Opcional) Realice otros cambios en el título, los títulos de leyenda, el tipo, el tamaño y la ubicación de cada visualización según sea necesario.
11. Seleccione Guardar panel de control en la esquina superior derecha para guardar su panel.

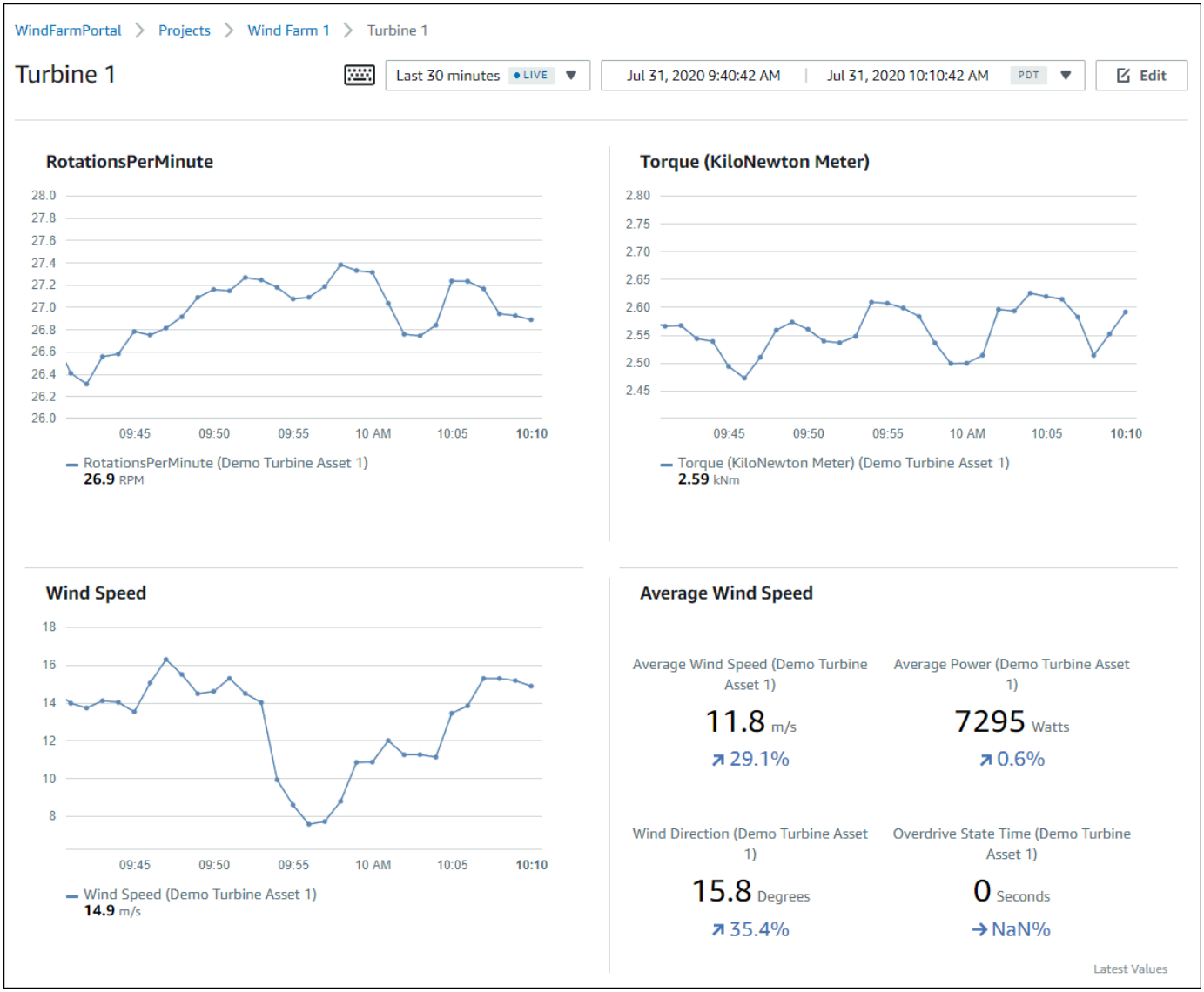
    El panel debe tener un aspecto similar a la siguiente captura de pantalla.



12. (Opcional) Cree un panel adicional para cada activo de turbina eólica.

    Como práctica recomendada, se recomienda crear un panel para cada activo de modo que los observadores del proyecto puedan investigar cualquier problema con cada activo individual. Solo puede añadir hasta 5 activos a cada visualización, por lo que debe crear varios paneles para los activos jerárquicos en muchos escenarios.

    Un panel para una turbina eólica de demostración podría tener un aspecto similar a la siguiente captura de pantalla.



13. (Opcional) Cambie la línea temporal o seleccione puntos de datos en una visualización para explorar los datos del panel. Para obtener más información, consulte Visualización de paneles de control en la Guía de la aplicación AWS IoT SiteWise Monitor .

Paso 5: Explore el portal

En este procedimiento, puede explorar el portal como un usuario con menos permisos que un administrador AWS IoT SiteWise del portal.

Para explorar el portal y finalizar el tutorial

- (Opcional) Si ha añadido otros usuarios al proyecto como propietarios u observadores, puede iniciar sesión en el portal como estos usuarios. Esto le permite explorar el portal como un usuario con menos permisos que un administrador del portal.

  > **Important**
  >
  > Se le cobra por cada usuario que inicie sesión en el portal. Para obtener más información, consulte AWS IoT SiteWise Precios.

  Para explorar el portal como otros usuarios, haga lo siguiente:

  a. Seleccione Cerrar sesión en la parte inferior izquierda del portal para salir de la aplicación web.

  b. Seleccione Cerrar sesión en la parte superior derecha del portal de la aplicación del Centro de identidades de IAM para cerrar sesión como usuario de IAM.

  c. Inicie sesión en el portal como el usuario de Centro de identidades de IAM que asignó como propietario del proyecto u observador del proyecto. Para obtener más información, consulte Paso 2: inicie sesión en un portal.

Ha completado este tutorial. Cuando termine de explorar su parque eólico de demostración en SiteWise Monitor, siga el siguiente procedimiento para limpiar sus recursos.

Paso 6: Limpiar los recursos después del tutorial

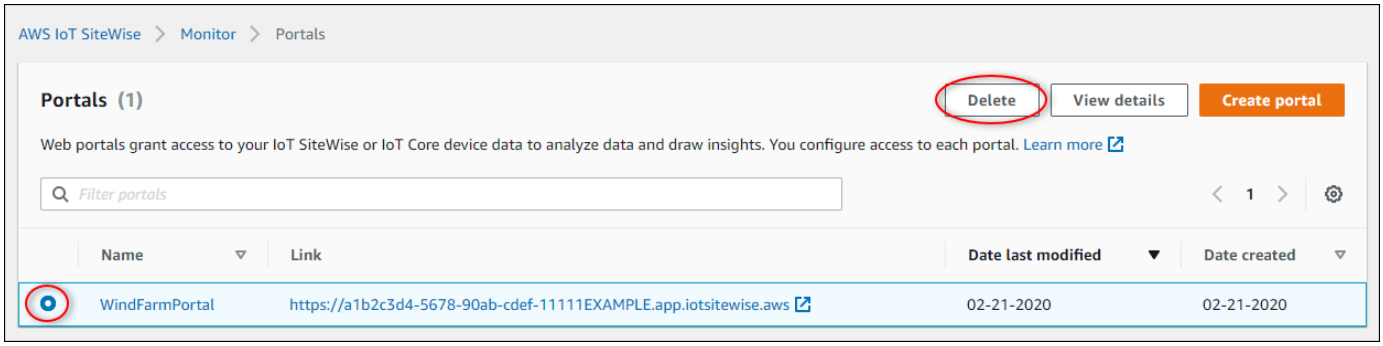
Una vez que complete el tutorial, puede sanear sus recursos. No se le cobrará por AWS IoT SiteWise si los usuarios no inician sesión en el portal, pero puede eliminar este y los usuarios de Directorio de AWS IAM Identity Center . Sus activos de parque eólico de demostración se eliminan al final de la duración que eligió al crear la demostración, o puede eliminar la demostración manualmente. Para obtener más información, consulte Eliminar la AWS IoT SiteWise demostración.

Utilice los siguientes procedimientos para eliminar su portal y los usuarios del Centro de identidades de IAM.

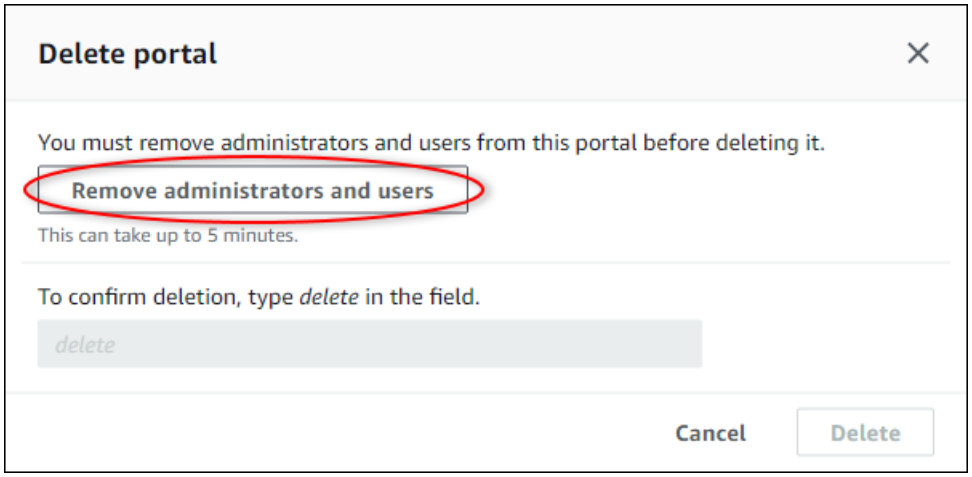
Para eliminar un portal

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación izquierdo, elija Portales.
3. Elija su portal y WindFarmPortal, a continuación, elija Eliminar.

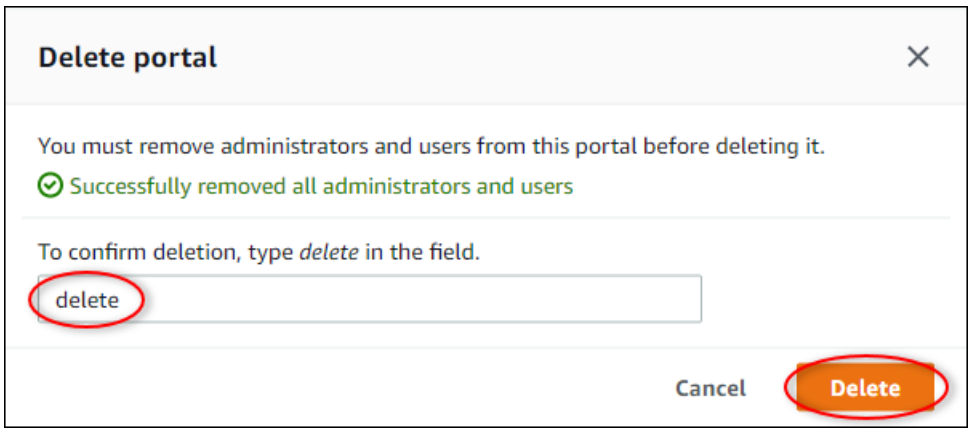
   Al eliminar un portal o proyecto, los activos asociados a los proyectos eliminados no se ven afectados.



4. En el cuadro de diálogo Eliminar portal, seleccione Eliminar administradores y usuarios.

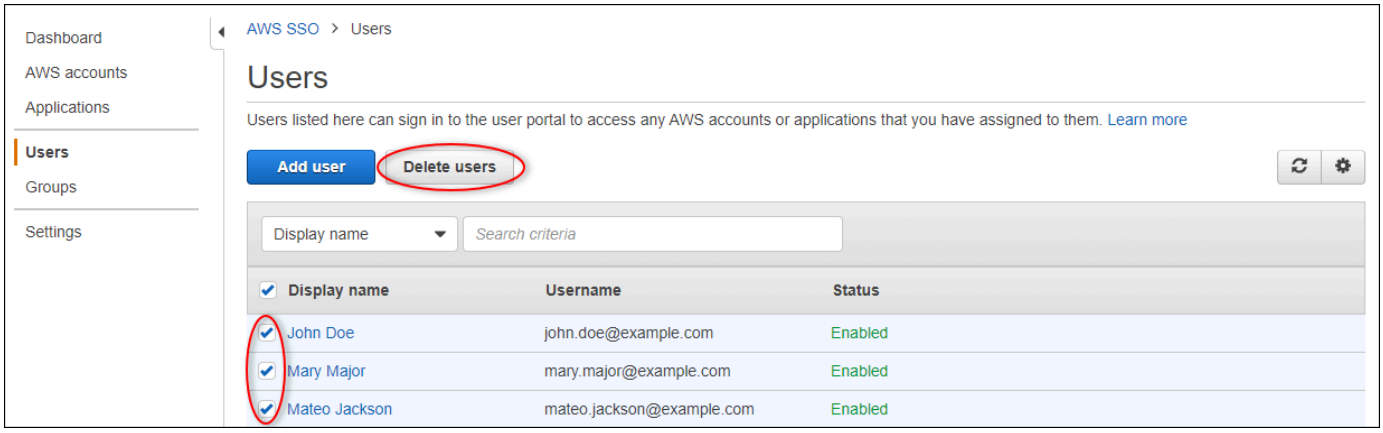


5. Escriba **`delete`** para confirmar la eliminación y, a continuación, elija Delete (Eliminar).

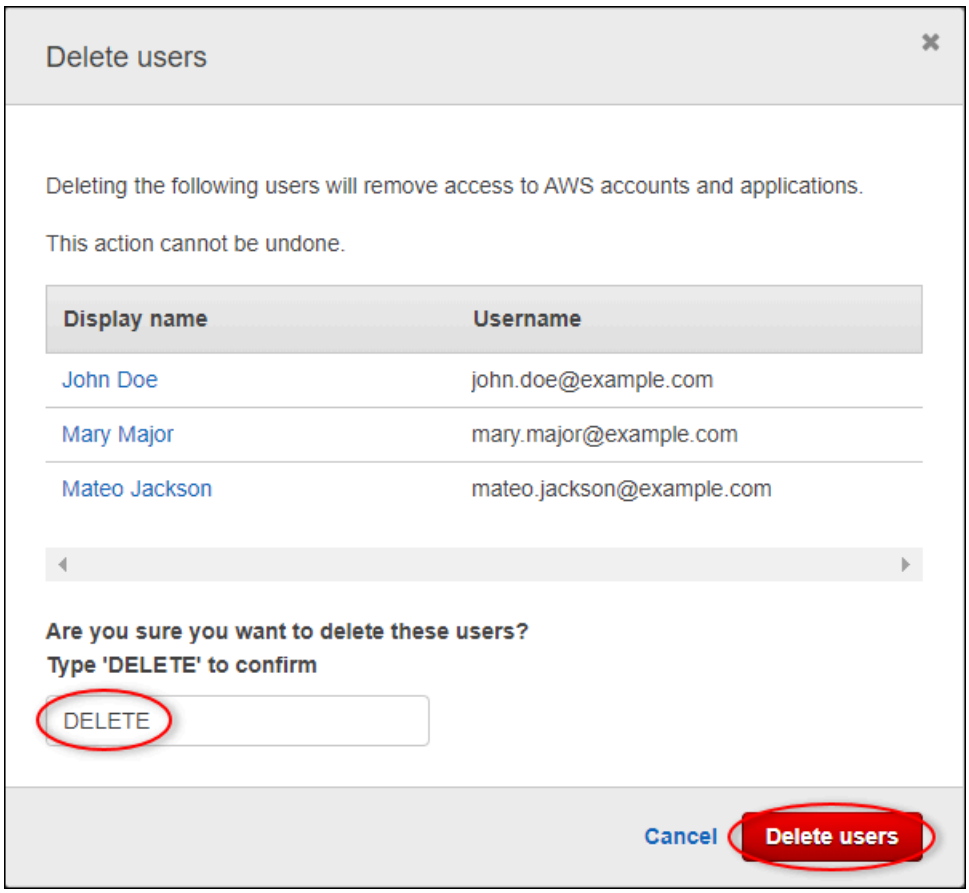


Para eliminar usuarios del Centro de identidades de IAM

1. Navegue hasta la consola del Centro de identidades de IAM.
2. En el panel de navegación izquierdo, elija Users (Usuarios).
3. Active la casilla de verificación de cada usuario que desee eliminar y, a continuación, elija Delete users (Eliminar usuarios).



4. En el cuadro de diálogo Eliminar usuarios, introduzca **DELETE** y, a continuación, seleccione Eliminar usuarios.



Publicar actualizaciones de valor de propiedad en Amazon DynamoDB

En este tutorial, se presenta una forma práctica de almacenar los datos mediante Amazon DynamoDB, lo que facilita el acceso a los datos históricos de los activos sin tener que consultar repetidamente la API. AWS IoT SiteWise Tras completar este tutorial, puede crear un software personalizado que consuma los datos de sus activos, como un mapa en tiempo real de la velocidad y la dirección del viento en todo un parque eólico. Si desea supervisar y visualizar sus datos sin implementar una solución de software personalizada, consulteMonitorización de datos con AWS IoT SiteWise Monitor.

En este tutorial, se basa en la AWS IoT SiteWise demostración que proporciona un conjunto de datos de muestra para un parque eólico. Puede configurar actualizaciones de valores de propiedad desde la demostración del parque eólico para enviar datos, a través de las reglas de AWS IoT Core, a una tabla de DynamoDB que cree. Cuando habilita las actualizaciones del valor de la propiedad, AWS IoT SiteWise envía sus datos a AWS IoT Core mensajes MQTT. A continuación, defina las reglas

AWS IoT principales que realicen acciones, como la acción de DynamoDB, en función del contenido de esos mensajes. Para obtener más información, consulte Interacción con otros AWS servicios.

Temas

Requisitos previos

Necesitará lo siguiente para completar este tutorial:

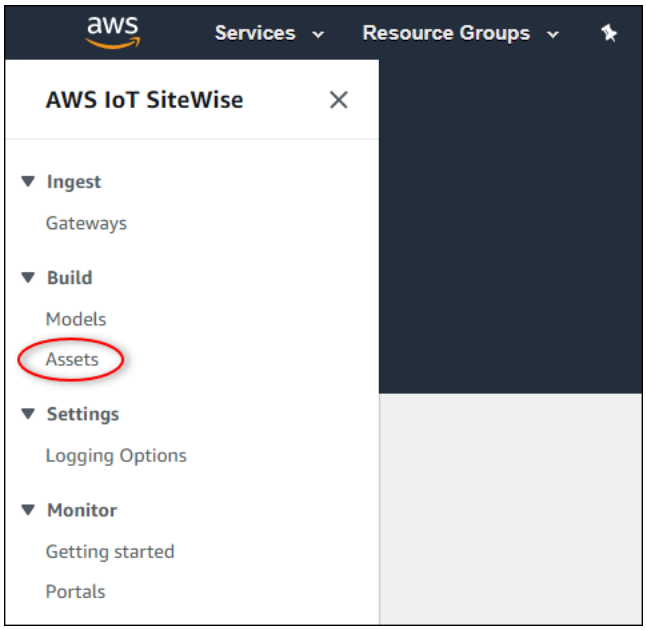
- Una AWS cuenta. Si no dispone de una, consulte Configuración de una Cuenta de AWS.
- Un ordenador de desarrollo que ejecute Windows, macOS, Linux o Unix para acceder al AWS Management Console. Para obtener más información, consulte Introducción a AWS Management Console.
- Un usuario de IAM con permisos de administrador.
- Una demostración de un AWS IoT SiteWise parque eólico en funcionamiento. Al configurar la demostración, esta define los modelos y los activos AWS IoT SiteWise y les transmite datos para representar un parque eólico. Para obtener más información, consulte Uso de la AWS IoT SiteWise demostración.

Paso 1: AWS IoT SiteWise Configúrelo para publicar las actualizaciones del valor de la propiedad

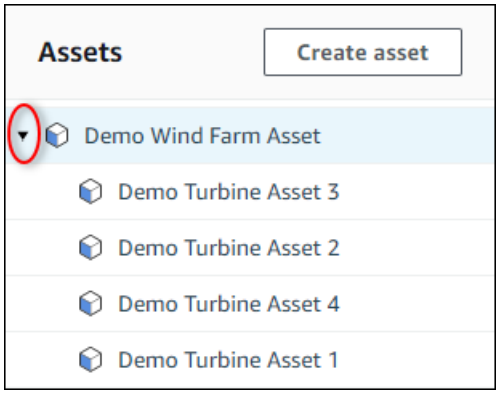
En este procedimiento, se habilitan las notificaciones de valores de propiedad en las propiedades Wind Speed de los activos de la turbina de demostración. Tras activar las notificaciones del valor de las propiedades, AWS IoT SiteWise publica cada actualización de valores en un mensaje de MQTT en AWS IoT Core.

Para habilitar las notificaciones de actualización de valores de propiedad en propiedades de activos

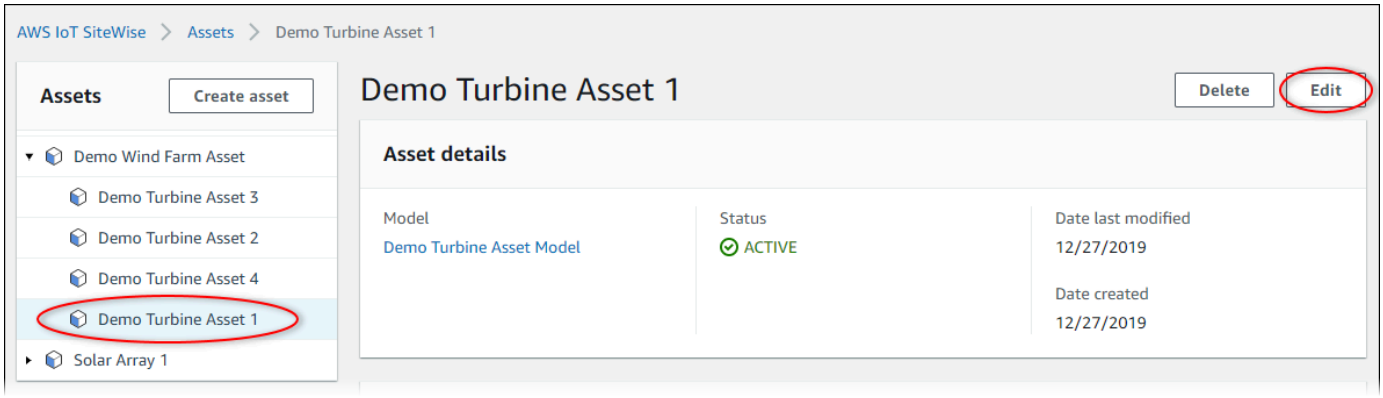
1. Inicie sesión en la consola de AWS IoT SiteWise.
2. Revise los AWS IoT SiteWise puntos finales y las cuotas compatibles y cambie de AWS región si AWS IoT SiteWise es necesario. Cambie a la región en la que esté realizando la AWS IoT SiteWise demostración.
3. En el panel de navegación izquierdo, elija Assets (activos).



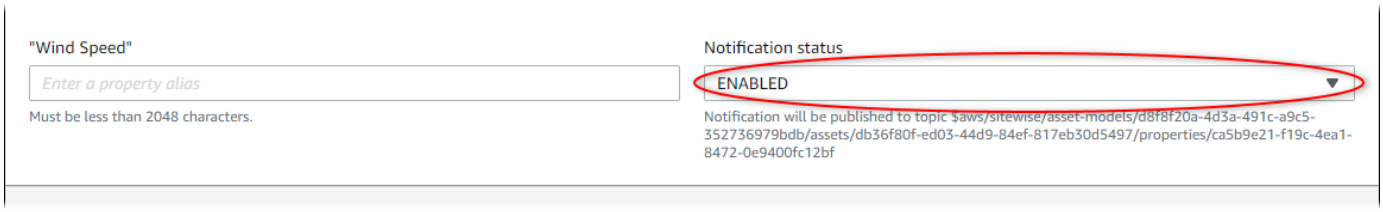
4. Elija la flecha situada junto a Demo Wind Farm Asset para ampliar la jerarquía del activo del parque eólico.



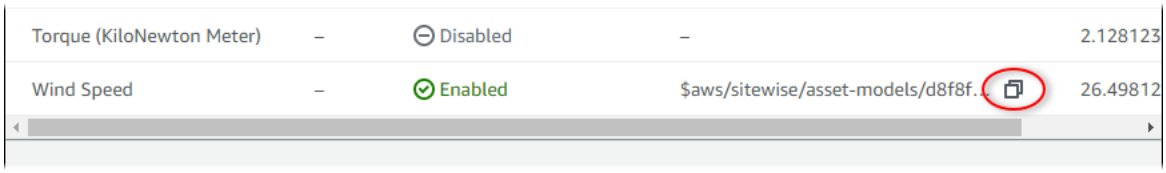
5. Elija una turbina de demostración y elija Edit (Editar).



6. Actualice el Estado de notificación de la propiedad Wind Speed a HABILITADO.



7. Elija Save asset (Guardar activo) en la parte inferior de la página.
8. Repita los pasos 5 a 7 para cada activo de turbina de demostración.
9. Elija una turbina de demostración (por ejemplo, Demo Turbine Asset 1).
10. Elija Measurements (Medidas).
11. Elija el icono copiar junto a la propiedad Wind Speed para copiar el tema de notificación en el portapapeles. Guarde el tema de notificación para utilizarlo más adelante en este tutorial. Solo necesita registrar el tema de notificación desde una turbina.



El tema de notificación debe ser similar al siguiente ejemplo.

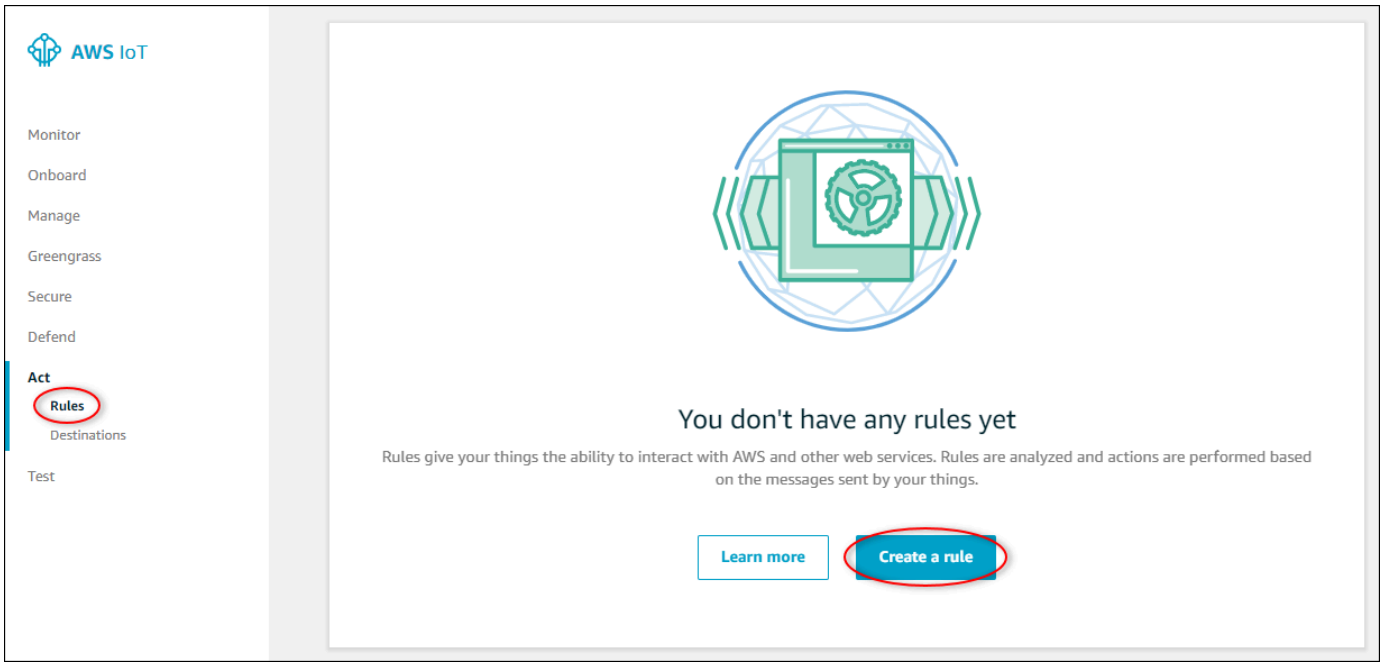
```
$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/
assets/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE/properties/a1b2c3d4-5678-90ab-
cdef-33333EXAMPLE
```

Paso 2: Crea una regla en AWS IoT Core

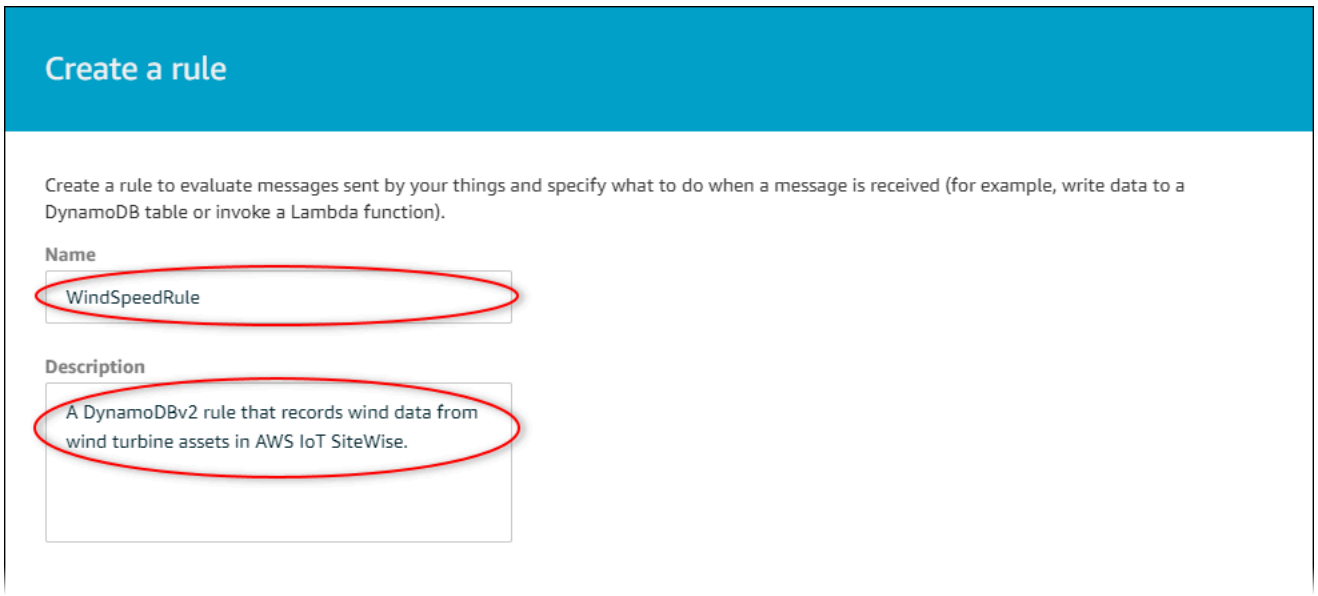
En este procedimiento, se crea una regla en AWS IoT Core que analiza los mensajes de notificación del valor de la propiedad e inserta los datos en una tabla de Amazon DynamoDB. AWS IoT Las reglas básicas analizan los mensajes de MQTT y realizan acciones en función del contenido y el tema de cada mensaje. A continuación, cree una regla con una acción de DynamoDB para insertar datos en una tabla de DynamoDB que cree como parte de este tutorial.

Para crear una regla con una acción de DynamoDB

1. Vaya a la consola de AWS IoT. Si aparece un botón Get started (Empezar), elíjalo.
2. En el panel de navegación izquierdo, elija Act (Acción) y, a continuación, elija Rules (Reglas).



3. Si aparece el cuadro de diálogo You don't have any rules yet (Aún no tiene ninguna regla), elija Create a rule (Crear una regla). De lo contrario, seleccione Crear.
4. Escriba un nombre y una descripción para la regla.



5. Busque el tema de notificación que guardó anteriormente en este tutorial.

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

   Sustituya el ID del activo (el ID que `assets/` aparece después) del tema por un+. Esto selecciona la propiedad de velocidad del viento para todos los activos de turbinas eólicas de demostración. El filtro de temas + acepta todos los nodos de un solo nivel de un tema. El tema debería tener un aspecto similar al del siguiente ejemplo.

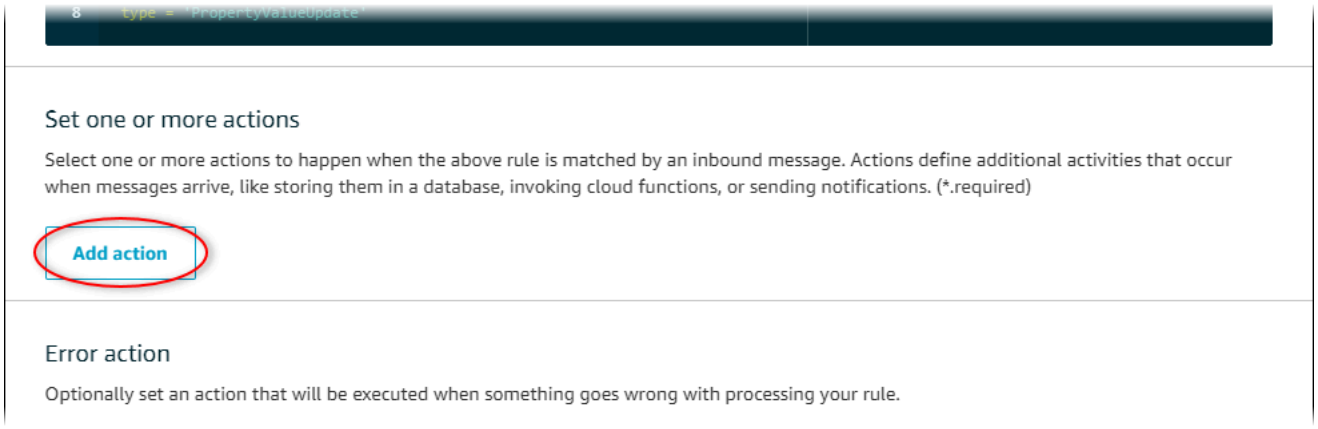
```
$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/assets/+/
properties/a1b2c3d4-5678-90ab-cdef-33333EXAMPLE
```

6. Introduzca la siguiente instrucción de consulta de reglas. Reemplace el tema de la sección `FROM` por el tema de notificación.

```
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. En Set one or more actions (Definir una o varias acciones), elija Add action (Añadir acción).



8. En la página Seleccionar una acción elija Dividir mensaje en varias columnas de una tabla de DynamoDB (DynamoDBv2).

9. Seleccione Configure action (Configurar acción) en la parte inferior de la página.
10. En la página Configure action, seleccione Create a new resource.

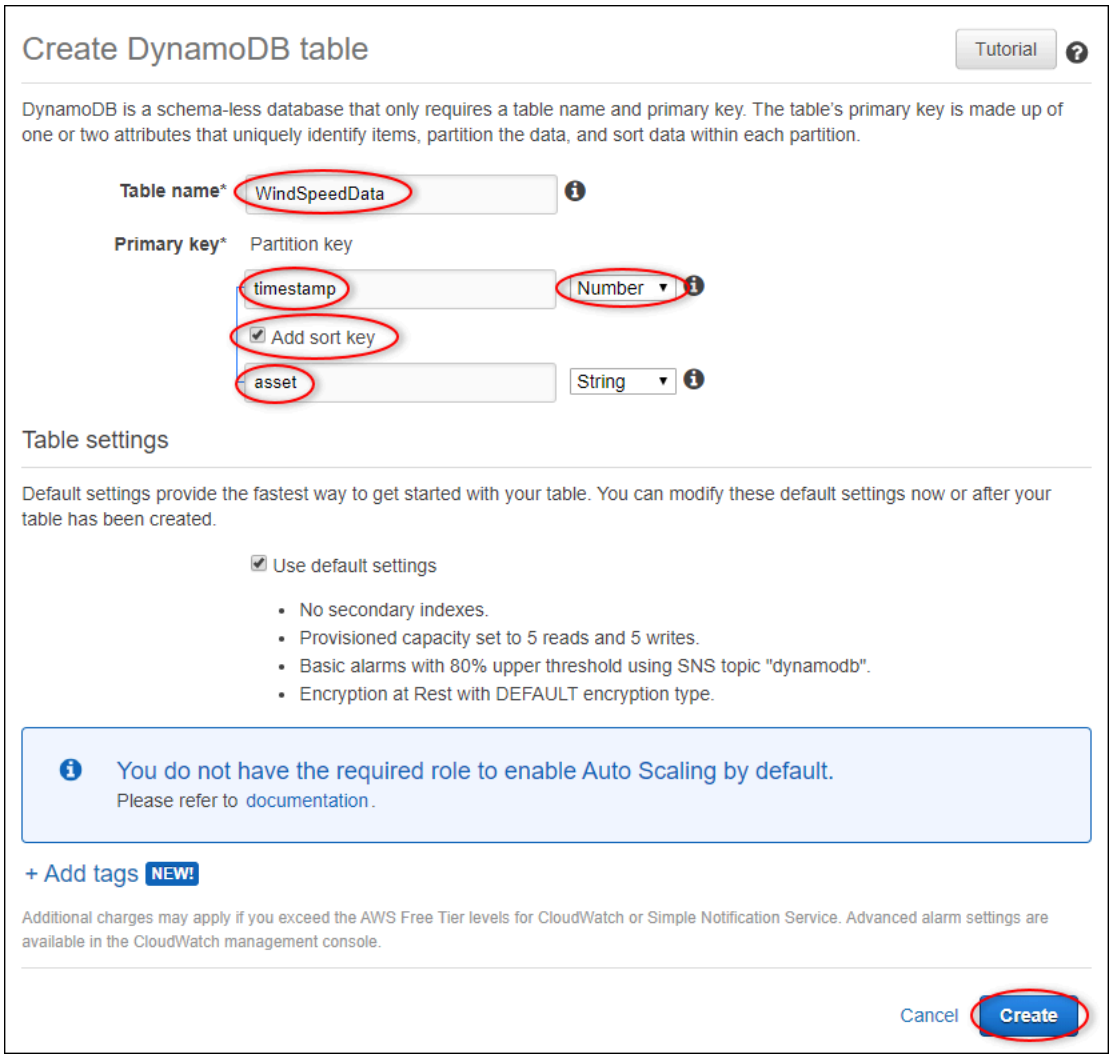
    La consola de DynamoDB se abre en una pestaña nueva. Mantenga abierta la pestaña de acción de regla mientras realiza los siguientes procedimientos.

Paso 3: Crear una tabla de DynamoDB

En este procedimiento, se crea una tabla de Amazon DynamoDB para recibir los datos de velocidad del viento de la acción de la regla.

Para crear una tabla de DynamoDB

1. En el panel de la consola de DynamoDB, elija Crear tabla.
2. Introduzca un nombre para la tabla.



3. En Primary key (Clave principal), haga lo siguiente:
   a. Escriba **`timestamp`** como clave de partición.
   b. Seleccione el tipo Number (Número) .
   c. Marque la casilla Add sort key (Añadir clave de ordenación).
   d. Escriba **`asset`** como clave de ordenación y deje el tipo de clave de ordenación predeterminado de String (Cadena).
4. Seleccione Crear.

   Cuando desaparece el aviso de creación de la tabla la tabla está lista.

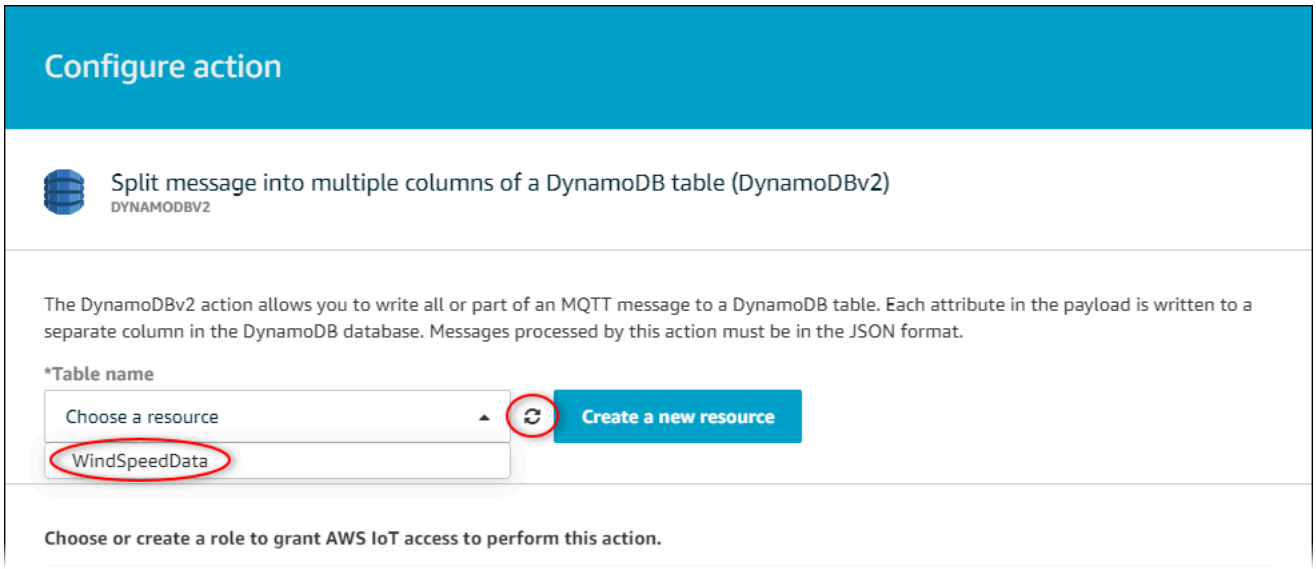
5. Vuelva a la pestaña con la página Configure action (Configurar acción) . Mantenga la pestaña de DynamoDB abierta mientras realiza los siguientes procedimientos.

Paso 4: Configurar la acción de la regla de DynamoDB

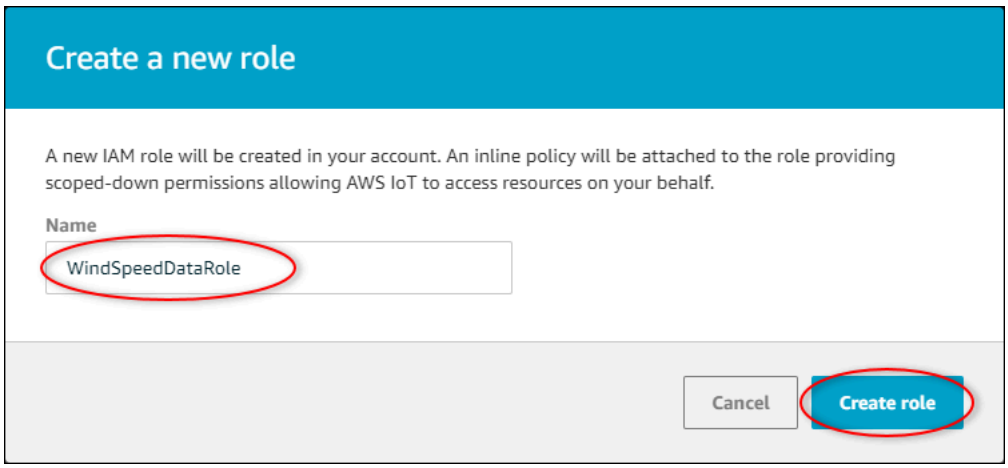
En este procedimiento, configurará la acción de la regla de Amazon DynamoDB para insertar datos de las actualizaciones de valores de propiedades en la nueva tabla de DynamoDB.

Para configurar la acción de regla de DynamoDB

1. En la página Configurar acción, actualice la lista Nombre de la tabla y elija la nueva tabla de DynamoDB.



2. Seleccione Crear rol para crear un rol de IAM que otorgue a AWS IoT Core acceso para realizar la acción de regla.
3. Introduzca un nombre de rol y elija Create Role (Crear rol).



4. Seleccione Agregar acción.
5. Seleccione Create rule (Crear regla) en la parte inferior de la página para terminar de crear la regla.

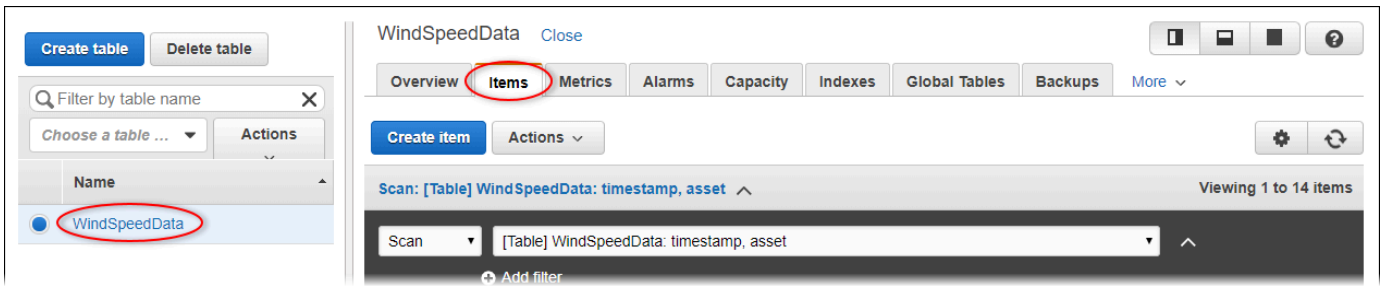
   Los datos de los activos de demostración deberían comenzar a aparecer en la tabla de DynamoDB.

Paso 5: Explore los datos en DynamoDB

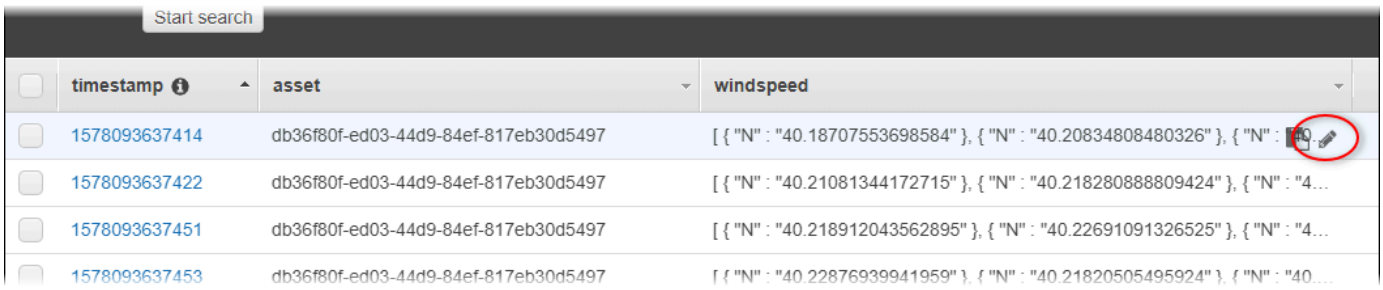
En este procedimiento, explorará los datos de velocidad del viento de los activos de demostración en su nueva tabla de Amazon DynamoDB.

Para explorar datos de activos en DynamoDB.

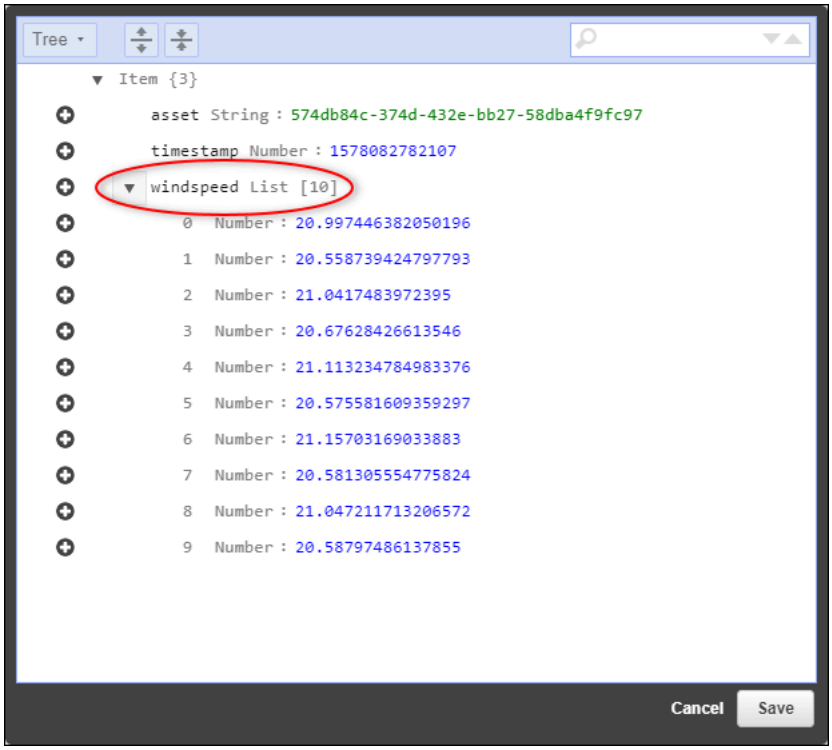
1. Vuelva a la pestaña con la tabla de DynamoDB abierta.
2. En la tabla que creó anteriormente, elija la ficha Items (Elementos) para ver los datos de la tabla. Actualice la página si no ve filas en la tabla. Si las filas no aparecen después de unos minutos, consulte Solución de problemas de las reglas.



3. En una fila de la tabla, elija el icono de edición para expandir los datos.



4. Seleccione la flecha situada junto a la estructura de windspeed para ampliar la lista de puntos de datos de velocidad del viento. Cada lista refleja un lote de puntos de datos de velocidad del viento enviados AWS IoT SiteWise por la demostración del parque eólico. Es posible que desee un formato de datos diferente si configura una acción de regla para su propio uso. Para obtener más información, consulte Consulta de mensajes de notificación sobre propiedades de los activos.



Ahora que ha completado el tutorial, desactive o elimine la regla y elimine la tabla de DynamoDB para evitar incurrir en cargos adicionales. Para limpiar sus recursos, consulte. Paso 6: Limpiar los recursos después del tutorial

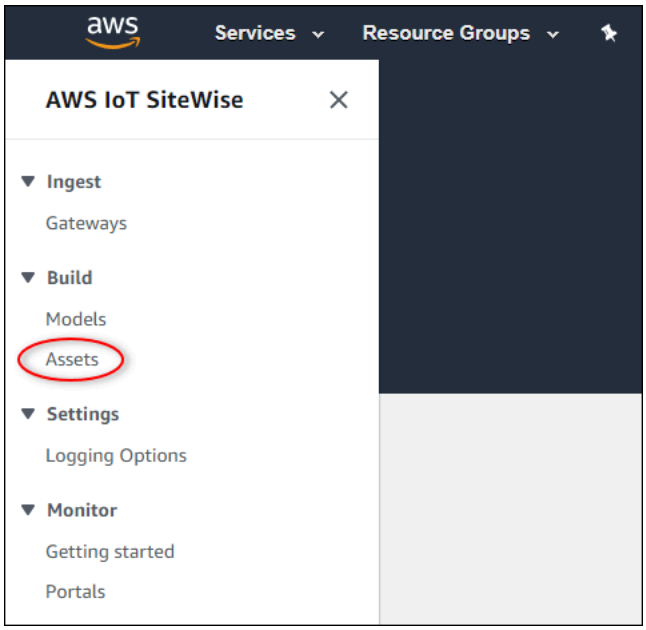
Paso 6: Limpiar los recursos después del tutorial

Después de completar el tutorial, limpie los recursos para evitar incurrir en cargos adicionales. Los activos de su parque eólico de demostración se eliminan al final del período que eligió al crear la demostración. También puede eliminar la demostración manualmente. Para obtener más información, consulte Eliminar la AWS IoT SiteWise demostración.

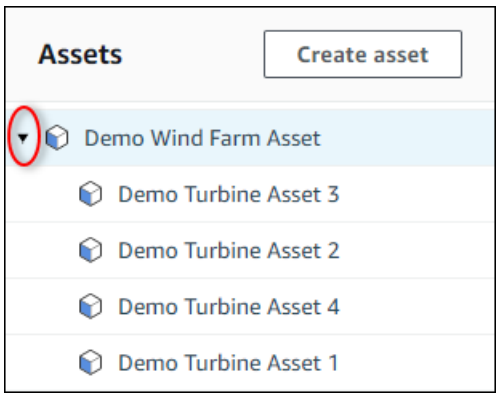
Utilice los siguientes procedimientos para deshabilitar las notificaciones de actualización del valor de las propiedades (si no ha eliminado la demostración), deshabilitar o eliminar la AWS IoT regla y eliminar la tabla de DynamoDB.

Para deshabilitar las notificaciones de actualización de valores de propiedad en propiedades de activos

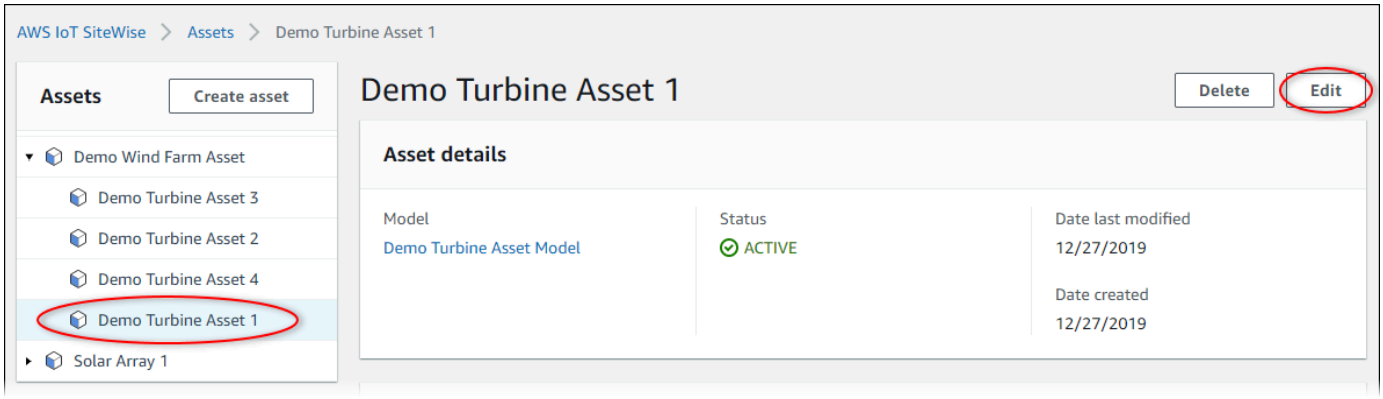
1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación izquierdo, elija Assets (activos).



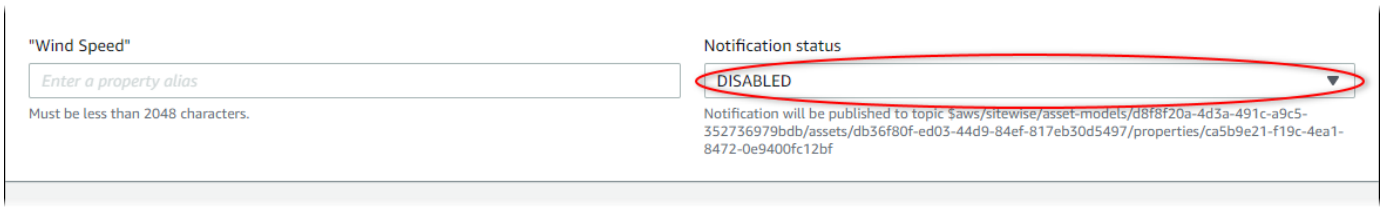
3. Elija la flecha situada junto a Demo Wind Farm Asset para ampliar la jerarquía del activo del parque eólico.



4. Elija una turbina de demostración y elija Edit (Editar).



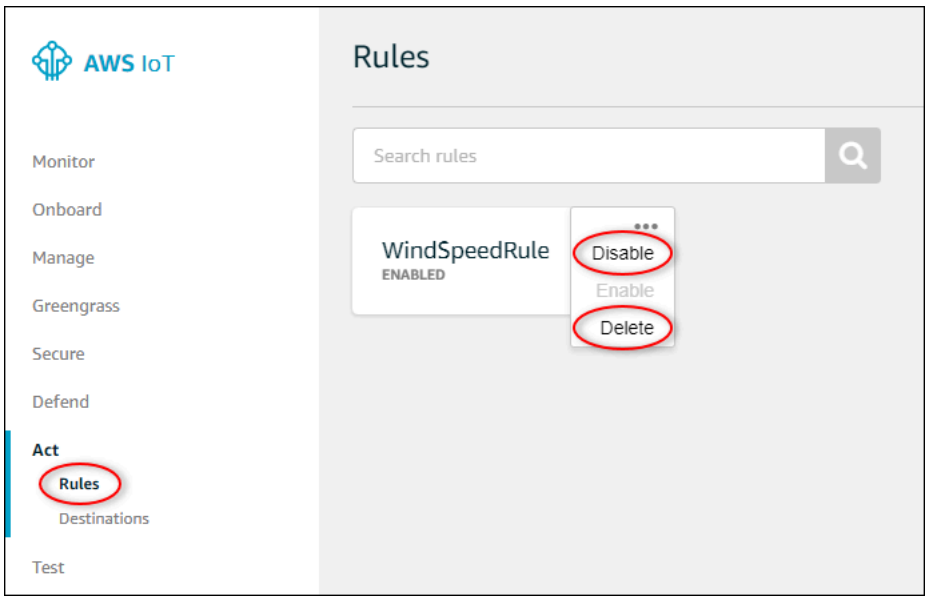
5. Actualice el Estado de notificación de la propiedad Wind Speed a DESHABILITADO.



6. Elija Save asset (Guardar activo) en la parte inferior de la página.
7. Repita los pasos 4 a 6 para cada activo de turbina de demostración.

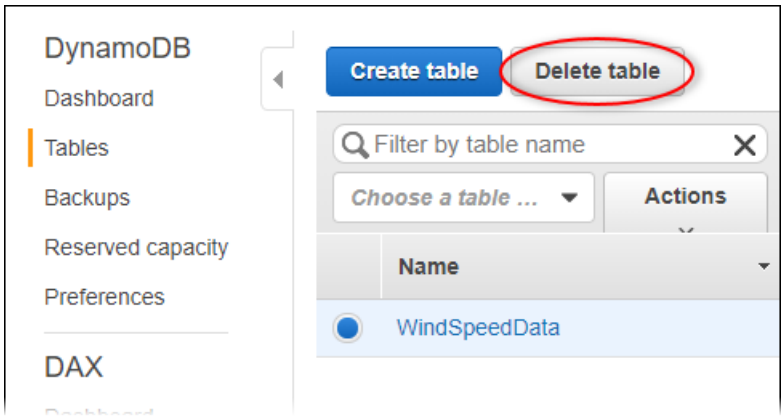
Para deshabilitar o eliminar una regla en AWS IoT Core

1. Vaya a la consola de AWS IoT.
2. En el panel de navegación izquierdo, elija Act (Acción) y, a continuación, elija Rules (Reglas).
3. Elija el menú de su regla y elija Disable (Desactivar) o Delete (Eliminar).

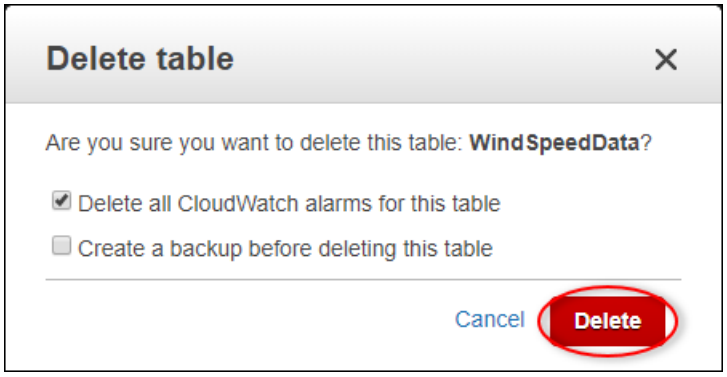


Para eliminar una tabla de DynamoDB

1. Navegue hasta la consola de DynamoDB.
2. En el panel de navegación izquierdo, elija Tables (Tablas).
3. Elija la tabla que creó anteriormente, WindSpeedData.
4. Elija Delete table (Eliminar tabla).



5. En el cuadro de diálogo Delete table (Eliminar tabla), elija Delete (Eliminar).


Delete table
Are you sure you want to delete this table: WindSpeedData?
Delete all CloudWatch alarms for this table
Create a backup before deleting this table
Cancel
Delete

Ingerir datos para AWS IoT SiteWise

AWS IoT SiteWise está diseñado para recopilar y correlacionar de manera eficiente los datos industriales con los activos correspondientes, que representan varios aspectos de las operaciones industriales. Esta documentación se centra en los aspectos prácticos de la ingesta de datos y ofrece varios métodos adaptados a diversos casos de uso industrial. AWS IoT SiteWise Para obtener instrucciones sobre cómo crear su operación industrial virtual, consulte Crear modelos de activos industriales.

Puede enviar datos industriales a AWS IoT SiteWise través de cualquiera de las siguientes opciones:

- AWS IoT SiteWise Edge: utilice la puerta de enlace SiteWise Edge como intermediario entre AWS IoT SiteWise y sus servidores de datos. AWS IoT SiteWise proporciona AWS IoT Greengrass componentes que puede implementar en cualquier plataforma que se pueda ejecutar AWS IoT Greengrass para configurar una puerta de enlace SiteWise Edge. Esta opción admite la vinculación con el protocolo de servidor OPC-UA.
- AWS IoT Reglas básicas: utilice las reglas AWS IoT básicas para cargar datos de los mensajes MQTT publicados por una AWS IoT cosa u otro servicio. AWS
- AWS IoT Events acciones: utilice AWS IoT Events acciones activadas por eventos específicos en. AWS IoT Events Este método es adecuado para situaciones en las que la carga de datos está vinculada a la aparición de eventos.
- AWS IoT Greengrass administrador de flujos: utilice el administrador de AWS IoT Greengrass flujos para cargar datos desde fuentes de datos locales mediante un dispositivo periférico. Esta opción se adapta a situaciones en las que los datos se originan en ubicaciones locales o periféricas.
- AWS IoT SiteWise API: utilice la AWS IoT SiteWise API para cargar datos desde cualquier otra fuente. Utilice nuestra BatchPutAssetPropertyValueAPI de streaming para la ingesta en cuestión de segundos, o la CreateBulkImportJobAPI orientada a lotes para facilitar la ingesta rentable en lotes más grandes.

Estos métodos ofrecen una gama de soluciones para gestionar datos de diferentes fuentes. Profundice en los detalles de cada opción para obtener una comprensión completa de las capacidades AWS IoT SiteWise de ingesta de datos que ofrecen.

Administración de flujos de datos

Antes de sumergirse en la creación de modelos y activos AWS IoT SiteWise, comience por configurar sus fuentes de datos para enviar información directamente desde su equipo industrial a la plataforma. AWS IoT SiteWise está diseñado para generar automáticamente flujos de datos que recopilan sus datos sin procesar. Cada uno de los flujos de datos se identifica con un alias único, lo que facilita el seguimiento del origen de cada dato.

Por ejemplo, pensemos en un parque eólico que utiliza una pasarela AWS IoT SiteWise Edge para enviar datos sobre la temperatura del aire, la velocidad de rotación de la hélice y los datos de series temporales de la potencia de salida desde un servidor OPC-UA a. AWS IoT SiteWise El alias del flujo de `server1-windfarm/3/turbine/7/temperature` datos identifica los valores de temperatura procedentes de la turbina #7 del parque eólico #3. `server1`es el nombre de la fuente de datos del OPC-UA. El `server1` prefijo se utiliza para todos los flujos de datos procedentes de este servidor, lo que ayuda a organizar los datos según su origen.

Tras crear los modelos de activos y los activos, organice la afluencia de datos asociando cada flujo de datos a propiedades específicas de los activos. Esta asociación AWS IoT SiteWise permite no solo recopilar, sino también procesar los datos de acuerdo con la estructura de sus activos. Si es necesario, también puede eliminar el vínculo entre los flujos de datos y las propiedades de los activos.

Actualmente, solo puede asociar flujos de datos con mediciones. Las Mediciones son un tipo de propiedad de activo que representan flujos de datos de sensores sin procesar de los dispositivos, como valores de temperatura con marca de tiempo o valores de revoluciones por minuto (RPM) con marca de tiempo.

Cuando estas mediciones definen métricas o transformaciones, los datos entrantes activan cálculos específicos. Es importante tener en cuenta que una propiedad de un activo solo se puede vincular a un flujo de datos a la vez.

> **Note**
>
> Una propiedad de activo no se puede asociar a varios flujos de datos al mismo tiempo.

AWS IoT SiteWise utiliza `TimeSeries` el recurso Amazon Resource Name (ARN) para determinar los cargos de almacenamiento. Para obtener más información, consulte AWS IoT SiteWise Precios.

En las siguientes secciones, se muestra cómo utilizar la AWS IoT SiteWise consola o la API para gestionar los flujos de datos.

Temas

Administrar secuencias de datos

Para empezar a administrar flujos de datos, complete lo siguiente.

> **Note**
>
> Si es la primera vez que lo has AWS IoT SiteWise hecho después del 24 de noviembre de 2021, puedes saltarte esta sección. Los clientes que hayan empezado a usarlo AWS IoT SiteWise antes de esta fecha deben configurar los ajustes del servicio AWS IoT SiteWise para permitir la ingesta de datos sin necesidad de modelos ni activos.

- Asegúrese de que su rol de IAM tenga los permisos que se muestran en el siguiente ejemplo.

  Example Política de usuario de 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**
>
> Antes de ingerir datos a un flujo de datos, realice lo siguiente.
>
> - El recurso `time-series` debe estar autorizado si utiliza un alias de propiedad para identificar el flujo de datos.
> - El activo `asset` debe estar autorizado si utiliza un ID de activo para identificar el activo que contiene la propiedad de activo asociada.

Para obtener más información sobre configuración de las políticas de IAM, consulte Administración de las políticas de IAM en la Guía del usuario de IAM.

- Configure los ajustes de ingesta de datos AWS IoT SiteWise para permitir la aceptación de flujos de datos que no estén asociados a las propiedades de los activos.

Temas

Configurar los ajustes de ingesta de datos

Console

AWS IoT SiteWise Configúrelo para aceptar flujos de datos no asociados a las propiedades de los activos mediante la AWS IoT SiteWise consola.

Para configurar los ajustes de ingesta de datos (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, en Configuración, seleccione Ingesta de datos.
3. En la página Ingesta de datos, seleccione Editar.
4. En la sección Ingesta de datos disociados, seleccione Habilitar ingesta de datos para flujos de datos no asociados a propiedades de activo.

> **Important**
>
> Después de configurarlo AWS IoT SiteWise para aceptar flujos de datos no asociados a las propiedades de los activos, no podrá desactivar esta configuración.

5. Seleccione Guardar.
6. En Habilitar ingesta de datos disociados, seleccione Actualizar. El estado de Ingesta de datos disociados pasa a ser Activo. Este proceso puede tardar unos minutos en completarse.

AWS CLI

AWS IoT SiteWise Configúrelo para aceptar flujos de datos no asociados a las propiedades de los activos mediante la operación de PutStorageConfigurationAPI. En la siguiente sección se utiliza la AWS CLI.

Para configuración los ajustes de ingesta de datos (AWS CLI)

1. AWS IoT SiteWise Para configurar la recepción de flujos de datos no asociados a las propiedades de los activos, ejecute el siguiente comando.

> **Important**
>
> Después de configurarlo AWS IoT SiteWise para aceptar flujos de datos no asociados a las propiedades de los activos, no podrá desactivar esta configuración.

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

Puede configurar el `storageType` como `MULTI_LAYER_STORAGE`. Para obtener más información, consulte Administrar el almacenamiento de datos.

Example Respuesta

```
{
            "storageType": "SITEWISE_DEFAULT_STORAGE",
            "disassociatedDataStorage": "ENABLED",
```

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

Este proceso puede tardar unos minutos en completarse.

2. Para recuperar la información de configuración del almacenamiento, ejecute el siguiente comando.

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

Example respuesta

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

Administración de flujos de datos

Administre sus flujos de datos mediante la Consola de AWS IoT SiteWise tecla o AWS CLI.

Console

Utilice la AWS IoT SiteWise consola para gestionar sus flujos de datos.

Para administrar flujos de datos (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, seleccione Flujos de datos.
3. (Opcional) Para añadir o actualizar etiquetas, seleccione el flujo de datos que desea editar y, a continuación, seleccione Administrar etiquetas.

   En la página Editar etiquetas, seleccione Añadir etiqueta. En el campo Clave, introduzca el nombre de la etiqueta que va a utilizar.

Seleccione Guardar.

4. (Opcional) En la tabla Flujo de datos puede filtrar los flujos de datos de las siguientes maneras.

   - En el primer menú desplegable, seleccione Prefijo de alias o ID de activo.
     - Prefijo de alias: el prefijo del alias del flujo de datos. Puede elegir esta opción si sus flujos de datos de destino tienen un prefijo de alias.
     - ID de activo: el identificador del activo en el que se creó la propiedad de activo. Puede elegir esta opción si sus flujos de datos de destino están asociados a una propiedad de activo.
   - En el segundo menú desplegable, seleccione Todos los flujos de datos, Flujos de datos asociados, o Flujos de datos disociados.
     - Todos los flujos de datos: flujos de datos asociados o no a una propiedad de activo.
     - Flujos de datos asociados: flujos de datos asociados a una propiedad de activo.
     - Flujos de datos disociados: flujos de datos que no están asociados a una propiedad de activo.
5. Seleccione los flujos de datos que está gestionando. AWS IoT SiteWise muestra los flujos de datos que ha elegido en un gráfico en la parte inferior de la página. Si selecciona más de 10, el gráfico mostrará solo los 10 primeros.
6. (Opcional) Configure el gráfico de las siguientes maneras.

   a. En Función de agregación, seleccione una de las siguientes.

      - Recuento de puntos de datos: el número total de puntos de datos para las variables dadas en el intervalo de tiempo actual.
      - Promedio: la media de los valores de las variables dadas en el intervalo de tiempo actual.
      - Suma: la suma de los valores de las variables dadas en el intervalo de tiempo actual.
      - Mínimo: el mínimo de los valores de las variables dadas en el intervalo de tiempo actual.
      - Máximo: el máximo de los valores de las variables dadas en el intervalo de tiempo actual.

Para obtener más información, consulte Uso de funciones de agregación en expresiones de fórmulas.

b. En Intervalos de tiempo, seleccione uno de los siguientes.

- Última 1 hora: el gráfico muestra los datos agregados de la última hora.
- Últimas 2 horas: el gráfico muestra los datos agregados de las dos últimas horas.
- Últimas 3 horas: el gráfico muestra los datos agregados de las últimas tres horas.
- Últimas 4 horas: el gráfico muestra los datos agregados de las últimas cuatro horas.

c. En Intervalo de tiempo, seleccione uno de los siguientes.

- 1 minuto: añade datos cada minuto en el intervalo de tiempo especificado.
- 1 hora: añade datos cada hora en el intervalo de tiempo especificado.

7. Seleccione Administrar flujos de datos.
8. En la sección Actualizar asociaciones de flujos de datos, en la columna Nombre de la medición, realice una de las siguientes acciones.
   - Si el flujo de datos está asociado a una medición, elimine la asociación eligiendo el icono de cierre.
   - Si el flujo de datos no está asociado a una medición, seleccione Elegir medición.
9. En la tabla Elegir una medición, navegue hasta el activo de destino y, a continuación, seleccione la medición que va a asociar.
10. (Opcional) En la sección Actualizar alias de propiedades de activo, introduzca un alias único para cada medición.
11. Seleccione Actualizar.

La columna Estado puede mostrar uno de los siguientes valores.

- Pendiente: está actualizando la asociación de flujo de datos o el alias de propiedad de activo.
- Envío: su cambio en la asociación o alias de propiedad de activo se ha guardado.
- Error: no se AWS IoT SiteWise pudo procesar la solicitud de actualización de la asociación del flujo de datos o el alias de la medición.
- Éxito: ha actualizado correctamente la asociación del flujo de datos o el alias de la medición.

AWS CLI

Utilice las siguientes operaciones de API para gestionar sus flujos de datos. En los ejemplos de código se utiliza la AWS CLI.

- AssociateTimeSeriesToAssetProperty— Asocia un flujo de datos (series temporales) a una propiedad de activo.
- DisassociateTimeSeriesFromAssetProperty— Disocia un flujo de datos de una propiedad de un activo.
- DeleteTimeSeries— Elimina un flujo de datos.
- DescribeTimeSeries— Recupera información sobre un flujo de datos.
- ListTimeSeries— Recupera una lista paginada de flujos de datos.

AssociateTimeSeriesToAssetProperty

Para asociar un flujo de datos a una propiedad de activo, ejecute el siguiente comando.

> **Important**
>
> La propiedad de activo especificada no debe estar actualmente asociada a ningún flujo de datos.

- *data-stream-alias*Sustitúyalo por el alias del flujo de datos que estás asociando.
- Sustituya *asset-ID* por el ID del activo en el que se creó la propiedad de activo.
- Sustituya *property-ID* por el ID de la propiedad de activo.

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

DisassociateTimeSeriesFromAssetProperty

Para disociar un flujo de datos de una propiedad de activo, ejecute el siguiente comando.

- *data-stream-alias*Sustitúyalo por el alias del flujo de datos que vas a desasociar.

- Sustituya *asset-ID* por el ID del activo en el que se creó la propiedad de activo.
- Sustituya *property-ID* por el ID de la propiedad de activo.

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

DeleteTimeSeries

Para eliminar un flujo de datos, ejecute el siguiente comando.

*data-stream-alias*Sustitúyalo por el alias del flujo de datos que vas a eliminar.

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

Para identificar un flujo de datos, realice una de las siguientes acciones:

- Si el flujo de datos no está asociado a una propiedad de activo, especifique el `alias` del flujo de datos.
- Si el flujo de datos está asociado a una propiedad de activo, especifique una de las siguientes opciones:
  - El `alias` del flujo de datos.
  - El `assetId` y `propertyId` que identifica la propiedad del activo.

DescribeTimeSeries

Utilice la operación de la `DescribeTimeSeries` API para comprobar si ha asociado o desasociado correctamente un flujo de datos.

Para recuperar información acerca de un flujo de datos, ejecute el siguiente comando.

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

Para identificar un flujo de datos, realice una de las siguientes acciones:

- Si el flujo de datos no está asociado a una propiedad de activo, especifique el `alias` del flujo de datos.

- Si el flujo de datos está asociado a una propiedad de activo, especifique una de las siguientes opciones:
  - El `alias` del flujo de datos.
  - El `assetId` y `propertyId` que identifica la propiedad del activo.

ListTimeSeries

Utilice la operación de `ListTimeSeries` API para comprobar si ha eliminado correctamente un flujo de datos.

Para recuperar una lista paginada de flujos de datos, ejecute el siguiente comando.

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

Ingerir datos mediante reglas AWS IoT Core

Envíe datos AWS IoT SiteWise desde AWS IoT objetos y otros AWS servicios mediante las reglas de AWS IoT Core. Las reglas transforman los mensajes de MQTT y realizan acciones para interactuar con AWS los servicios. La acción de la AWS IoT SiteWise regla reenvía los datos de los mensajes a la BatchPutAssetPropertyValueoperación desde la AWS IoT SiteWise API. Para obtener más información, consulte Reglas y Acción AWS IoT SiteWise en la Guía para desarrolladores de AWS IoT .

Para seguir un tutorial que explica los pasos necesarios para configurar una regla que ingiera datos a través de dispositivos ocultos, consulte. Ingerir datos de cosas AWS IoT

También puedes enviar datos desde AWS IoT SiteWise otros AWS servicios. Para obtener más información, consulte Interacción con otros AWS servicios.

Temas

- Otorgar AWS IoT el acceso requerido
- Configurar la acción de la AWS IoT SiteWise regla
- Reducción de costos con Basic Ingest

Otorgar AWS IoT el acceso requerido

Las funciones de IAM se utilizan para controlar los AWS recursos a los que tiene acceso cada regla. Antes de crear una regla, debe crear una función de IAM con una política que permita a la regla realizar acciones en el recurso requerido AWS . AWS IoT asume esta función al ejecutar una regla.

Si crea la acción de la regla en la AWS IoT consola, puede elegir un activo raíz para crear un rol que tenga acceso a una jerarquía de activos seleccionada. Para obtener más información sobre cómo definir manualmente un rol para una regla, consulte Otorgar AWS IoT el acceso necesario y transferir los permisos de rol en la Guía para AWS IoT desarrolladores.

Para la acción de la AWS IoT SiteWise regla, debe definir una función que permita el `iotsitewise:BatchPutAssetPropertyValue` acceso a las propiedades de los activos a las que la regla envía los datos. Para mejorar la seguridad, puede especificar una ruta jerárquica de AWS IoT SiteWise activos en la `Condition` propiedad.

La siguiente política de confianza de ejemplo permite el acceso a un activo específico y a sus secundarios.

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

Elimine la `Condition` de la política para permitir el acceso a todos sus activos. La política de confianza de ejemplo siguiente permite el acceso a todos los activos de la región actual.

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

Configurar la acción de la AWS IoT SiteWise regla

La acción de la AWS IoT SiteWise regla envía los datos del mensaje MQTT que inició la regla a las propiedades de los activos. AWS IoT SiteWise Puede cargar varias entradas de datos en diferentes propiedades de activos al mismo tiempo para enviar actualizaciones de todos los sensores de un dispositivo en un solo mensaje. También puede cargar varios puntos de datos a la vez para cada entrada de datos.

> **Note**
>
> Al enviar datos AWS IoT SiteWise con la acción de la regla, estos deben cumplir todos los requisitos de la `BatchPutAssetPropertyValue` operación. Por ejemplo, los datos no pueden tener una marca temporal anterior a 7 días a partir de la hora actual en formato Unix. Para obtener más información, consulte Ingesta de datos con la API AWS IoT SiteWise.

Para cada entrada de datos de la acción de regla, se identifica una propiedad de activo y se especifica la marca temporal, la calidad y el valor de cada punto de datos para esa propiedad de activo. La acción de regla espera cadenas para todos los parámetros.

Para identificar una propiedad de activo en una entrada, puede especificar uno de los elementos siguientes:

- El Asset ID (ID de activo) (`assetId`) y Property ID (ID de propiedad) (`propertyId`) de la propiedad del activo al que está enviando los datos. Para encontrar el identificador del activo y el identificador de la propiedad, utilice el Consola de AWS IoT SiteWise. Si conoce el identificador del activo, puede utilizar el AWS CLI para llamar y DescribeAssetbuscar el identificador de la propiedad.

- El Property alias (Alias de propiedad) (`propertyAlias`), que es un alias de flujo de datos (por ejemplo, `/company/windfarm/3/turbine/7/temperature`). Para utilizar esta opción, primero debe establecer el alias de la propiedad del activo. Para aprender a configurar los alias de las propiedades, consulte Asignación de flujos de datos industriales a propiedades de activos.

Para la marca de tiempo de cada entrada, usa la marca de tiempo indicada por tu equipo o la marca de tiempo proporcionada por. AWS IoT Core La marca temporal tiene dos parámetros:

- Tiempo en segundos (`timeInSeconds`): la hora en formato Unix, en segundos, a la que el sensor o el equipo notificó los datos.
- Desfase en nanosegundos (`offsetInNanos`): (opcional) el desfase en nanosegundos respecto al tiempo en segundos.

Important

Si la marca temporal es una cadena, tiene una parte decimal o no está en segundos, AWS IoT SiteWise rechaza la solicitud. Debe convertir la marca temporal en segundos y el desfase en nanosegundos. Usa las funciones del motor de AWS IoT reglas para convertir la marca de tiempo. Para más información, consulte los siguientes temas:

- Obtener marcas temporales para dispositivos que no indican la hora exacta
- Convertir las marcas temporales que están en formato de cadena

Puede utilizar plantillas de sustitución para varios parámetros para realizar cálculos, invocar funciones y extraer valores de la carga útil del mensaje. Para obtener más información, consulte Plantillas de sustitución en la Guía para desarrolladores de AWS IoT .

Note

Dado que una expresión de una plantilla de sustitución se evalúa por separado de la instrucción `SELECT`, no se puede utilizar una plantilla de sustitución para hacer referencia a un alias creado mediante una cláusula `AS`. Solo puede hacer referencia a la información presente en la carga original, además de a las funciones y operadores compatibles.

Temas

- Obtener marcas temporales para dispositivos que no indican la hora exacta
- Convertir las marcas temporales que están en formato de cadena
- Convertir cadenas de marcas temporales con una precisión de nanosegundos
- Ejemplo de configuraciones de regla
- Solución de problemas de la acción de regla de

Obtener marcas temporales para dispositivos que no indican la hora exacta

Si su sensor o equipo no proporciona datos de tiempo precisos, obtenga la época actual de Unix desde el motor de AWS IoT reglas con timestamp (). Esta función muestra la hora en milisegundos, por lo que debe convertir el valor a tiempo en segundos y desfase en nanosegundos. Para ello, utilice las siguientes conversiones:

- En Time in seconds (Hora en segundos) (`timeInSeconds`), utilice **`${floor(timestamp() / 1E3)}`** para convertir la hora de milisegundos a segundos.
- En Offset in nanos (Desfase en nanosegundos) (`offsetInNanos`), utilice **`${(timestamp() % 1E3) * 1E6}`** para calcular el desfase en nanosegundos de la marca temporal.

Convertir las marcas temporales que están en formato de cadena

Si su sensor o equipo informa los datos de tiempo en formato de cadena (por ejemplo,`2020-03-03T14:57:14.699Z`), utilice time_to_epoch (String, String). Esta función introduce la marca temporal y el patrón de formato como parámetros y genera el tiempo en milisegundos. A continuación, debe convertir el tiempo en tiempo en segundos y el desfase en nanosegundos. Para ello, utilice las siguientes conversiones:

- En Hora en segundos (`timeInSeconds`), utilice **`${floor(time_to_epoch("2020-03-03T14:57:14.699Z", "yyyy-MM-dd'T'HH:mm:ss'Z'") / 1E3)}`** para convertir la cadena de marca temporal a milisegundos, y luego a segundos.
- En Desfase en nanosegundos (`offsetInNanos`), utilice **`${(time_to_epoch("2020-03-03T14:57:14.699Z", "yyyy-MM-dd'T'HH:mm:ss'Z'") % 1E3) * 1E6}`** para calcular el desfase en nanosegundos de la cadena de la marca temporal.

> **Note**
>
> La función `time_to_epoch` admite cadenas de marcas temporales con una precisión de hasta milisegundos. Para convertir cadenas con una precisión de microsegundos o nanosegundos, configure una AWS Lambda función que la regla invoque para convertir la marca de tiempo en valores numéricos. Para obtener más información, consulte Convertir cadenas de marcas temporales con una precisión de nanosegundos.

Convertir cadenas de marcas temporales con una precisión de nanosegundos

Si su dispositivo envía información de marca temporal en formato de cadena (por ejemplo, `2020-03-03T14:57:14.699728491Z`), siga este procedimiento para configurar su acción de la regla. Puedes crear una AWS Lambda función que convierta la marca temporal de una cadena en Tiempo en segundos (**`timeInSeconds`**) y Offset en nanos (). `offsetInNanos` A continuación, utilice aws_lambda (FunctionArn, InputJson) en los parámetros de acción de la regla para invocar esa función de Lambda y utilizar el resultado en la regla.

> **Note**
>
> En esta sección se incluyen instrucciones avanzadas que suponen que está familiarizado con la forma de crear estos recursos:
>
> - Funciones de Lambda. Para obtener más información, consulte este artículo acerca de Cómo crear una función de Lambda con la consola o Cómo usar Lambda con la AWS CLI en la Guía para desarrolladores de AWS Lambda .
> - AWS IoT gobierna con la acción de la regla. AWS IoT SiteWise Para obtener más información, consulte Ingerir datos mediante reglas AWS IoT Core.

Para crear una acción de AWS IoT SiteWise regla que analice cadenas de marcas de tiempo

1. Cree una función de Lambda con las siguientes propiedades:

   - Nombre de la función: utilice un nombre de función descriptivo (por ejemplo, **`ConvertNanosecondTimestampFromString`**).
   - Tiempo de ejecución: utilice un entorno de ejecución de Python 3, como Python 3.11 (`python3.11`).

- Permisos: cree un rol con permisos Lambda básicos () AWS LambdaBasicExecutionRole.
- Capas: añada la capa AWS sdkPandas-python311 para que la utilice la función Lambda. numpy
- Código de función: utilice el siguiente código de función, que consume un argumento de cadena denominado `timestamp` y las salidas `timeInSeconds` y `offsetInNanos` los valores de esa marca temporal.

```
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
    }
```

Esta función Lambda introduce cadenas de marcas de tiempo en formato ISO 8601 mediante datetime64 from. NumPy

> **Note**
>
> Si las cadenas de marca temporal no están en formato ISO 8601, puede implementar una solución con pandas que defina el formato de la marca temporal. Para obtener más información, consulte pandas.to_datetime..

2. Al configurar la AWS IoT SiteWise acción de la regla, utilice las siguientes plantillas de sustitución para Time in seconds (**`timeInSeconds`**) y Offset in nanos (). `offsetInNanos` Estas plantillas de sustitución suponen que su carga de mensaje contiene la cadena de marca temporal en `timestamp`. La función `aws_lambda` consume una estructura JSON para su

segundo parámetro, por lo que puede modificar las siguientes plantillas de sustitución en caso necesario.

- En Time in seconds (Tiempo en segundos) (`timeInSeconds`), use la siguiente plantilla de sustitución.

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

- En Offset in nanos (Desfase en nanosegundos) (`offsetInNanos`), use la siguiente plantilla de sustitución.

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

Para cada parámetro, sustituye *la región* y el identificador de *cuenta por tu región e AWS identificador* de cuenta. Si ha usado otro nombre para su función de Lambda, cámbielo también.

3. Concede AWS IoT permisos para invocar tu función con el permiso. `lambda:InvokeFunction` Para obtener más información, consulte aws_lambda(functionArn, inputJson).
4. Pruebe la regla (por ejemplo, utilice el cliente de prueba AWS IoT MQTT) y compruebe que AWS IoT SiteWise recibe los datos que envía.

   Si su regla no funciona según lo previsto, consulte Solución de problemas y acción de AWS IoT SiteWise regla.

> **Note**
>
> Esta solución invoca la función de Lambda dos veces para cada cadena de marca temporal. Puede crear otra regla para reducir el número de invocaciones de funciones de Lambda si su regla gestiona varios puntos de datos que tienen la misma marca temporal en cada carga. Para ello, cree una regla con una acción de volver a publicar que invoca Lambda y publica la carga original con la cadena de marca temporal convertida en `timeInSeconds` y `offsetInNanos`. A continuación, cree una regla con una acción de AWS IoT SiteWise regla para consumir la carga útil convertida. Con este enfoque, se reduce el número de veces que

la regla invoca la Lambda, pero se aumenta el número de acciones AWS IoT de la regla que se ejecutan. Considere los precios de cada servicio si aplica esta solución a su caso de uso.

Ejemplo de configuraciones de regla

Esta sección contiene ejemplos de configuraciones de reglas para crear una regla con una AWS IoT SiteWise acción.

Example Acción de regla de ejemplo que utiliza alias de propiedad como temas de mensaje

En el siguiente ejemplo, se crea una regla con una AWS IoT SiteWise acción que utiliza el tema (a través del tema ()) como alias de la propiedad para identificar las propiedades de los activos. Utilice este ejemplo para definir una regla para transferir datos de tipo doble a todas las turbinas eólicas de todos los parques eólicos. Este ejemplo requiere que defina alias de propiedad en todas las propiedades de los activos de la turbina. Necesitaría definir una segunda regla similar para ingerir datos de tipo entero.

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

La carga de ejemplo en `sitewise-rule-payload.json` contiene el siguiente contenido.

```
{
  "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 esta acción de regla, envíe el siguiente mensaje a un alias de propiedad de una turbina eólica (por ejemplo,`/company/windfarm/3/turbine/7/temperature`) como tema para ingerir datos.

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

Example Ejemplo de acción de regla que utiliza timestamp() para determinar la hora

En el siguiente ejemplo, se crea una regla con una AWS IoT SiteWise acción que identifica una propiedad de activo mediante sus identificadores y utiliza timestamp () para determinar la hora actual.

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

La carga de ejemplo en `sitewise-rule-payload.json` contiene el siguiente contenido.

```
{
  "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 esta acción de regla, envía el siguiente mensaje a la para que ingiera `my/asset/property/topic` los datos.

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

Solución de problemas de la acción de regla de

Para solucionar la acción de la AWS IoT SiteWise regla AWS IoT Core, configura CloudWatch los registros o configura una acción de error al volver a publicar la regla. Para obtener más información, consulte Solución de problemas y acción de AWS IoT SiteWise regla.

Reducción de costos con Basic Ingest

AWS IoT Core proporciona una función denominada ingesta básica que puede utilizar para enviar datos AWS IoT Core sin incurrir AWS IoT en gastos de mensajería. Basic Ingest optimiza el flujo de

datos para las cargas de trabajo de ingesta de grandes volúmenes de datos mediante la eliminación del agente de mensajería de publicación y suscripción en la ruta de ingesta. Puede utilizar Basic Ingest si sabe a qué reglas deben dirigirse sus mensajes.

Para utilizar Basic Ingest, se envían mensajes directamente a una regla específica utilizando un tema especial, `$aws/rules/rule-name`. Por ejemplo, para enviar un mensaje a una regla denominada `SiteWiseWindFarmRule`, envíe un mensaje al tema `$aws/rules/SiteWiseWindFarmRule`.

Si la acción de regla utiliza plantillas de sustitución que contengan topic(Decimal), puede transferir el tema original al final del tema especial de Basic Ingest, como `$aws/rules/rule-name/original-topic`. Por ejemplo, para utilizar Basic Ingest con el ejemplo de alias de propiedad del parque eólico de la sección anterior, puede enviar mensajes al tema siguiente.

```
$aws/rules/SiteWiseWindFarmRule//company/windfarm/3/turbine/7/temperature
```

> **Note**
>
> El ejemplo anterior incluye una segunda barra (`//`) porque AWS IoT elimina el prefijo de ingesta básica (`$aws/rules/rule-name/`) del tema que está visible para la acción de la regla. En este ejemplo, la regla recibe el tema `/company/windfarm/3/turbine/7/temperature`.

Para obtener más información, consulte Reducción de los costos de mensajería con Basic Ingest en la Guía para desarrolladores de AWS IoT .

Ingerir datos de AWS IoT Events

Con AWS IoT Events, puede crear aplicaciones de monitoreo de eventos complejas para su flota de IoT en la AWS nube. Utilice la SiteWise acción de IoT AWS IoT Events para enviar datos a las propiedades de los activos AWS IoT SiteWise cuando se produzca un evento.

AWS IoT Events está diseñado para agilizar el desarrollo de aplicaciones de monitoreo de eventos para dispositivos y sistemas de IoT dentro de la AWS nube. Si lo usa AWS IoT Events, puede:

- Detecte cambios, anomalías o condiciones específicas en toda su flota de IoT y responda a ellos.
- Mejore su eficiencia operativa y habilite la administración proactiva de su ecosistema de IoT.

Al integrarse a AWS IoT SiteWise través de la AWS IoT SiteWise acción, AWS IoT Events amplía sus capacidades, lo que le permite actualizar automáticamente las propiedades de los activos AWS IoT SiteWise en respuesta a eventos específicos. Esta interacción puede simplificar la ingesta y la administración de datos. También puede proporcionarle información útil.

Para obtener más información, consulte los siguientes temas de la Guía para desarrolladores de AWS IoT Events :

- ¿Qué es? AWS IoT Events
- Acciones de AWS IoT Events
- SiteWise Acción de IoT

Uso del administrador de AWS IoT Greengrass transmisiones

AWS IoT Greengrass El administrador de flujos es una función de integración que facilita la transferencia de flujos de datos de fuentes locales a la AWS nube. Actúa como una capa intermedia que gestiona los flujos de datos, lo que permite a los dispositivos que funcionan en la periferia recopilar y almacenar datos antes de enviarlos AWS IoT SiteWise, para su posterior análisis y procesamiento.

Agregue un destino de datos configurando una fuente local en la AWS IoT SiteWise consola. También puede usar el administrador de transmisiones en su AWS IoT Greengrass solución personalizada para ingerir AWS IoT SiteWise datos.

> **Note**
>
> Para ingerir datos de fuentes OPC-UA, configure una puerta de enlace AWS IoT SiteWise Edge que se ejecute en. AWS IoT Greengrass Para obtener más información, consulte Uso de puertas de enlace SiteWise Edge.

Para obtener más información sobre cómo configurar un destino para los datos de origen local, consulte. Configuración de orígenes de datos

Para obtener más información sobre cómo ingerir datos mediante el administrador de transmisiones en una AWS IoT Greengrass solución personalizada, consulte los siguientes temas de la Guía para AWS IoT Greengrass Version 2 desarrolladores:

- ¿Qué es? AWS IoT Greengrass
- Administrar secuencias de datos en el núcleo de AWS IoT Greengrass
- Exportación de datos a propiedades AWS IoT SiteWise de activos

Ingerir datos mediante la API AWS IoT SiteWise

Utilice la AWS IoT SiteWise API para enviar datos industriales con fecha y hora a las propiedades de medición y atributos de sus activos. La API acepta una carga útil que contiene estructuras (TQV). timestamp-quality-value

Utilice la BatchPutAssetPropertyValueoperación para cargar los datos. Con esta operación, puede cargar varias entradas de datos a la vez para recopilar datos de varios dispositivos y enviarlos todos en una sola solicitud.

> **Important**
>
> La BatchPutAssetPropertyValueoperación está sujeta a las siguientes cuotas:
>
> - Hasta 10 entradas por solicitud.
> - Hasta 10 valores de propiedad (puntos de datos TQV) por entrada.
> - AWS IoT SiteWise rechaza cualquier dato con una marca de tiempo fechada en más de 7 días o más de 10 minutos en el futuro.
>
> Para obtener más información sobre estas cuotas, consulta la referencia BatchPutAssetPropertyValuede la AWS IoT SiteWise API.

Para identificar una propiedad de un activo, especifique una de las siguientes opciones:

- El `assetId` extremo `propertyId` de la propiedad del activo a la que se envían los datos.
- El `propertyAlias`, que es un alias de flujo de datos (por ejemplo, `/company/windfarm/3/turbine/7/temperature`). Para utilizar esta opción, primero debe establecer el alias de la propiedad del activo. Para establecer los alias de las propiedades, consulteAsignación de flujos de datos industriales a propiedades de activos.

El siguiente ejemplo muestra cómo enviar lecturas de temperatura y rotaciones por minuto (RPM) de una turbina eólica desde una carga útil almacenada en un archivo JSON.

```
aws iotsitewise batch-put-asset-property-value --cli-input-json file://batch-put-
payload.json
```

La carga de ejemplo en `batch-put-payload.json` contiene el siguiente contenido.

```
{
  "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"
        }
      ]
    }
  ]
}
```

Cada entrada de la carga contiene un `entryId` que puede definir como una única cadena. Si la entrada de la solicitud no se realiza correctamente, cada error contendrá el `entryId` de la solicitud correspondiente para que sepa qué solicitudes deben volver a intentarse.

Cada estructura de la lista de `propertyValues` es una estructura timestamp-quality-value (TQV) que contiene `a`value, a y, opcionalmente`timestamp`, a. `quality`

- `value`: una estructura que contiene uno de los siguientes campos, en función del tipo de propiedad que se establezca:
  - `booleanValue`
  - `doubleValue`
  - `integerValue`
  - `stringValue`
- `timestamp`: una estructura que contiene el tiempo en segundos en formato de tiempo Unix, `timeInSeconds`. También puede establecer la `offsetInNanos` clave en la `timestamp` estructura si dispone de datos precisos en el momento. AWS IoT SiteWise rechaza cualquier punto de datos con marcas de tiempo anteriores a 7 días o posteriores a 10 minutos en el futuro.
- `quality`: (opcional) una de las siguientes cadenas de calidad:
  - `GOOD`: (predeterminado) los datos no se ven afectados por ningún problema.
  - `BAD`: los datos se ven afectados por un problema, como un fallo del sensor.
  - `UNCERTAIN`: los datos se ven afectados por un problema, como la falta de precisión de un sensor.

  Para obtener más información sobre cómo se AWS IoT SiteWise gestiona la calidad de los datos en los cálculos, consulte Calidad de [los datos en las expresiones de](#) fórmulas.

Ingerir datos mediante la API CreateBulkImportJob

Utilice la `CreateBulkImportJob` API para importar grandes cantidades de datos de Amazon S3. Los datos deben guardarse en formato CSV en Amazon S3. Los archivos de datos pueden tener las siguientes columnas.

> **Note**
>
> Para identificar una propiedad de un activo, especifique una de las siguientes opciones.

- La `ASSET_ID` y `PROPERTY_ID` de la propiedad del activo al que va a enviar los datos.
- El `ALIAS`, que es un alias de flujo de datos (por ejemplo, `/company/windfarm/3/turbine/7/temperature`). Para utilizar esta opción, primero debe establecer el alias de la propiedad del activo. Para aprender a configurar los alias de las propiedades, consulte the section called “Asignación de flujos de datos industriales a propiedades de activos”.

- `ALIAS`: el alias que identifica la propiedad, como una ruta de flujo de datos del servidor OPC-UA (por ejemplo, `/company/windfarm/3/turbine/7/temperature`). Para obtener más información, consulte Asignación de flujos de datos industriales a propiedades de activos.
- `ASSET_ID`: el ID del activo.
- `PROPERTY_ID`: el ID de la propiedad del activo.
- `DATA_TYPE`: el tipo de datos de la propiedad puede ser uno de los siguientes.
  - `STRING` – Una cadena con hasta 1024 bytes.
  - `INTEGER`: un entero de 32 bits con signo con rango [-2.147.483.648, 2.147.483.647].
  - `DOUBLE`: un número de punto flotante con rango [-10^100, 10^100] e IEEE 754 doble precisión.
  - `BOOLEAN` – `true` o `false`.
- `TIMESTAMP_SECONDS`: la marca temporal del punto de datos, con la hora en formato Unix.
- `TIMESTAMP_NANO_OFFSET`: el desplazamiento de nanosegundos convertido de `TIMESTAMP_SECONDS`.
- `QUALITY`: (opcional) La calidad del valor de la propiedad del activo. El valor puede ser uno de los siguientes:
  - `GOOD`: (predeterminado) los datos no se ven afectados por ningún problema.
  - `BAD`: los datos se ven afectados por un problema, como un fallo del sensor.
  - `UNCERTAIN`: los datos se ven afectados por un problema, como la falta de precisión de un sensor.

  Para obtener más información sobre cómo se AWS IoT SiteWise gestiona la calidad de los datos en los cálculos, consulte Calidad de los datos en las expresiones de fórmulas.
- `VALUE`: el valor de la propiedad del activo.

Example archivo(s) de datos en 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 proporciona las siguientes operaciones de API para crear un trabajo de importación masiva y obtener información sobre un trabajo existente.

- CreateBulkImportJob— Crea un nuevo trabajo de importación masiva.
- DescribeBulkImportJob— Recupera información sobre un trabajo de importación masiva.
- ListBulkImportJob— Recupera una lista paginada de resúmenes de todos los trabajos de importación masiva.

Crea un trabajo de importación por lotes (AWS CLI)

Utilice la operación de CreateBulkImportJobAPI para transferir datos de Amazon S3 a AWS IoT SiteWise. Utilice la CreateBulkImportJobAPI para ingerir datos en lotes pequeños de forma rentable. El siguiente ejemplo utiliza AWS CLI.

> **Important**
>
> Antes de crear un trabajo de importación masiva, debe habilitar el nivel AWS IoT SiteWise cálido o el nivel AWS IoT SiteWise frío. Para obtener más información, consulte Configurar los ajustes de almacenamiento.

> La importación masiva está diseñada para almacenar datos históricos en AWS IoT SiteWise. No inicia los cálculos ni las notificaciones en el nivel AWS IoT SiteWise cálido o en el nivel AWS IoT SiteWise frío.

Ejecute el siguiente comando de la . Reemplace *file-name* por el nombre del archivo que contiene la configuración del trabajo de importación por lotes.

```
aws iotsitewise create-bulk-import-job --cli-input-json file://file-name.json
```

Example Configuración de trabajos de importación masiva

Los siguientes son ejemplos de opciones de configuración:

- Reemplace *adaptive-ingestion-flag* por `true` o `false`.
  - Si se establece en`false`, el trabajo de importación masiva ingiere datos históricos en AWS IoT SiteWiseél.
  - Si se establece en`true`, el trabajo de importación masiva hace lo siguiente:
    - Ingiere nuevos datos en. AWS IoT SiteWise
    - Calcula las métricas y las transforma, y admite las notificaciones de datos con una marca temporal de siete días.
- Sustituya *delete-files-after-import-flag* por `true` para eliminar los datos del depósito de datos de S3 después de haberlos introducido en un almacenamiento de nivel AWS IoT SiteWise cálido.
- Reemplace *error-bucket* por el nombre del bucket de Amazon S3 al que se envían los errores asociados a este trabajo de importación por lotes.
- *error-bucket-prefix*Sustitúyalo por el prefijo del bucket de Amazon S3 al que se envían los errores asociados a este trabajo de importación masiva.

  Amazon S3 usa el prefijo como nombre de carpeta para organizar los datos del bucket. Cada objeto de Amazon S3 tiene una clave que es su identificador único en el bucket. Cada objeto de un bucket tiene exactamente una clave. El prefijo debe terminar con una barra diagonal: (/). Para obtener más información, consulte Organizar objetos usando prefijos en la Guía para usuarios de Amazon Simple Storage Service.
- Reemplace *data-bucket* por el nombre del bucket de Amazon S3 desde el que se importan los datos.

- *data-bucket-key*Sustitúyala por la clave del objeto de Amazon S3 que contiene los datos. Cada objeto tiene una clave que es un identificador único. Cada objeto tiene exactamente una clave.
- *data-bucket-version-id*Sustitúyalo por el ID de versión para identificar una versión específica del objeto de Amazon S3 que contiene sus datos. Este parámetro es opcional.
- Reemplace *column-name* por el nombre de la columna especificado en el archivo .csv.
- Reemplace *job-name* por un nombre de trabajo único que identifique el trabajo de importación por lotes.
- *job-role-arn*Sustitúyalo por el rol de IAM que AWS IoT SiteWise permite leer los datos de Amazon S3.

> **Note**
>
> Asegúrese de que el rol tenga los permisos que se muestran en el siguiente ejemplo. Sustituya *data-bucket* por el nombre del bucket de Amazon S3 que contiene sus datos. Además, sustituya *error-bucket* por el nombre del bucket de Amazon S3 al que se envían los errores asociados a este trabajo de importación masiva.

```
{
    "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 Respuesta

```
{
   "jobId":"f8c031d0-01d1-4b94-90b1-afe8bb93b7e5",
   "jobStatus":"PENDING",
   "jobName":"myBulkImportJob"
}
```

Describa un trabajo de importación por lotes (AWS CLI)

Utilice la operación DescribeBulkImportJobde API para recuperar información sobre un trabajo de importación masiva. En el siguiente ejemplo se utiliza AWS CLI.

Reemplace *job-ID* por el ID del trabajo de importación por lotes que desea recuperar.

```
aws iotsitewise describe-bulk-import-job --job-id job-ID
```

Example Respuesta

```
{
   "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"
}
```

Enumere los trabajos de importación por lotes (AWS CLI)

Utilice la operación de ListBulkImportJobsAPI para recuperar una lista paginada de resúmenes de todos los trabajos de importación masiva. En el siguiente ejemplo se utiliza. AWS CLI

```
aws iotsitewise list-bulk-import-jobs --filter COMPLETED
```

Example Respuesta

```
{
   "jobSummaries":[
      {
         "id":"bdbbfa52-d775-4952-b816-13ba1c7cb9da",
         "name":"myBulkImportJob",
         "status":"COMPLETED"
      },
      {
         "id":"15ffc641-dbd8-40c6-9983-5cb3b0bc3e6b",
         "name":"myBulkImportJob2",
         "status":"RUNNING"
      }
   ]
}
```

Uso de puertas de enlace SiteWise Edge

Una puerta de enlace AWS IoT SiteWise Edge sirve de intermediario entre su equipo industrial y. AWS IoT SiteWise Se ejecuta la puerta de enlace SiteWise Edge AWS IoT Greengrass V2 que permite la recopilación y el procesamiento de datos en las instalaciones. Puede utilizarla AWS OpsHub AWS IoT SiteWise para administrar sus puertas de enlace SiteWise Edge y monitorear las operaciones in situ.

Puede supervisar los datos de forma local en sus instalaciones mediante los portales SiteWise Monitor de sus dispositivos locales. Para obtener más información, consulte Habilitación del portal en la periferia.

Temas

SiteWise Requisitos de Edge Gateway

AWS IoT SiteWise Las puertas de enlace perimetrales se ejecutan AWS IoT Greengrass V2 como un conjunto de AWS IoT Greengrass componentes que permiten la recopilación, el procesamiento y

la publicación de datos in situ. Para configurar una puerta de enlace SiteWise Edge que se ejecute AWS IoT Greengrass V2, debe crear una puerta de enlace Nube de AWS y ejecutar el software de puerta de enlace SiteWise Edge para configurar su dispositivo local.

Requisitos

Los dispositivos locales deben cumplir los siguientes requisitos para instalar y ejecutar el software de puerta de enlace SiteWise Edge.

- Es compatible con la versión 2.3.0 o posterior del software AWS IoT Greengrass V2 Core. Para obtener más información, consulte Requisitos en la Guía para desarrolladores de AWS IoT Greengrass Version 2 .
- Una de las siguientes plataformas admitidas:
  - Sistema operativo: Ubuntu 20.04 o posterior

    Arquitectura: x86_64 (AMD64) o ARMv8 (Aarch64)
  - OS: Red Hat Enterprise Linux (RHEL) 8

    Arquitectura: x86_64 (AMD64) o ARMv8 (Aarch64)
  - OS: Amazon Linux 2

    Arquitectura: x86_64 (AMD64) o ARMv8 (Aarch64)
  - OS: Debian 11

    Arquitectura: x86_64 (AMD64) o ARMv8 (Aarch64)
  - OS: Windows Server 2019 o posterior

    Arquitectura: x86_64 (AMD64)

> **Note**
>
> Las plataformas ARM solo admiten puertas de enlace SiteWise Edge con el paquete de recopilación de datos. El paquete de procesamiento de datos no es compatible.

- Mínimo 4 GB de RAM.
- Espacio en disco mínimo de 10 GB disponible para el software SiteWise Edge Gateway.
- Si planea procesar datos en la periferia AWS IoT SiteWise, su dispositivo local también debe cumplir los siguientes requisitos:

  - Tener un procesador x86 de 64 bits y cuatro núcleos.
  - Tener al menos 16 GB de RAM.
  - Tiene al menos 32 GB de RAM si utiliza Windows.
  - Tener al menos 256 GB de espacio libre en disco.
- Los requisitos mínimos de espacio en disco y capacidad de procesamiento dependen de una variedad de factores que son exclusivos de la implementación y el caso de uso.
  - El espacio en disco necesario para almacenar en caché los datos para una conectividad a Internet intermitente depende de los siguientes factores:
    - Número de flujos de datos cargados
    - Puntos de datos por flujo de datos por segundo
    - Tamaño de cada punto de datos
    - Velocidades de comunicación
    - Tiempo de inactividad de red esperado
  - La capacidad de cómputo necesaria para sondear y cargar los datos depende de los siguientes factores:
    - Número de flujos de datos cargados
    - Puntos de datos por flujo de datos por segundo
- Configure su dispositivo local para asegurarse de que se pueda acceder a los siguientes puertos:
  - El dispositivo local debe permitir el tráfico entrante de la red en el puerto 443.
  - El dispositivo local debe permitir el tráfico saliente en los puertos 443 y 8883.

    Para obtener una lista completa de los puntos finales de servicio salientes necesarios, consulte Puntos de enlace de servicio necesarios para las puertas de enlace Edge. AWS IoT SiteWise
  - Los siguientes puertos están reservados para su uso por AWS IoT SiteWise: 80, 443, 3001, 4569, 4572, 8000, 8081, 8082, 8084, 8085, 8445, 8086, 9000, 9500, 11080 y 50010. El uso de un puerto reservado para el tráfico puede causar la terminación de la conexión.
- Java Runtime Environment (JRE) versión 11 o superior. Java debe estar disponible en la variable de entorno `PATH` en el dispositivo. Para utilizar Java para desarrollar componentes personalizados, debe instalar un kit de desarrollo de Java (JDK). Le recomendamos que utilice Amazon Corretto u OpenJDK.

Debe tener los siguientes permisos para usar SiteWise las puertas de enlace Edge:

> **Note**
>
> Si usa la AWS IoT SiteWise consola para crear su puerta de enlace SiteWise Edge, estos permisos se añaden automáticamente.

- La función de IAM de su puerta de enlace SiteWise Edge debe permitirle utilizar una puerta de enlace SiteWise Edge en un AWS IoT Greengrass V2 dispositivo para procesar los datos del modelo de activos y los datos de los activos.

  El rol permite que el siguiente servicio asuma el rol: `credentials.iot.amazonaws.com`.

  Detalles de los permisos

  El rol debe tener los siguientes permisos:

  - `iotsitewise`: permite a las entidades principales recuperar datos de modelos de activos y datos de activos en la periferia.
  - `iot`— Permite que sus AWS IoT Greengrass V2 dispositivos interactúen con ellos AWS IoT.
  - `logs`— Permite que tus AWS IoT Greengrass V2 dispositivos envíen registros a Amazon CloudWatch Logs.
  - `s3`— Permite que sus AWS IoT Greengrass V2 dispositivos descarguen artefactos de componentes personalizados de 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": "*"
        }
    ]
}
```

Creación de una puerta de enlace SiteWise Edge

Puede usar la AWS IoT SiteWise consola para crear una puerta de enlace SiteWise Edge. Este procedimiento detalla cómo crear una puerta de enlace SiteWise Edge autohospedada que instalará en su propio hardware. Para obtener información sobre cómo crear una puerta de enlace SiteWise Edge que se ejecute en Siemens Industrial Edge, consulteRunning SiteWise Edge en Siemens Industrial Edge.

Cree una puerta de enlace SiteWise Edge

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija puertas de enlace Edge.
3. Seleccione Crear puerta de enlace.
4. En el tipo de implementación, elija una puerta de enlace autohospedada.
5. Introduzca un nombre para su puerta de enlace SiteWise Edge o utilice el nombre generado por AWS IoT SiteWise.
6. En el sistema operativo del dispositivo Greengrass, selecciona el sistema operativo del dispositivo en el que instalarás esta puerta de enlace SiteWise Edge.

> **Note**
>
> El paquete de procesamiento de datos solo está disponible en plataformas x86.

7. (Opcional) Para procesar y organizar los datos en la periferia, en Capacidades perimetrales, seleccione Paquete de procesamiento de datos.

> **Note**
>
> Para conceder a los grupos de usuarios de su directorio corporativo acceso a esta puerta de enlace SiteWise Edge, consulte Configuración de la capacidad de periferia

8. (Opcional) En la configuración avanzada, haga lo siguiente:

   - En Dispositivo central de Greengrass, elija una de las siguientes opciones:

     - Configuración predeterminada: utiliza AWS automáticamente la configuración predeterminada para crear un dispositivo principal de Greengrass. AWS IoT Greengrass V2

       1. Introduzca un nombre para el dispositivo principal de Greengrass o utilice el nombre generado por. AWS IoT SiteWise

     - Configuración avanzada: elija esta opción si desea utilizar un dispositivo principal de Greengrass existente o crear uno manualmente.

       1. Elija un dispositivo central de Greengrass o elija Crear dispositivo central de Greengrass para crear uno en la consola de AWS IoT Greengrass V2 . Para obtener más información, consulte Configuración de los dispositivos AWS IoT Greengrass V2 principales en la Guía para AWS IoT Greengrass Version 2 desarrolladores.

9. Seleccione Crear puerta de enlace.

10. En el cuadro de diálogo del instalador de la puerta de enlace Generate SiteWise Edge, seleccione Generar y descargar. AWS IoT SiteWise genera automáticamente un instalador que puede usar para configurar su dispositivo local.

> **Important**
>
> Asegúrese de guardar el archivo del instalador en una ubicación segura. Lo utilizará más adelante.

Ahora que ha creado la puerta de enlace SiteWise Edge, añada fuentes de datos, configure el componente de publicación y haga que su puerta de enlace SiteWise Edge reciba los datos y los envíe a la AWS nube.

Instalación del software SiteWise Edge Gateway en su dispositivo local

Una vez que haya creado una puerta de enlace SiteWise Edge, debe instalar el software de puerta de enlace SiteWise Edge en su dispositivo local. SiteWise El software de puerta de enlace Edge se puede instalar en dispositivos locales que tengan instalados los sistemas operativos de servidor Linux o Windows.

> **Important**
>
> Asegúrese de que el dispositivo local esté conectado a Internet.

Linux

El siguiente procedimiento utiliza SSH para conectarse al dispositivo local. Como alternativa, puede utilizar una unidad flash USB u otras herramientas para transferir el archivo de instalación a su dispositivo local. Si no quieres usar SSH, ve al paso 2: instala el software SiteWise Edge Gateway que se muestra a continuación.

Requisitos previos de SSH

Antes de conectarte al dispositivo mediante SSH, cumple los siguientes requisitos previos.

- Obtén la dirección IP de tu dispositivo.
- Obtén el nombre de usuario para conectarte a tu dispositivo.
- Instale un cliente SSH en su ordenador local según sea necesario.

  Es posible que el equipo local tenga instalado un cliente SSH de forma predeterminada. Para comprobarlo, escriba ssh en la línea de comandos. Si su equipo no reconoce el comando, puede instalar un cliente SSH.

  - Linux y macOS: descargue e instale OpenSSH. Para obtener más información, consulte https://www.openssh.com.

Paso 1: copia el instalador en tu dispositivo SiteWise Edge Gateway

Las siguientes instrucciones explican cómo conectarse a su dispositivo local mediante un cliente SSH.

1. Para conectarte a tu dispositivo, ejecuta el siguiente comando en una ventana de terminal de tu computadora y reemplaza el nombre de *usuario* y la *IP* por un nombre de usuario que tenga privilegios y una dirección IP elevados.

```
ssh username@IP
```

2. Para transferir el archivo de instalación AWS IoT SiteWise generado a su dispositivo de puerta de enlace SiteWise Edge, ejecute el siguiente comando.

> **Note**
>
> - *path-to-saved-installer*Reemplácelo por la ruta de su computadora que utilizó para guardar el archivo de instalación y el nombre del archivo de instalación.
> - Sustituya la *dirección IP* por la dirección IP de su dispositivo local.
> - *directory-to-receive-installer*Sustitúyala por la ruta del dispositivo local que utilizaste para recibir el archivo de instalación.

```
scp path-to-saved-installer.sh user-name@IP-address:directory-to-receive-
installer
```

Paso 2: Instale el software SiteWise Edge Gateway

En los siguientes procedimientos, ejecute los comandos en una ventana de terminal de su dispositivo de puerta de enlace SiteWise Edge.

1. Otorgue al archivo instalador el permiso de ejecución.

```
chmod +x path-to-installer.sh
```

2. Ejecute el instalador.

```
sudo ./path-to-installer.sh
```

Windows server

Requisitos previos

Debe cumplir los siguientes requisitos previos para instalar el software de puerta de enlace SiteWise Edge:

- Windows Server 2019 o posterior instalado
- Privilegios de administrador
- PowerShell instalada la versión 5.1 o posterior
- SiteWise El instalador de Edge Gateway se descargó en el servidor Windows donde se aprovisionará

Paso 1: Ejecute PowerShell como administrador

1. En el servidor Windows en el que desee instalar SiteWise Edge Gateway, inicie sesión como administrador.
2. Ingresa PowerShellen la barra de búsqueda de Windows.
3. En los resultados de la búsqueda, abre el menú contextual (con el botón derecho) de la PowerShell aplicación de Windows. Seleccione Ejecutar como administrador.

Paso 2: Instale el software SiteWise Edge Gateway

Ejecute los siguientes comandos en una ventana de terminal de su dispositivo SiteWise Edge Gateway.

1. Desbloquee el instalador de SiteWise Edge Gateway.

```
unblock-file path-to-installer.ps1
```

2. Ejecute el instalador.

```
./path-to-installer.ps1
```

> **Note**
>
> Si la ejecución del script está deshabilitada en el sistema, cambie la política de ejecución del script a `RemoteSigned`.
>
> ```
> Set-ExecutionPolicy RemoteSigned
> ```

Habilitación del procesamiento de datos de la periferia

Puede usar AWS IoT SiteWise Edge para recopilar, procesar y monitorear los datos del equipo a nivel local. Puede usar SiteWise Edge para modelar sus datos industriales y SiteWise Monitor para crear paneles de control para que su personal operativo visualice los datos a nivel local. Puede procesar sus datos de forma local y enviarlos a ella Nube de AWS, o procesarlos localmente mediante la AWS IoT SiteWise API.

Con AWS IoT SiteWise Edge, puedes procesar los datos sin procesar de forma local y elegir enviar solo datos agregados a ella para optimizar el Nube de AWS uso del ancho de banda y los costos de almacenamiento en la nube.

> **Note**
>
> - AWS IoT SiteWise conserva los datos perimetrales en sus gateways SiteWise Edge durante un máximo de 30 días. El período de retención de sus datos depende del espacio en disco disponible en su dispositivo.
> - Si su puerta de enlace SiteWise Edge ha estado desconectada de ella Nube de AWS durante 30 días, el paquete de procesamiento de datos se deshabilita automáticamente.

Configuración de la capacidad de periferia

AWS IoT SiteWise proporciona los siguientes paquetes que su puerta de enlace SiteWise Edge puede usar para determinar cómo recopilar y procesar sus datos. Seleccione paquetes para habilitar las capacidades perimetrales de su puerta de enlace SiteWise perimetral.

- El paquete de recopilación de datos permite a su puerta de enlace SiteWise Edge recopilar datos de varios servidores OPC-UA y, a continuación, exportar los datos del borde al. Nube de AWS Se activa una vez que haya agregado fuentes de datos a su puerta de enlace SiteWise Edge.
- El paquete de procesamiento de datos permite que su pasarela SiteWise Edge procese los datos de su equipo en la periferia. Por ejemplo, puede utilizar modelos de activos para calcular métricas y transformaciones. Para obtener más información sobre modelos de activos y los activos, consulte Crear modelos de activos industriales.

> **Note**
>
> El paquete de procesamiento de datos solo está disponible en plataformas x86.

Para configurar las capacidades perimetrales

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija las puertas de enlace Edge.
3. Seleccione la puerta de enlace de SiteWise Edge para la que desee activar las capacidades de Edge.
4. En la sección de capacidades de Edge, elija Editar
5. En la sección de capacidades de Edge, selecciona Habilitar el paquete de procesamiento de datos (conlleva cargos adicionales).
6. (Opcional) En la sección de conexión LDAP de Edge, puede conceder a los grupos de usuarios de su directorio corporativo acceso a esta SiteWise puerta de enlace de Edge. Los grupos de usuarios pueden usar las credenciales del Protocolo ligero de acceso a directorios (LDAP) para acceder a la puerta de enlace Edge. SiteWise Luego, pueden usarlas AWS OpsHub para la AWS IoT SiteWise aplicación, las operaciones de la AWS IoT SiteWise API u otras herramientas para administrar la puerta de enlace SiteWise Edge. Para obtener más información, consulte Administración de puertas de enlace SiteWise perimetrales.

> **Note**
>
> También puede usar las credenciales de Linux o Windows para acceder a la puerta de enlace SiteWise Edge. Para obtener más información, consulte Acceder a su puerta de enlace SiteWise Edge con las credenciales del sistema operativo Linux.

a. Selecciona Activado.

b. En Nombre del proveedor, introduzca un nombre para su proveedor de LDAP.

c. En Nombre de host o dirección IP, introduzca el nombre de host o la dirección IP de su servidor LDAP.

d. En Puerto, introduzca un número de puerto.

e. En Nombre distinguido (DN) de base, introduzca un nombre distinguido (DN) para la base.

   Se admiten los siguientes tipos de atributos: CommonName (CN), LocalityName (L), Name (ST), stateOrProvince OrganizationName (O), (OU), CountryName (C), organizationalUnitName StreetAddress (STREET), DomainComponent (DC) e ID de usuario (UID).

f. En DN de grupo de administradores, introduzca un DN.

g. En DN de grupo de usuarios, introduzca un DN.

7. Seleccione Guardar.

Ahora que ha activado las funciones periféricas en su puerta de enlace Edge, debe configurar su modelo de activos para la SiteWise periferia. La configuración de periferia de su modelo de activo especifica dónde se calculan las propiedades de los activos. Puede calcular todas las propiedades en la periferia o puede configurar las propiedades de su modelo de activo por separado. Las propiedades del modelo de activos incluyen métricas, transformaciones y mediciones.

Para obtener más información sobre las propiedades de activos, consulte the section called “Definición de las propiedades de datos”.

Después de crear el modelo de activo, puede configurarlo para la periferia. Para obtener más información sobre cómo configurar su modelo de activos para la periferia, consulte the section called “Creación de un modelo de activos (consola)”.

> **Note**
>
> Los modelos de activos y los paneles de control se sincronizan automáticamente entre la puerta de enlace Edge Nube de AWS y la de SiteWise Edge cada 10 minutos. También puedes sincronizarlos manualmente desde la aplicación SiteWise Edge Gateway local.

Procesamiento de datos en el borde

Debe configurar su modelo de activos para la periferia antes de poder procesar los datos de la puerta de enlace SiteWise perimetral en la periferia. La configuración de periferia de su modelo de activo especifica dónde se calculan las propiedades de los activos. Puede optar por calcular todas las propiedades en el borde y enviar los resultados a él Nube de AWS, o personalizar dónde se computará cada propiedad del activo por separado. Para obtener más información, consulte Habilitación del procesamiento de datos de la periferia.

Las propiedades de los activos incluyen métricas, transformaciones y medidas:

- Las métricas son los datos agregados del activo en un periodo de tiempo determinado. Puede calcular nuevas métricas utilizando los datos de métricas existentes. AWS IoT SiteWise siempre envía tus métricas a la AWS nube para almacenarlas a largo plazo. AWS IoT SiteWise calcula las métricas en la AWS nube de forma predeterminada. Puede configurar su modelo de activos para calcular sus métricas en la periferia. AWS IoT SiteWise envía los resultados procesados a la AWS nube.
- Las transformaciones son expresiones matemáticas que asignan puntos de datos de la propiedad de un activo de un formulario a otro. Las transformaciones pueden utilizar métricas como datos de entrada y deben computarse y almacenarse en la misma ubicación que sus entradas. Si configura una entrada métrica para que se calcule en el borde, AWS IoT SiteWise también calculará la transformación asociada en el borde.
- Las mediciones se formatean como datos en sin procesar que su dispositivo recopila y envía a la nube de AWS de forma predeterminada. Puede configurar su modelo de activos para almacenar estos datos en su dispositivo local.

Para obtener más información sobre las propiedades de activos, consulte the section called “Definición de las propiedades de datos”.

Después de crear el modelo de activo, puede configurarlo para la periferia. Para obtener más información sobre cómo configurar su modelo de activos para la periferia, consulte the section called “Creación de un modelo de activos (consola)”.

> **Note**
>
> Los modelos de activos y los paneles de control se sincronizan automáticamente entre la AWS nube y su puerta de enlace de SiteWise Edge cada 10 minutos. También puedes

sincronizarlos manualmente desde. Administración de puertas de enlace SiteWise perimetrales

Puede usar las API AWS IoT SiteWise REST y AWS Command Line Interface (AWS CLI) para consultar los datos de la SiteWise periferia en su puerta de enlace Edge. Antes de consultar los datos de la SiteWise periferia en la puerta de enlace de Edge, debe cumplir los siguientes requisitos previos:

- Sus credenciales deben estar configuradas para las API de REST. Para obtener más información acerca de cómo configurar las credenciales, consulte the section called “Administración de puertas de enlace SiteWise perimetrales”.
- El punto final del SDK debe apuntar a la dirección IP de su puerta de enlace SiteWise Edge. Puede encontrar más información en la documentación de su SDK. Por ejemplo, consulte Especificar puntos de conexión personalizados en la Guía para desarrolladores de AWS SDK for Java 2.x .
- Su certificado de puerta de enlace SiteWise Edge debe estar registrado. Puedes encontrar más información sobre cómo registrar tu certificado de puerta de enlace SiteWise Edge en la documentación de tu SDK. Por ejemplo, consulte el Registro de paquetes de certificados en Node.js en la Guía para desarrolladores de AWS SDK for Java 2.x .

Para obtener más información sobre cómo consultar datos con AWS IoT SiteWise, consulteConsulta datos de AWS IoT SiteWise.

Configuración del componente AWS IoT SiteWise Publisher

Tras crear una puerta de enlace AWS IoT SiteWise Edge e instalar el software, configure el componente Publisher para que la puerta de enlace SiteWise Edge pueda exportar datos a la AWS nube. Para obtener más información, consulte AWS IoT SiteWise Publisher en la Guía para AWS IoT Greengrass Version 2 desarrolladores.

Para configurar el editor (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Edge Gateways.
3. Seleccione la puerta de enlace SiteWise Edge para la que desee configurar el publicador.
4. En la sección de configuración de Publisher, elija Editar

5. En Orden de publicación, elija una de las siguientes opciones:

   - Publique primero los datos más antiguos: la puerta de enlace SiteWise Edge publica primero los datos más antiguos en la nube de forma predeterminada.
   - Publique primero los datos más recientes: la puerta de enlace SiteWise Edge publica primero los datos más recientes en la nube.

6. (Opcional) Si no desea que la puerta de enlace SiteWise Edge comprima sus datos, anule la selección de Activar la compresión al cargar datos.

7. (Opcional) Si no quieres publicar datos antiguos, selecciona Excluir datos caducados y haz lo siguiente:

   - En Periodo límite, introduzca un número y elija una unidad. El periodo límite debe ser de entre cinco minutos y siete días. Por ejemplo, si el periodo límite es de tres días, los datos anteriores a tres días no se publicarán en la nube.

8. (Opcional) Para establecer una configuración personalizada sobre cómo se gestionan los datos en el dispositivo local, selecciona Configuración de almacenamiento local y haz lo siguiente:

   a. En Periodo de retención, introduzca un número y elija una unidad. El periodo de retención debe ser de entre un minuto y 30 días, y mayor o igual que el periodo de rotación. Por ejemplo, si el período de retención es de 14 días, la puerta de enlace SiteWise Edge eliminará todos los datos del perímetro que sean anteriores al período límite especificado después de haberlos almacenado durante 14 días.

   b. En Periodo de rotación, introduzca un número y elija una unidad. El período de rotación debe ser superior a un minuto e igual o inferior al período de retención. Por ejemplo, si el período de rotación es de dos días, la puerta de enlace SiteWise Edge agrupa los datos anteriores al período límite y los guarda en un solo archivo. La puerta de enlace SiteWise Edge también transfiere un lote de datos al siguiente directorio local una vez cada dos días:. `/greengrass/v2/work/aws.iot.SiteWiseEdgePublisher/exports`

   c. En Capacidad de almacenamiento, introduzca un número que sea mayor o igual a 1. Si la capacidad de almacenamiento es de 2 GB, la puerta de enlace SiteWise Edge comienza a eliminar datos cuando hay más de 2 GB de datos almacenados localmente.

9. Elija Guardar.

Configuración de orígenes de datos

Después de configurar una puerta de enlace AWS IoT SiteWise Edge, puede configurar las fuentes de datos para que la puerta de enlace SiteWise Edge pueda ingerir datos de equipos industriales locales a otros. AWS IoT SiteWise Cada fuente representa un servidor local, como un servidor OPC-UA, al que la puerta de enlace SiteWise Edge conecta y recupera los flujos de datos industriales. Para obtener más información sobre la configuración de una puerta de enlace SiteWise Edge, consulte. Configuración de una puerta de enlace AWS IoT Greengrass V1 SiteWise Edge

> **Note**
>
> AWS IoT SiteWise reinicia la puerta de enlace SiteWise Edge cada vez que agrega o edita una fuente. La puerta de enlace SiteWise Edge no ingiere datos mientras se reinicia. El tiempo necesario para reiniciar la puerta de enlace SiteWise Edge depende de la cantidad de etiquetas que haya en las fuentes de la puerta de enlace SiteWise Edge. El tiempo de reinicio puede oscilar entre unos segundos (para una puerta de enlace SiteWise Edge con pocas etiquetas) y varios minutos (para una puerta de enlace SiteWise Edge con muchas etiquetas).

Después de crear los orígenes, puede asociar sus flujos de datos a las propiedades de los activos. Para obtener más información sobre cómo crear y utilizar activos, consulte Crear modelos de activos industriales y Asignación de flujos de datos industriales a propiedades de activos.

Puede ver CloudWatch las métricas para comprobar a qué fuente de datos está conectada AWS IoT SiteWise. Para obtener más información, consulte AWS IoT Greengrass Version 2 métricas de pasarela.

Actualmente, AWS IoT SiteWise es compatible con los siguientes protocolos de fuente de datos:

- OPC-UA: protocolo de comunicación machine-to-machine (M2M) para la automatización industrial.

> **Note**
>
> SiteWise Las pasarelas perimetrales que se ejecutan AWS IoT Greengrass V2 actualmente no son compatibles con las fuentes IP Modbus TCP y Ethernet.

Temas

Configuración de un origen OPC-UA

Puede usar la AWS IoT SiteWise consola o la capacidad de una puerta de enlace SiteWise Edge para definir y agregar una fuente OPC-UA a su puerta de enlace SiteWise Edge para representar un servidor OPC-UA local.

Temas

Configuración de un origen OPC-UA (consola)

Para configurar una fuente OPC-UA mediante la consola AWS IoT SiteWise

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, seleccione Puertas de enlace.
3. Seleccione la puerta de enlace SiteWise Edge para añadir una fuente OPC-UA.
4. Seleccione Añadir origen de datos.
5. Introduzca un nombre para el origen.
6. (Opcional) Introduzca un Prefijo de flujo de datos. La puerta de enlace SiteWise Edge agrega este prefijo a todos los flujos de datos de esta fuente. Utilice un prefijo de flujo de datos para distinguir entre flujos de datos que tienen el mismo nombre y orígenes diferentes. Cada flujo de datos debe tener un nombre único en su cuenta.
7. Escriba el Punto de conexión local del servidor de origen de datos. El punto de conexión puede ser la dirección IP o el nombre de host. También puede añadir un número de puerto

al punto de conexión local. Por ejemplo, su punto final local podría tener este aspecto: **`opc.tcp://203.0.113.0:49320`**

> **Note**
>
> Si su puerta `Deployment type` de enlace SiteWise Edge tiene un dispositivo Siemens Industrial Edge (nuevo) y desea ingerir datos de la aplicación Edge OPC UA Server que se ejecuta en el mismo dispositivo Siemens Industrial Edge que la aplicación AWS IoT SiteWise Edge, introduzca. **`opc.tcp://ie-opcua:48010`**

8. (Opcional) Para seleccionar el ID de nodo, añada filtros de nodo para limitar los flujos de datos que se transfieren al nodo. Nube de AWS De forma predeterminada, las puertas de enlace SiteWise Edge utilizan el nodo raíz de un servidor para ingerir todos los flujos de datos. Para definir filtros de nodo, puede utilizar ID de nodo y los caracteres comodín `*` y `**`.
9. En Destinos, elija el destino de los datos de origen:

   - AWS IoT SiteWise en tiempo real: elija esta opción para enviar los datos directamente al AWS IoT SiteWise almacenamiento. Ingiera y supervise los datos en tiempo real y procese los datos en la periferia.
   - AWS IoT SiteWise Almacenados en búfer mediante Amazon S3: envíe datos en formato parquet a Amazon S3 y, a continuación, impórtelos al AWS IoT SiteWise almacenamiento. Elija esta opción para ingerir datos en lotes y almacenar los datos históricos de forma rentable. Puede configurar la ubicación del bucket de Amazon S3 que prefiera y la frecuencia con la que desea que se carguen los datos en Amazon S3. También puede elegir qué hacer con los datos después de ingerirlos AWS IoT SiteWise. Puede elegir que los datos estén disponibles tanto SiteWise en Amazon S3 como en Amazon S3 o puede optar por eliminarlos automáticamente de Amazon S3.
     - El bucket de Amazon S3 es un mecanismo de almacenamiento y almacenamiento en búfer y admite archivos en formato parquet.
     - Si selecciona la casilla Importar datos al AWS IoT SiteWise almacenamiento, los datos se cargan primero en Amazon S3 y, después, en el AWS IoT SiteWise almacenamiento.
       - Si selecciona la casilla Eliminar datos de Amazon S3, los datos se eliminarán de Amazon S3 después de importarlos al SiteWise almacenamiento.
       - Si desactiva la casilla Eliminar datos de Amazon S3, los datos se almacenan tanto en Amazon S3 como en SiteWise almacenamiento.

- Si desactiva la casilla Importar datos al AWS IoT SiteWise almacenamiento, los datos solo se almacenan en Amazon S3. No se importan al SiteWise almacenamiento.

Visite Administrar el almacenamiento de datos para obtener más información sobre las distintas opciones de almacenamiento que AWS IoT SiteWise ofrece. Para obtener más información sobre las opciones de precios, consulta AWS IoT SiteWise los precios.

- AWS IoT Greengrass administrador de transmisiones: utilice AWS IoT Greengrass el administrador de transmisiones para enviar datos a los siguientes Nube de AWS destinos: canales entrantes AWS IoT Analytics, transmisiones en Amazon Kinesis Data Streams, propiedades de activos u objetos AWS IoT SiteWise en Amazon Simple Storage Service (Amazon S3). Para obtener más información, consulte Administrar transmisiones de datos en la Guía AWS IoT Greengrass básica para AWS IoT Greengrass Version 2 desarrolladores.

  Introduzca un nombre para la AWS IoT Greengrass transmisión.

10. Al configurar una fuente de datos, el ID de nodo de selección se utiliza para determinar el destino del flujo de datos.

    - Si los mismos datos se publican AWS IoT SiteWise en tiempo real y en AWS IoT SiteWise búfer mediante Amazon S3, debe añadir dos fuentes de datos que se publiquen en ambos destinos.
    - Para dividir los datos de forma que una parte de ellos se publique AWS IoT SiteWise en tiempo real y la otra parte en AWS IoT SiteWise Buffered mediante Amazon S3, debe filtrar los siguientes alias de datos:

      ```
      /Alias01/Data1
      /Alias02/Data1
      /Alias03/Data1
      /Alias03/Data2
      ```

      Por ejemplo, puede añadir una fuente de datos que apunte al filtro de `/**/Data1` nodos, a AWS IoT SiteWise tiempo real, y otra fuente de datos que apunte a un `/**/Data2` AWS IoT SiteWise búfer mediante Amazon S3.

11. En la ventana Configuración avanzada, realice lo siguiente:

    a. Elija un modo de seguridad de mensajes para las conexiones y los datos en tránsito entre el servidor de origen y la puerta de enlace SiteWise Edge. Este campo es la combinación de la política de seguridad OPC-UA y el modo de seguridad de mensajes. Elija la misma política

de seguridad y el mismo modo de seguridad de mensajes que especificó para su servidor OPC-UA.

b. Si su fuente requiere autenticación, elija un AWS Secrets Manager secreto de la lista de configuración de autenticación. La puerta de enlace SiteWise Edge usa las credenciales de autenticación de este secreto cuando se conecta a esta fuente de datos. Debe adjuntar los secretos al AWS IoT Greengrass componente de la puerta de enlace SiteWise Edge para utilizarlos en la autenticación de la fuente de datos. Para obtener más información, consulte the section called “Configuración de la autenticación del origen de datos”.

> **Tip**
>
> Es posible que el servidor de datos tenga una opción denominada Permitir inicio de sesión anónimo. Si esta opción es Sí, entonces el origen no requerirá autenticación.

c. En Grupos de propiedades, seleccione Añadir nuevo grupo.

d. Introduzca un Nombre para el grupo de propiedades.

e. En Propiedades:

1. (Opcional) En Rutas de nodo, añada filtros de nodo OPC-UA para limitar las rutas OPC-UA que se cargan en AWS IoT SiteWise. Puede usar filtros de nodos para reducir el tiempo de inicio de la puerta de enlace SiteWise Edge y el uso de la CPU al incluir únicamente las rutas a los datos que usted modele AWS IoT SiteWise. De forma predeterminada, las pasarelas SiteWise Edge cargan todas las rutas OPC-UA excepto las que comienzan por. `/Server/` Para definir filtros de nodo OPC-UA, puede utilizar rutas de nodo y los caracteres comodín * y **. Para obtener más información, consulte Uso de filtros de nodos OPC-UA.

f. En Configuración, realice lo siguiente:

1. (Opcional) Para configurar la calidad de los datos, elija el tipo de calidad de datos que desea que incorpore AWS IoT SiteWise Collector.
2. (Opcional) En Ajuste de modo de escaneo, configure las siguientes propiedades de suscripción estándar:
   - En Modo de escaneo, elija el modo que desea que AWS IoT SiteWise utilice para recopilar sus datos. Para obtener más información sobre el modo de escaneo, consulte the section called “Filtrado de rangos de ingesta de datos con OPC-UA”.

- Inicio del cambio de datos: puede definir la condición que inicia una alerta de cambio de datos.
- Tamaño de la cola de suscripciones: la profundidad de la cola en un servidor OPC-UA para una métrica concreta en la que se ponen en cola las notificaciones de los elementos monitorizados.
- Intervalo de publicación de la suscripción: el intervalo (en milisegundos) del ciclo de publicación especificado al crear la suscripción.
- Intervalo de instantáneas: puede configurar el ajuste de frecuencia de espera de las instantáneas para garantizar que AWS IoT SiteWise Edge ingiera un flujo constante de datos.
- En Velocidad de escaneo, actualice la velocidad a la que desea que la puerta de enlace SiteWise Edge lea sus registros. AWS IoT SiteWise calcula automáticamente la velocidad de escaneo mínima permitida para su puerta de enlace SiteWise Edge.

3. (Opcional) Configure un Tipo de banda muerta para su origen. Esto controla qué datos le envía su AWS IoT SiteWise fuente y qué datos descarta. Para obtener más información sobre configuración de la banda muerta, consulte the section called “Filtrado de rangos de ingesta de datos con OPC-UA”.

g. Seleccione Añadir.

12. Elija Siguiente.

Configuración de un origen OPC-UA (CLI)

Puede definir las fuentes de datos OPC-UA para una puerta de enlace SiteWise Edge mediante. AWS CLI Para ello, cree un archivo JSON de configuración de capacidades OPC-UA y utilice el update-gateway-capability-configurationcomando para actualizar la configuración de la puerta de enlace Edge. SiteWise Debe definir todos los orígenes OPC-UA en una única configuración de capacidad.

Para obtener más información sobre cómo definir las fuentes con AWS Command Line Interface, consulte. the section called “Configuración de orígenes de datos (AWS CLI)”

Esta capacidad tiene las siguientes versiones.

Versión	Espacio de nombres
1	`iotsitewise:opcuacollector:1`

Sintaxis de la solicitud

```
{
  "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"
                }
            ]
        }
    }
  ]
}
```

Cuerpo de la solicitud

fuentes

Es una lista de estructuras de definición de origen OPC-UA que contienen la siguiente información:

name

Un nombre único y sencillo para el origen.

punto de conexión

Una estructura de punto de conexión que contiene la siguiente información:

Fideicomiso certificado

Una estructura de política de confianza de certificados que contiene la siguiente información:

type

El modo de confianza del certificado para el origen. Seleccione una de las siguientes opciones:

- **`TrustAny`**— La puerta de enlace SiteWise Edge confía en cualquier certificado cuando se conecta a la fuente OPC-UA.
- `X509`— La puerta de enlace SiteWise Edge confía en un certificado X.509 cuando se conecta a la fuente OPC-UA. Si elige esta opción, debe definir `certificateBody` en `certificateTrust`. También puede definir `certificateChain` en `certificateTrust`.

Entidad certificadora

(Opcional) Cuerpo de un certificado X.509.

Este campo es obligatorio si elige `X509` para `type` en `certificateTrust`.

CertificateChain

(Opcional) Cadena de confianza para un certificado X.509.

Este campo solo se utiliza si elige `X509` para `type` en `certificateTrust`.

URI de Endpoint

El punto de conexión local del origen OPC-UA. Por ejemplo, su punto de conexión local podría tener el siguiente aspecto: `opc.tcp://203.0.113.0:49320`.

Política de seguridad

La política de seguridad que debe utilizar para que pueda proteger los mensajes que se leen desde el origen OPC-UA. Seleccione una de las siguientes opciones:

- `NONE`— La puerta de enlace SiteWise Edge no protege los mensajes de la fuente OPC-UA. Le recomendamos que elija una política de seguridad diferente. Si elige esta opción, también debe elegir `NONE` para `messageSecurityMode`.
- `BASIC256_SHA256`: la política de seguridad `Basic256Sha256`.
- `AES128_SHA256_RSAOAEP`: la política de seguridad `Aes128_Sha256_RsaOaep`.
- `AES256_SHA256_RSAPSS`: la política de seguridad `Aes256_Sha256_RsaPss`.
- `BASIC128_RSA15`: (obsoleta) la política de seguridad `Basic128Rsa15` está en desuso en la especificación OPC-UA dado que ya no se considera segura. Le recomendamos que elija una política de seguridad diferente. Para obtener más información, consulte Basic128Rsa15.
- `BASIC256`: (obsoleta) la política de seguridad `Basic256` está en desuso en la especificación OPC-UA dado que ya no se considera segura. Le recomendamos que elija una política de seguridad diferente. Para obtener más información, consulte Basic256.

> **Important**
>
> Si elige una política de seguridad distinta a `NONE`, debe elegir `SIGN` o `SIGN_AND_ENCRYPT` para `messageSecurityMode`. También debe configurar el servidor de origen para que confíe en la puerta de enlace SiteWise Edge. Para obtener más información, consulte Permitir que sus servidores de origen OPC-UA confíen en la puerta de enlace Edge SiteWise .

messageSecurityMode

Es el modo de seguridad de mensajes que se va a utilizar para proteger las conexiones al origen OPC-UA. Seleccione una de las siguientes opciones:

- `NONE`— La puerta de enlace SiteWise Edge no protege las conexiones a la fuente OPC-UA. Le recomendamos que elija un modo de seguridad de mensajes diferente. Si elige esta opción, también debe elegir `NONE` para `securityPolicy`.
- `SIGN`— Los datos en tránsito entre la puerta de enlace SiteWise Edge y la fuente OPC-UA están firmados pero no cifrados.
- `SIGN_AND_ENCRYPT`: los datos en tránsito entre la puerta de enlace y el origen OPC-UA se firman y cifran.

> **Important**
>
> Si elige un modo de seguridad de mensajes que no sea `NONE`, debe elegir una `securityPolicy` distinta de `NONE`. También debe configurar el servidor de origen para que confíe en la puerta de enlace SiteWise Edge. Para obtener más información, consulte Permitir que sus servidores de origen OPC-UA confíen en la puerta de enlace Edge SiteWise .

Proveedor de identidad

Estructura de proveedor de identidades que contiene la siguiente información:

type

Tipo de credenciales de autenticación requeridas por el origen. Seleccione una de las siguientes opciones:

- `Anonymous`: el origen no requiere autenticación para conectarse.
- `Username`: el origen requiere un nombre de usuario y una contraseña para conectarse. Si elige esta opción, debe definir `usernameSecretArn` en `identityProvider`.

usernameSecretArn

(Opcional) El ARN de un AWS Secrets Manager secreto. La puerta de enlace SiteWise Edge usa las credenciales de autenticación de este secreto cuando se conecta a esta fuente. Debe adjuntar los secretos al SiteWise conector IoT de su puerta de

enlace SiteWise Edge para usarlos en la autenticación de origen. Para obtener más información, consulte Configuración de la autenticación del origen de datos.

Este campo es obligatorio si elige `Username` para `type` en `identityProvider`.

nodeFilterRules

Una lista de estructuras de reglas de filtrado de nodos que definen las rutas de flujo de datos OPC-UA que se van a enviar a la AWS nube. Puedes usar filtros de nodos para reducir el tiempo de inicio de la puerta de enlace SiteWise Edge y el uso de la CPU al incluir únicamente las rutas a los datos que modeles. AWS IoT SiteWise De forma predeterminada, las pasarelas SiteWise Edge cargan todas las rutas OPC-UA excepto las que comienzan por. `/Server/` Para definir filtros de nodo OPC-UA, puede utilizar rutas de nodo y los caracteres comodín `*` y `**`. Para obtener más información, consulte Uso de filtros de nodos OPC-UA.

Cada estructura de la lista debe contener la siguiente información:

action

Es la acción de esta regla de filtro de nodo. Puede elegir la siguiente opción:

- `INCLUDE`— La puerta de enlace SiteWise Edge incluye solo los flujos de datos que cumplen esta regla.

definición

Estructura de reglas de filtros de nodo que contiene la siguiente información:

type

Es el tipo de ruta de filtro de nodo para esta regla. Puede elegir la siguiente opción:

- `OpcUaRootPath`— La puerta de enlace SiteWise Edge evalúa esta ruta de filtro de nodos comparándola con la raíz de la jerarquía de rutas OPC-UA.

RootPath

Ruta de filtro de nodo que se va a evaluar con la raíz de la jerarquía de rutas de OPC-UA. Esta ruta debe comenzar con `/`.

measurementDataStreamPrefijo

Cadena que se debe anteponer a todos los flujos de datos del origen. La puerta de enlace SiteWise Edge agrega este prefijo a todos los flujos de datos de esta fuente. Utilice un prefijo de flujo de datos para distinguir entre flujos de datos que tienen el mismo nombre y orígenes diferentes. Cada flujo de datos debe tener un nombre único en su cuenta.

Grupos de propiedades

(Opcional) La lista de grupos de propiedades que definen la `deadband` y el `scanMode` solicitados por el protocolo.

name

El nombre del grupo de propiedades. Debe ser un identificador único.

banda muerta

La estructura de `deadband` que contiene la siguiente información:

type

Los tipos de banda muerta admitidos. Los valores aceptados son `ABSOLUTE` y `PERCENT`.

value

El valor de la banda muerta. Cuando `type` es `ABSOLUTE`, este valor es un doble sin unidades. Cuando `type` es `PERCENT`, este valor es un doble entre `1` y `100`.

eGumin

(Opcional) La unidad de ingeniería mínima al utilizar una banda muerta `PERCENT`. Usted la establece si el servidor OPC-UA no tiene unidades de ingeniería configuradas.

EguMax

(Opcional) La unidad de ingeniería máxima al utilizar una banda muerta `PERCENT`. Usted la establece si el servidor OPC-UA no tiene unidades de ingeniería configuradas.

Tiempo de espera en milisegundos

La duración en milisegundos antes del tiempo de espera. El mínimo es `100`.

Modo de escaneo

La estructura de `scanMode` que contiene la siguiente información:

type

Los tipos admitidos de `scanMode`. Los valores aceptados son `POLL` y `EXCEPTION`.

tasa

El intervalo de muestreo para el modo de escaneo.

nodeFilterRuleDefiniciones

(Opcional) Una lista de rutas de nodos para incluir en el grupo de propiedades. Los grupos de propiedades no pueden solaparse. Si no especifica un valor para este campo, el grupo contendrá todas las rutas bajo la raíz y no podrá crear grupos de propiedades adicionales. La estructura `nodeFilterRuleDefinitions` contiene la siguiente información:

type

`OpcUaRootPath` es el único tipo admitido. Especifica que el valor de `rootPath` es una ruta relativa a la raíz del espacio de navegación OPC-UA.

RootPath

Lista delimitada por comas que especifica las rutas (relativas a la raíz) por incluir en el grupo de propiedades.

Ejemplos de configuración de capacidad

El siguiente ejemplo define la configuración de la capacidad de una puerta de enlace OPC-UA SiteWise Edge a partir de una carga útil almacenada en un archivo JSON.

```
aws iotsitewise update-gateway-capability-configuration \
--capability-namespace "iotsitewise:opcuacollector:1" \
--capability-configuration file://opc-ua-configuration.json
```

Example : Configuración de origen OPC-UA

El siguiente archivo `opc-ua-configuration.json` define una configuración de origen OPC-UA básica e insegura.

```
{
"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 : Configuración de origen OPC-UA con grupos de propiedades definidos

El siguiente archivo `opc-ua-configuration.json` define una configuración de origen OPC-UA básica e insegura con grupos de propiedades definidos.

```
{
  "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 : Configuración de origen OPC-UA con propiedades

El siguiente ejemplo JSON para `opc-ua-configuration.json` define una configuración de origen OPC-UA con las siguientes propiedades:

- Confía en cualquier certificado.
- Utiliza la política de seguridad `BASIC256` para proteger los mensajes.
- Utiliza el modo `SIGN_AND_ENCRYPT` para proteger las conexiones.
- Utiliza credenciales de autenticación almacenadas en un secreto del administrador de secretos.
- Filtra los flujos de datos, excepto aquellos cuya ruta comienza por `/WindFarm/2/WindTurbine/`.
- Añade `/Washington` al inicio de cada ruta de flujo de datos para distinguir entre este “Wind Farm #2” y un “Wind Farm #2” en otra área.

```
{
"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

El siguiente ejemplo JSON para `opc-ua-configuration.json` define una configuración de origen OPC-UA con las siguientes propiedades:

- Confiar en un certificado X.509 dado.
- Utiliza la política de seguridad `BASIC256` para proteger los mensajes.
- Utiliza el modo `SIGN_AND_ENCRYPT` para proteger las conexiones.

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

Permitir que sus servidores de origen OPC-UA confíen en la puerta de enlace Edge SiteWise

Si elige una opción `messageSecurityMode` distinta de Ninguna al configurar su fuente OPC-UA, debe permitir que sus servidores de origen confíen en la puerta de enlace Edge. AWS IoT SiteWise La puerta de enlace SiteWise Edge genera un certificado que puede necesitar su servidor de origen. El proceso varía en función de los servidores de origen. Para obtener más información, consulte la documentación de sus servidores.

El siguiente procedimiento describe los pasos básicos.

Para permitir que un servidor OPC-UA confíe en la SiteWise puerta de enlace Edge

1. Abra la interfaz para configurar el servidor OPC-UA.
2. Escriba el nombre de usuario y la contraseña del administrador del servidor OPC-UA.
3. Localice Clientes de confianza en la interfaz y, a continuación, seleccione Cliente de puerta de enlace de AWS IoT SiteWise .para conectarse.
4. Elija Confiar.

Exportación del certificado de cliente OPC-UA

Algunos servidores OPC-UA requieren acceso al archivo de certificado del cliente OPC-UA para confiar en la puerta de enlace Edge. SiteWise Si esto se aplica a sus servidores OPC-UA, puede utilizar el siguiente procedimiento para exportar el certificado de cliente OPC-UA desde la puerta de enlace Edge. SiteWise A continuación, puede importar el certificado en su servidor OPC-UA.

Para exportar el archivo de certificado de cliente OPC-UA de un origen

1. Ejecute el siguiente comando para ir al directorio que contiene el archivo de certificado. *Sustituya sitewise-work por la ruta de almacenamiento local del aws.iot. SiteWiseEdgeCollectorOpcua*Greengrass en la carpeta de trabajo y sustituya el nombre de la *fuente de datos por el nombre* de la fuente de datos.

   *Por defecto, la carpeta de trabajo de Greengrass es /greengrass/v2/ work/aws.iot. SiteWiseEdgeCollectorOpcua*en Linux y *C: /greengrass/v2/work/ aws.iot. SiteWiseEdgeCollectorOpcua*en Windows.

   ```
   cd /sitewise-work/source-name/opcua-certificate-store
   ```

2. El certificado de cliente OPC-UA de la puerta de enlace SiteWise Edge para esta fuente está en el `aws-iot-opcua-client.pfx` archivo.

   Ejecute el siguiente comando para exportar el certificado a un archivo `.pem` llamado `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. Transfiera el archivo de certificado desde la puerta de enlace SiteWise Edge al servidor OPC-UA. `aws-iot-opcua-client-certificate.pem`

   Para ello, puede utilizar un software común como el programa `scp` para transferir el archivo utilizando el protocolo SSH. Para obtener más información, consulte Copia segura en Wikipedia.

   > **Note**
   >
   > Si su puerta de enlace SiteWise Edge se ejecuta en Amazon Elastic Compute Cloud (Amazon EC2) y se conecta a ella por primera vez, debe configurar los requisitos previos para conectarse. Para obtener más información, consulte Conexión con la instancia de Linux en la Guía del usuario de Amazon EC2 para instancias de Linux.

4. Importe el archivo de certificado en el servidor OPC-UA para confiar en la puerta de enlace Edge. `aws-iot-opcua-client-certificate.pem` SiteWise Los pasos pueden variar en función del servidor de origen que utilice. Consulte la documentación de cada servidor.

Filtrado de rangos de ingesta de datos con OPC-UA

Puede controlar la forma de ingerir datos con un origen OPC-UA mediante el modo de escaneo e intervalos de banda muerta. Estas funciones le permiten controlar qué tipo de datos desea ingerir y cómo y cuándo su servidor y la puerta de enlace SiteWise Edge intercambian esta información.

Control de la frecuencia de recopilación de datos con el modo de escaneo

Puede configurar el modo de escaneo OPC-UA para controlar el modo de recopilación de datos de su origen OPC-UA. Puede elegir el modo de suscripción o de sondeo.

- Modo de suscripción: la fuente OPC-UA recopila datos para enviarlos a su puerta de enlace SiteWise Edge con la frecuencia definida por su velocidad de escaneo. El servidor solo envía datos cuando el valor ha cambiado, por lo que esta es la frecuencia máxima con la que su puerta de enlace SiteWise Edge recibe datos.
- Modo de sondeo: su puerta de enlace SiteWise Edge sondea la fuente OPC-UA a una frecuencia establecida definida por su velocidad de escaneo. El servidor envía los datos independientemente

de si el valor ha cambiado, por lo que su puerta de enlace SiteWise Edge siempre recibe los datos en este intervalo.

> **Note**
>
> La opción de modo de sondeo anula sus ajustes de banda muerta para este origen.

Filtrado de la ingesta de datos OPC-UA con intervalos de banda muerta

Puedes aplicar una banda inactiva a tus grupos de propiedades de origen del OPC-UA para filtrar y descartar determinados datos en lugar de enviarlos a la nube. AWS Una banda muerta especifica una ventana de fluctuaciones esperadas en los valores de datos entrantes desde su origen OPC-UA. Si los valores se encuentran dentro de esta ventana, tu servidor OPC-UA no los enviará a la nube. AWS Puedes usar el filtrado de banda muerta para reducir la cantidad de datos que procesas y envías a la nube. AWS Para obtener información sobre cómo configurar las fuentes OPC-UA para su puerta de enlace SiteWise Edge, consulte. the section called “Configuración de orígenes de datos”

> **Note**
>
> Su servidor elimina todos los datos que caen dentro de la ventana especificada por su banda muerta. Los datos descartados no se pueden recuperar.

Tipos de bandas muertas

Puede especificar dos tipos de bandas muertas para su grupo de propiedades del servidor OPC-UA. Estas le permiten elegir la cantidad de datos que se envían a la AWS nube y la cantidad que se descarta.

- Porcentaje: usted especifica una ventana utilizando un porcentaje de fluctuación esperada en el valor de medición. El servidor calcula el intervalo exacto a partir de este porcentaje y envía a la AWS nube los datos que exceden el margen. Por ejemplo, si se especifica un valor de banda muerta del 2% en un sensor con un rango de -100 grados Fahrenheit a +100 grados Fahrenheit, se indica al servidor que envíe los datos a la AWS nube cuando el valor cambie 4 grados Fahrenheit o más.

> **Note**
>
> Si lo desea, puede especificar un valor mínimo y máximo de banda muerta para esta ventana si su servidor de origen no define unidades de ingeniería. Si no se proporciona un rango de unidades de ingeniería, el servidor OPC-UA utiliza de forma predeterminada el rango completo del tipo de datos de medición.

- Absoluto: usted especifica una ventana utilizando unidades exactas. Por ejemplo, al especificar un valor de banda muerta de 2 en un sensor, se indica al servidor que envíe datos a la nube de AWS cuando su valor cambie al menos en 2 unidades. Puede utilizar la banda muerta absoluta para entornos dinámicos en los que se esperan fluctuaciones regulares durante las operaciones normales.

Tiempos de espera de banda muerta

Si lo desea, puede configurar un tiempo de espera de banda muerta. Una vez transcurrido este tiempo de espera, el servidor OPC-UA envía el valor de medición actual aunque se encuentre dentro de la fluctuación de banda muerta esperada. Puede utilizar la configuración de tiempo de espera para asegurarse de que AWS IoT SiteWise se ingiere un flujo constante de datos en todo momento, incluso cuando los valores no superen el intervalo de tiempo muerto definido.

Uso de filtros de nodos OPC-UA

Al definir las fuentes de datos OPC-UA para una puerta de enlace SiteWise Edge, puede definir filtros de nodos. Los filtros de nodos le permiten limitar las rutas de flujo de datos que la puerta de enlace SiteWise Edge envía a la nube. Puedes usar filtros de nodos para reducir el tiempo de inicio de la puerta de enlace SiteWise Edge y el uso de la CPU al incluir únicamente las rutas a los datos que modeles AWS IoT SiteWise. De forma predeterminada, las pasarelas SiteWise Edge cargan todas las rutas OPC-UA excepto las que comienzan por. `/Server/` Puede utilizar los caracteres comodín * y ** en los filtros de nodos para incluir varios flujos de datos con un solo filtro. Para obtener información sobre cómo configurar las fuentes OPC-UA para su SiteWise puerta de enlace Edge, consulte. Configuración de orígenes de datos

> **Note**
>
> AWS IoT SiteWise reinicia la puerta de enlace SiteWise Edge cada vez que añada o edite una fuente. La puerta de enlace SiteWise Edge no ingiere datos mientras se reinicia. El

tiempo necesario para reiniciar la puerta de enlace SiteWise Edge depende de la cantidad de etiquetas que haya en las fuentes de la puerta de enlace SiteWise Edge. El tiempo de reinicio puede oscilar entre unos segundos (para una puerta de enlace SiteWise Edge con pocas etiquetas) y varios minutos (para una puerta de enlace SiteWise Edge con muchas etiquetas).

En la tabla siguiente se enumeran los caracteres comodín que se pueden utilizar para filtrar orígenes de datos de OPC-UA.

Comodines para filtros de nodos de OPC-UA

Comodín	Descripción
*	Coincide con un solo nivel en una ruta de flujo de datos.
**	Coincide con varios niveles en una ruta de flujo de datos.

Note

Si configura una fuente con un filtro amplio y luego cambia la fuente para usar un filtro más restrictivo, AWS IoT SiteWise deja de almacenar los datos que no coinciden con el nuevo filtro.

Example Escenario de ejemplo con filtros de nodos

Piense en los siguientes flujos de datos hipotéticos:

- `/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`

Con los flujos de datos anteriores, puede definir filtros de nodos para limitar qué datos se van a incluir de su origen OPC-UA.

- Para seleccionar todos los nodos en este ejemplo, utilice `/` o `/**/`. Puede incluir varios directorios o carpetas con los caracteres comodín `**`.
- Para seleccionar todos los flujos de datos de `PLC`, utilice `/*/*/*/PLC*` o `/**/PLC*`.
- Para seleccionar todos los contadores en este ejemplo, utilice `/**/Counter*` o `/*/*/*/Counter*`.
- Para seleccionar todos los contadores de `Line 2`, utilice `/**/Line 2/Counter*`.

Configuración de la autenticación del origen de datos

Si su servidor OPC-UA requiere credenciales de autenticación para conectarse, puede utilizarlas AWS Secrets Manager para crear e implementar un secreto en su puerta de enlace SiteWise Edge. AWS Secrets Manager cifra los secretos del dispositivo para proteger su nombre de usuario y contraseña hasta que necesite usarlos. Para obtener más información, consulte Administrador de secretos en la Guía para desarrolladores de AWS IoT Greengrass Version 2 .

Paso 1: Crear secretos de autenticación de origen

Se puede utilizar AWS Secrets Manager para crear un secreto de autenticación para la fuente de datos. En el secreto, defina pares clave-valor, **`username`** y **`password`**, que contengan detalles de autenticación para su origen de datos.

Para crear un secreto (consola)

1. Vaya a la consola de AWS Secrets Manager.
2. Seleccione Almacenar un nuevo secreto.
3. En Tipo de secreto, seleccione Otro tipo de secretos.
4. En Pares clave/valor, haga lo siguiente:
    1. En el primer cuadro de entrada, introduzca el nombre de usuario **`username`** y, en el segundo cuadro de entrada, introduzca el nombre de usuario.
    2. Seleccione Agregar regla.
    3. En el primer cuadro de entrada, introduzca **`password`** y en el segundo cuadro introduzca la contraseña.

5. Para la clave de cifrado, seleccione aws/secretsmanager y, a continuación, elija Siguiente.
6. En la página Guardar un nuevo secreto, introduzca un Nombre secreto.
7. (Opcional) Introduzca una Descripción que le ayude a identificar este secreto y, a continuación, seleccione Siguiente.
8. (Opcional) En la página Guardar un nuevo secreto, active Rotación automática. Para obtener más información, consulte Rotación de secretos en la Guía del usuario de AWS Secrets Manager .
9. Especifique un calendario de rotación.
10. Elija una función de Lambda que pueda rotar este secreto y, a continuación, seleccione Siguiente.
11. Revise la configuración de sus secretos y, a continuación, seleccione Guardar.

Para autorizar la interacción con la puerta de enlace de SiteWise Edge AWS Secrets Manager, la función de IAM de la puerta de enlace de SiteWise Edge debe permitir la acción. `secretsmanager:GetSecretValue` Puede utilizar el dispositivo principal de Greengrass para buscar la política de IAM. Para obtener más información sobre la actualización de una política de IAM, consulte Edición de políticas de IAM en la Guía del usuario.AWS Identity and Access Management

Example política

Sustituya *`secret-arn`* por el nombre de recurso de Amazon (ARN) del secreto que creó en el paso anterior. Para obtener más información sobre cómo obtener el ARN de un secreto, consulte Recuperación de su secreto de AWS Secrets Manager en la Guía del usuario de AWS Secrets Manager .

```
{
"Version":"2012-10-17",
"Statement":[
  {
     "Action":[
        "secretsmanager:GetSecretValue"
     ],
     "Effect":"Allow",
     "Resource":[
        "secret-arn"
     ]
  }
```

```
]
}
```

Paso 2: Implemente secretos en su dispositivo de puerta de enlace SiteWise Edge

Puede usar la AWS IoT SiteWise consola para implementar datos secretos en su puerta de enlace SiteWise Edge.

Para implementar un secreto (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, seleccione Puertas de enlace.
3. En la lista de puertas de enlace, elija la puerta de enlace SiteWise Edge de destino.
4. En la sección de configuración de la puerta de enlace, elija el enlace del dispositivo principal de Greengrass para abrir el AWS IoT Greengrass núcleo asociado a la puerta de enlace SiteWise Edge.
5. En el panel de navegación, seleccione Implementaciones.
6. Seleccione la implementación de destino y, a continuación, Revisar.
7. En la página Especificar destino, seleccione Siguiente.
8. En la página Seleccionar componentes, en la sección Componentes públicos, desactive la opción Mostrar solo componentes seleccionados.
9. Busque y elija aws.greengrass. SecretManagercomponente y, a continuación, elija Siguiente.
10. En la lista de componentes seleccionados, elija aws.greengrass. SecretManagercomponente y, a continuación, elija Configurar componente.
11. En el campo Configuración por fusionar, añada el siguiente objeto JSON.

> **Note**
>
> Sustituya *`secret-arn`* por el ARN del secreto que creó en el paso anterior. Para obtener más información sobre cómo obtener el ARN de un secreto, consulte Recuperación de su secreto de AWS Secrets Manager en la Guía del usuario de AWS Secrets Manager .

```
{
```

```
"cloudSecrets":[
  {
     "arn":"secret-arn"
  }
]
}
```

12. Seleccione Confirmar.
13. Elija Siguiente.
14. En la página Configurar opciones avanzadas, seleccione Siguiente.
15. Revise las configuraciones de su implementación y, a continuación, seleccione Implementar.

Paso 3: Añadir configuraciones de autenticación

Puede usar la AWS IoT SiteWise consola para agregar configuraciones de autenticación a su puerta de enlace SiteWise Edge.

Para añadir configuraciones de autenticación (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En la lista de puertas de enlace, elija la puerta de enlace SiteWise Edge de destino.
3. En la lista Orígenes de datos, seleccione el origen de datos de destino y, a continuación, Editar.
4. En la página Añadir un origen de datos, seleccione Configuración avanzada.
5. En Configuración de autenticación, elija el secreto que implementó en el paso anterior.
6. Seleccione Guardar.

Configuración de orígenes de datos (AWS CLI)

Puede usar la AWS IoT SiteWise API y agregar fuentes AWS Command Line Interface a su puerta de enlace AWS IoT SiteWise Edge. Las fuentes se definen en las capacidades de la puerta de enlace de SiteWise Edge. La capacidad de una puerta de enlace SiteWise Edge representa una función de software que se ejecuta en la puerta de enlace SiteWise Edge, como la capacidad de recopilar datos industriales de fuentes OPC-UA.

SiteWise Las capacidades de la puerta de enlace perimetral tienen los siguientes componentes:

- Una configuración: un documento JSON que define todos los orígenes de datos de una capacidad.

- Un espacio de nombre: una cadena única que identifica el tipo y la versión de una capacidad. Por ejemplo, el espacio de nombres de la capacidad de origen OPC-UA es `iotsitewise:opcuacollector:`*`version`*, donde *`version`* es la versión de la capacidad de OPC-UA. Todos los orígenes OPC-UA se definen en una sola capacidad con este espacio de nombres.
- Un estado de sincronización: un estado que indica si una capacidad está sincronizada entre la AWS nube y la puerta de enlace SiteWise Edge. El estado de sincronización puede ser uno de los siguientes valores:
  - `IN_SYNC`— La puerta de enlace SiteWise Edge ejecuta la configuración de capacidades.
  - `OUT_OF_SYNC`— La puerta de enlace SiteWise Edge no ha recibido la configuración de capacidad.
  - `SYNC_FAILED`— La puerta de enlace SiteWise Edge rechazó la configuración de la capacidad.

  Tras actualizar una configuración de capacidades, su estado de sincronización es `OUT_OF_SYNC` hasta que la puerta de enlace SiteWise Edge reciba y aplique o rechace la configuración actualizada.

Utilice las siguientes operaciones para consultar y actualizar las configuraciones de capacidades y las fuentes de la puerta de enlace SiteWise Edge:

- DescribeGateway— Recupera información sobre una puerta de enlace SiteWise Edge específica. La respuesta incluye una lista de resúmenes de capacidades, incluidos los espacios de nombres de capacidades.
- DescribeGatewayCapabilityConfiguration— Recupera la configuración de una capacidad específica. Utilice esta operación para recuperar una configuración de capacidad para actualizarla.
- ListGateways— Muestra información sobre todas las pasarelas SiteWise Edge. La respuesta incluye una lista de resúmenes de las capacidades de cada puerta de enlace SiteWise Edge, incluidos los espacios de nombres de las capacidades.
- UpdateGatewayCapabilityConfiguration— Actualiza la configuración de capacidades de una puerta de enlace SiteWise Edge o define una nueva configuración de capacidades. Esta operación identifica las capacidades por espacio de nombres de capacidades. Si proporciona un espacio de nombres que ya existe, esta operación actualizará la capacidad para ese espacio de nombres. De lo contrario, esta operación creará una capacidad nueva.

> **Warning**
>
> La UpdateGatewayCapabilityConfigurationoperación sobrescribe la configuración de capacidad existente con la configuración que usted proporciona en la carga útil. Para evitar eliminar la configuración de la capacidad, deberá añadirla a la configuración existente al actualizar la capacidad.

SiteWise Capacidades de Edge Gateway

- ???
- ???
- ???

Elección de un destino para los datos de su servidor de origen

Los datos se exportan desde la periferia a AWS IoT SiteWise tiempo real o en lotes mediante Amazon S3. También puede enviar la transmisión a otro componente mediante una AWS IoT Greengrass transmisión.

- AWS IoT SiteWise tiempo real: elija esta opción para enviar los datos directamente al AWS IoT SiteWise almacenamiento. Ingiera y supervise los datos en tiempo real y procese los datos en la periferia.
- AWS IoT SiteWise Almacenados en búfer mediante Amazon S3: envíe datos en formato parquet a Amazon S3 y, a continuación, impórtelos al AWS IoT SiteWise almacenamiento. Elija esta opción para ingerir datos en lotes y almacenar los datos históricos de forma rentable. Puede configurar la ubicación del bucket de Amazon S3 que prefiera y la frecuencia con la que desea que se carguen los datos en Amazon S3. También puede elegir qué hacer con los datos después de ingerirlos AWS IoT SiteWise. Puede elegir que los datos estén disponibles tanto SiteWise en Amazon S3 como en Amazon S3 o puede optar por eliminarlos automáticamente de Amazon S3.
  - El bucket de Amazon S3 es un mecanismo de almacenamiento y almacenamiento en búfer y admite archivos en formato parquet.
  - Si selecciona la casilla Importar datos al AWS IoT SiteWise almacenamiento, los datos se cargan primero en Amazon S3 y, después, en el AWS IoT SiteWise almacenamiento.

    - Si selecciona la casilla Eliminar datos de Amazon S3, los datos se eliminarán de Amazon S3 después de importarlos al SiteWise almacenamiento.
    - Si desactiva la casilla Eliminar datos de Amazon S3, los datos se almacenan tanto en Amazon S3 como en SiteWise almacenamiento.
  - Si desactiva la casilla Importar datos al AWS IoT SiteWise almacenamiento, los datos solo se almacenan en Amazon S3. No se importan al SiteWise almacenamiento.

  Visite Administrar el almacenamiento de datos para obtener más información sobre las distintas opciones de almacenamiento que AWS IoT SiteWise ofrece. Para obtener más información sobre las opciones de precios, consulta AWS IoT SiteWise los precios.
- AWS IoT Greengrass administrador de transmisiones: utilice AWS IoT Greengrass el administrador de transmisiones para enviar datos a los siguientes Nube de AWS destinos: canales entrantes AWS IoT Analytics, transmisiones en Amazon Kinesis Data Streams, propiedades de activos u objetos AWS IoT SiteWise en Amazon Simple Storage Service (Amazon S3). Para obtener más información, consulte Administrar transmisiones de datos en la Guía AWS IoT Greengrass básica para AWS IoT Greengrass Version 2 desarrolladores.

En el siguiente ejemplo se muestra la estructura del mensaje de flujo de datos requerida. Todos los campos son obligatorios.

```
{
    "assetId": "string",
    "propertyAlias": "string",
    "propertyId": "string",
    "propertyValues": [
      {
         "quality": "string",
         "timestamp": {
            "offsetInNanos": number,
            "timeInSeconds": number
         },
         "value": {
            "booleanValue": boolean,
            "doubleValue": number,
            "integerValue": number,
            "stringValue": "string"
         }
      }
```

```
    ]
}
```

> **Note**
>
> El mensaje de flujo de datos debe incluir (`assetIdypropertyId`) o `propertyAlias` en su estructura.

`assetId`

(Opcional) El ID del activo que se va a actualizar.

`propertyAlias`

(Opcional) El alias que identifica la propiedad, como la ruta de flujo de datos de un servidor OPC-UA. Por ejemplo:

```
/company/windfarm/3/turbine/7/temperature
```

Para obtener más información, consulte Asignación de flujos de datos industriales a propiedades de activos en la Guía del AWS IoT SiteWise usuario.

`propertyId`

(Opcional) El ID de la propiedad del activo de esta entrada.

`propertyValues`

(Obligatorio) La lista de valores de propiedades que se va a cargar. Puede especificar hasta 10 elementos `propertyValues` de matriz.

`quality`

(Opcional) La calidad del valor de la propiedad de activo.

`timestamp`

(Obligatorio) La marca temporal del valor de la propiedad del activo.

`offsetInNanos`

(Opcional) El desfase de nanosegundos desde. `timeInSeconds`

`timeInSeconds`

(Obligatorio) La fecha y hora, en segundos, en formato de época de Unix. Los datos fraccionarios de nanosegundos los proporciona `offsetInNanos`.

`value`

(Obligatorio) El valor de la propiedad del activo.

> **Note**
>
> Solo puede existir uno de los siguientes valores en el `value` campo.

`booleanValue`

(Opcional) Datos de propiedades de activos de tipo booleano (`trueofalse`).

`doubleValue`

(Opcional) Datos de propiedades de activos de tipo double (número de punto flotante).

`integerValue`

(Opcional) Datos de propiedades de activos de tipo entero (número entero).

`stringValue`

(Opcional) Datos de propiedades de activos de tipo cadena (secuencia de caracteres).

Agregar fuentes de datos de socios a las puertas de enlace SiteWise Edge

Al usar una puerta de enlace de AWS IoT SiteWise Edge, puede conectar una fuente de datos asociada a su puerta de enlace de SiteWise Edge y recibir datos del socio en su puerta de enlace de SiteWise Edge y en la AWS nube. Estos orígenes de datos de socios son componentes AWS IoT Greengrass desarrollados en colaboración entre AWS y el socio. Cuando añada una fuente de datos asociada, AWS IoT SiteWise creará este componente y lo implementará en su puerta de enlace SiteWise Edge.

Para añadir un origen de datos de un socio, realice lo siguiente:

- Adición de un origen de datos de un socio
- Vaya al portal web del socio y configure la fuente de datos del socio para que se conecte a la puerta de enlace SiteWise Edge.

Temas

Seguridad

Como parte del Modelo de responsabilidad compartida entre AWS, nuestros clientes y nuestros socios, a continuación se describe quién es responsable de los diferentes aspectos de la seguridad:

Responsabilidad del cliente

- Investigar al socio.
- Configurar el acceso a la red otorgado al socio.

Responsabilidad de AWS

- Aislar al socio de los recursos en la nube de AWS del cliente excepto aquellos que el socio necesite. En este caso, ingesta de AWS IoT SiteWise.
- Restrinja la solución asociada a un uso razonable de los recursos de la máquina de la puerta de enlace SiteWise Edge (CPU, memoria, sistema de archivos).

Responsabilidad del socio

- Uso de valores predeterminados seguros.
- Mantener la solución segura en el tiempo mediante parches y otras actualizaciones apropiadas.
- Mantener la confidencialidad de los datos de los clientes.

Adición de un origen de datos de un socio

Para conectar una fuente de datos asociada a su puerta de enlace SiteWise Edge, agréguela como fuente de datos. Cuando lo añada como fuente de datos, AWS IoT SiteWise implementará un AWS IoT Greengrass componente privado en su puerta de enlace SiteWise Edge.

Requisitos previos

Para añadir un origen de datos de un socio, debe hacer lo siguiente:

- Crear una cuenta con el socio.
- Vincular las cuentas.

Para crear una puerta de enlace SiteWise Edge con una fuente de datos asociada

Si desea crear una nueva puerta de enlace SiteWise Edge, complete los pasos que se indican a continuaciónCreación de una puerta de enlace SiteWise Edge. Una vez que haya creado la puerta de enlace SiteWise Edge, siga los pasos que se indican Para agregar una fuente de datos asociada a una puerta de enlace de SiteWise Edge existente para agregar una fuente de datos asociada.

Para agregar una fuente de datos asociada a una puerta de enlace de SiteWise Edge existente

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, seleccione Puertas de enlace.
3. Elija la puerta de enlace SiteWise Edge a la que desee conectar la fuente de datos del socio.
4. En Orígenes de datos, elija Añadir origen de datos.
5. En Tipo de fuente, elija el socio al que desee conectar su puerta de enlace SiteWise Edge.

   > **Note**
   >
   > Actualmente, EasyEdge es la única fuente de datos de socios disponible. La primera vez que añada una fuente de EasyEdge datos, tendrá que crear una EasyEdge cuenta.

6. Introduzca un nombre para el origen.
7. Para conceder al socio acceso al origen de datos, seleccione Autorizar.
8. Para permitir que AWS IoT SiteWise actualice su componente de publicador de AWS IoT SiteWise y, si el paquete de procesamiento de datos está habilitado, el componente de procesador de AWS IoT SiteWise, seleccione Actualizar componentes.
9. Seleccione Guardar.

Configura el docker en tu puerta de enlace Edge SiteWise

Para añadir una fuente de datos asociada, debe estar instalado Docker Engine 1.9.1 o una versión posterior en su dispositivo local.

> **Note**
>
> Se ha comprobado que la versión 20.10 es la última versión que funciona con el software SiteWise Edge Gateway.

Para verificar si Docker está instalado

Para comprobar que Docker está instalado, ejecuta el siguiente comando desde un terminal conectado a tu puerta de enlace SiteWise Edge:

```
docker info
```

Si el comando devuelve un resultado `docker is not recognized` o hay instalada una versión anterior de Docker, Instale Docker Engine antes de continuar.

Para configurar Docker

El usuario del sistema que ejecute un componente contenedor de Docker debe tener permisos de raíz o administrador, o bien debe configurar Docker para que se ejecute como un usuario no de raíz o no administrador.

En los dispositivos Linux, debe añadir un usuario `ggc_user` al grupo de `docker` para ejecutar los comandos de Docker sin `sudo`.

Para añadir el `ggc_user`, o el usuario no raíz que utilice para ejecutar los componentes del contenedor de Docker, al grupo de `docker`, ejecute el siguiente comando:

```
sudo usermod -aG docker ggc_user
```

Para obtener más información, consulte Pasos posteriores a la instalación en Linux para Docker Engine.

SiteWise Fuentes de datos de socios de Edge Gateway

Utilice la siguiente información para configurar un origen de datos de un socio.

EasyEdge

Portal:

https://studio.easyedge.io/

EasyEdge documentación:

EasyEdge para AWS

Uso de los paquetes

AWS IoT SiteWiseLas pasarelas Edge utilizan diferentes paquetes para determinar cómo recopilar y procesar los datos.

Actualmente están disponibles los siguientes paquetes:

- Paquete de recopilación de datos: utilice este paquete para recopilar sus datos industriales y enrutarlos a los destinos en la nube de AWS. De forma predeterminada, este paquete se habilita automáticamente para su puerta de enlace SiteWise Edge.
- Paquete de procesamiento de datos: utilice este paquete para habilitar la comunicación de la puerta de enlace SiteWise Edge con modelos de activos y activos configurados de forma perimetral. Puede utilizar la configuración de periferia para controlar qué datos de activos se van a computar y procesar en las instalaciones. A continuación, puede enviar los datos a AWS IoT SiteWise o a otros servicios de AWS. Para obtener más información sobre el paquete de procesamiento de datos, consulte the section called “Habilitación del procesamiento de datos de la periferia”.

Actualización de paquetes

> **Important**
>
> La actualización de versiones de paquetes de procesamiento de datos de la versión 2.0.x y anteriores a la versión 2.1.x provocará la pérdida de datos de las mediciones almacenadas localmente.

SiteWise Las pasarelas perimetrales utilizan diferentes paquetes para determinar cómo recopilar y procesar los datos. Puede utilizar la consola de AWS IoT SiteWise para actualizar los paquetes.

Para actualizar paquetes (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, seleccione Puertas de enlace.
3. En la lista de puertas de enlace, elija la puerta de enlace SiteWise Edge con los paquetes que desee actualizar.
4. En la página de resumen de SiteWise Edge Gateway, selecciona Actualizaciones.

   > **Note**
   >
   > Solo puede actualizar los paquetes que estén habilitados. Para ver la lista de paquetes que están habilitados para esta puerta de enlace de SiteWise Edge, seleccione Descripción general y, a continuación, consulte la sección de capacidades de Edge.

5. En la sección Actualizaciones de paquetes, realice una de las siguientes acciones.
   - Para el recopilador OPC-UA, elige una versión y, a continuación, selecciona Deploy.
   - Para Publisher, elija una versión y, a continuación, elija Implementar.
   - Para el paquete de procesamiento de datos, elija una versión y, a continuación, elija Implementar.
6. Para confirmar la implementación, seleccione Implementar. En la columna Implementación de la lista Puertas de enlace, verá Completado. Si no ve alguna actualización de estado de la implementación, actualice la página.

> **Note**
>
> - Implemente solo un paquete a la vez. Si implementa varios paquetes a la vez, solo se implementará el último que haya elegido.

Si tiene problemas para actualizar los paquetes, consulte No se han podido implementar paquetes en las puertas de enlace de SiteWise Edge.

Administración de puertas de enlace SiteWise perimetrales

Puede usar la AWS IoT SiteWise consola y las operaciones de la API para administrar las puertas de enlace AWS IoT SiteWise Edge. También puede usar la aplicación AWS OpsHub para Windows AWS IoT SiteWise para administrar algunos aspectos de su puerta de enlace SiteWise Edge desde su dispositivo local.

Le recomendamos encarecidamente que utilice la AWS IoT SiteWise aplicación AWS OpsHub for para supervisar el uso del disco en su dispositivo local. También puedes monitorear las CloudWatch métricas `Gateway.AvailableDiskSpace` y las de `Gateway.UsedPercentageDiskSpace` Amazon y crear alarmas para recibir notificaciones cuando se agote el espacio en disco. Para obtener más información sobre CloudWatch las alarmas de Amazon, consulta Crear una CloudWatch alarma basada en un umbral estático.

Asegúrese de que su dispositivo disponga de espacio suficiente para los datos venideros. Cuando estés a punto de quedarte sin espacio en tu dispositivo local, el servicio eliminará automáticamente una pequeña cantidad de datos con las marcas de tiempo más antiguas para dejar espacio para los próximos datos.

Para comprobar si el servicio ha eliminado sus datos, haga lo siguiente:

1. Inicia sesión en la AWS OpsHub aplicación. AWS IoT SiteWise
2. Elija Configuración.
3. En Registros, especifique un intervalo de tiempo y, a continuación, seleccione Descargar.
4. Descomprima el archivo de registro.

5. Si el archivo de registro contiene el siguiente mensaje, el servicio ha eliminado sus datos: se ha eliminado un *número* de bytes de datos para evitar que el almacenamiento de SiteWise Edge Gateway se quede sin espacio.

Administrar la puerta de enlace SiteWise Edge con la AWS IoT SiteWise consola

Puede usar la AWS IoT SiteWise consola para configurar, actualizar y monitorear todas las puertas de enlace SiteWise Edge de su AWS cuenta.

Puede ver sus puertas de enlace de SiteWise Edge navegando a la página de puertas de enlace de Edge de la consola.AWS IoT SiteWise Para acceder a la página de detalles de la puerta de enlace de Edge de una puerta de enlace específica, elija el nombre de una puerta de enlace de Edge.

En la pestaña Descripción general de la página de detalles de la puerta de enlace Edge, puede hacer lo siguiente:

- En la sección Fuentes de datos, actualice la configuración de la fuente de datos y configure fuentes de datos adicionales
- Seleccione Abrir CloudWatch métricas para ver la cantidad de puntos de datos ingeridos por fuente de datos en la consola de CloudWatch métricas
- En la sección de capacidades de Edge, añada paquetes de datos a su puerta de enlace de SiteWise Edge haciendo clic en Editar
- En la sección de configuración de la puerta de enlace, consulte el estado de conectividad de las puertas de enlace SiteWise Edge
- En la sección de configuración del editor, consulte el estado de sincronización y la configuración de la puerta de enlace SiteWise Edge del componente del AWS IoT SiteWise editor

En la pestaña Actualizaciones de la página de detalles de la puerta de enlace Edge, puede ver las versiones actuales de los componentes y paquetes que están implementadas en la puerta de enlace Edge. Aquí también se implementan las nuevas versiones, cuando están disponibles.

Administrar las puertas de enlace SiteWise Edge mediante AWS OpsHubAWS IoT SiteWise

Utiliza la AWS IoT SiteWise aplicación AWS OpsHub for para administrar y monitorear sus puertas de enlace SiteWise Edge. Esta aplicación proporciona las siguientes opciones de monitoreo y administración:

- En Información general puede hacer lo siguiente:
  - Vea los detalles de la puerta de enlace SiteWise Edge que le ayudarán a obtener información sobre los datos de sus dispositivos de puerta de enlace SiteWise Edge, identificar problemas y mejorar el rendimiento de la puerta de enlace SiteWise Edge.
  - Vea los portales SiteWise Monitor que monitorean los datos de los servidores y equipos locales ubicados en la periferia. Para obtener más información, consulte Qué es AWS IoT SiteWise Monitor en la Guía de la aplicación AWS IoT SiteWise Monitor .
- En Salud, hay un panel de control que muestra los datos de su puerta de enlace SiteWise Edge. Los expertos en el campo, como los ingenieros de procesos, pueden usar el panel para ver una descripción general del comportamiento de las puertas de enlace SiteWise Edge.
- En Activos, consulta los activos desplegados en el dispositivo local y el último valor recopilado o calculado para las propiedades de los activos.
- En Configuración puede hacer lo siguiente:
  - Si el paquete de procesamiento de datos está instalado, consulte la información de configuración de la puerta de enlace SiteWise Edge y sincronice los recursos con la AWS nube.
  - Descargue los archivos de autenticación que puede usar para acceder a la puerta de enlace SiteWise Edge mediante otras herramientas.
  - Descarga los registros que puedes usar para solucionar problemas con la puerta de enlace SiteWise Edge.
  - Vea los AWS IoT SiteWise componentes implementados en la puerta de enlace SiteWise Edge.

> **Important**
>
> Se requiere lo siguiente AWS OpsHub para su uso AWS IoT SiteWise:
>
> - El dispositivo local y la AWS IoT SiteWise aplicación AWS OpsHub for deben estar conectados a la misma red.

- El paquete de procesamiento de datos debe estar activado.

Para administrar las puertas de enlace SiteWise Edge mediante AWS OpsHub

1. Descargue e instale la aplicación AWS OpsHubAWS IoT SiteWise para Windows.
2. Abra la aplicación.
3. Si no ha configurado las credenciales locales para su puerta de enlace, siga los pasos que se indican Acceder a su puerta de enlace SiteWise Edge con las credenciales del sistema operativo local a continuación para configurarlas.
4. Puede iniciar sesión en su puerta de enlace SiteWise Edge con sus credenciales de Linux o del Protocolo ligero de acceso a directorios (LDAP). Para iniciar sesión en su puerta de enlace SiteWise Edge, realice una de las siguientes acciones:

   Linux

   1. Para el nombre de host o la dirección IP, introduzca el nombre de host o la dirección IP de su dispositivo local.
   2. En Autenticación, elija Linux.
   3. En Nombre de usuario, introduzca el nombre de usuario de su sistema operativo Linux.
   4. En Contraseña, introduzca la contraseña de su sistema operativo Linux.
   5. Elija Iniciar sesión.

   LDAP

   1. En Nombre de host o dirección IP, introduzca el nombre de host o la dirección IP de su dispositivo local.
   2. En Autenticación, elija LDAP.
   3. En Nombre de usuario, introduzca su nombre de usuario de LDAP.
   4. En Contraseña, introduzca su contraseña de LDAP.
   5. Seleccione Iniciar sesión.

Acceder a su puerta de enlace SiteWise Edge con las credenciales del sistema operativo local

Además del Protocolo ligero de acceso a directorios (LDAP), puede utilizar las credenciales de Linux o Windows para acceder a su puerta de enlace SiteWise Edge.

> **Important**
>
> Para acceder a su puerta de enlace SiteWise Edge con credenciales de Linux, debe activar el paquete de procesamiento de datos de su puerta de enlace SiteWise Edge.

Acceder a su puerta de enlace SiteWise Edge con las credenciales del sistema operativo Linux

En los siguientes pasos se asume que utiliza un dispositivo con Ubuntu. Si utiliza una distribución de Linux diferente, consulte la documentación correspondiente a su dispositivo.

Para crear un grupo de usuarios de Linux

1. Para crear un grupo de administradores, ejecute el siguiente comando.

   ```
   sudo groupadd --system SWE_ADMIN_GROUP
   ```

   Los usuarios del `SWE_ADMIN_GROUP` grupo pueden permitir el acceso de administrador a la puerta de enlace SiteWise Edge.
2. Para crear un grupo de usuarios, ejecute el siguiente comando.

   ```
   sudo groupadd --system SWE_USER_GROUP
   ```

   Los usuarios del `SWE_USER_GROUP` grupo pueden permitir el acceso de solo lectura a la puerta de enlace SiteWise Edge.
3. Para añadir un usuario al grupo de administradores, ejecute el siguiente comando. Sustituya *`user-name`* y *`password`* por el nombre de usuario y la contraseña que desee añadir.

   ```
   sudo useradd -p $(openssl passwd -1 password) user-name
   ```
4. Para añadir un usuario a `SWE_ADMIN_GROUP` o `SWE_USER_GROUP`, sustituya *`user-name`* por el nombre de usuario que añadió en el paso anterior.

```
sudo usermod -a -G SWE_ADMIN_GROUP user-name
```

Ahora puede usar el nombre de usuario y la contraseña para iniciar sesión en la puerta de enlace SiteWise Edge en la aplicación AWS OpsHub for AWS IoT SiteWise .

Acceder a su puerta de enlace SiteWise Edge con las credenciales de Windows

En los pasos siguientes se asume que utiliza un dispositivo con Windows.

> **Important**
>
> La seguridad es una responsabilidad compartida entre usted AWS y usted. Cree una política de contraseña segura con al menos 12 caracteres y una combinación de mayúsculas, minúsculas, números y símbolos. Además, configure las reglas del cortafuegos de Windows para permitir el tráfico entrante en el puerto 443 y bloquear el tráfico entrante en todos los demás puertos.

Para crear un grupo de usuarios de Windows Server

1. Ejecute PowerShell como administrador.
   a. En el servidor Windows en el que desee instalar SiteWise Edge Gateway, inicie sesión como administrador.
   b. Ingresa PowerShellen la barra de búsqueda de Windows.
   c. En los resultados de la búsqueda, haz clic con el botón derecho en la PowerShell aplicación de Windows. Seleccione Ejecutar como administrador.
2. Para crear un grupo de administradores, ejecute el siguiente comando.

   ```
   net localgroup SWE_ADMIN_GROUP /add
   ```

   Debe ser un usuario del `SWE_ADMIN_GROUP` grupo para permitir el acceso de administrador a la puerta de enlace SiteWise Edge.
3. Para crear un grupo de usuarios, ejecute el siguiente comando.

   ```
   net localgroup SWE_USER_GROUP /add
   ```

Debe ser un usuario del `SWE_USER_GROUP` grupo para permitir el acceso exclusivo a la puerta de enlace SiteWise Edge.

4. Para añadir un usuario, ejecute el siguiente comando. Sustituya *`user-name`* y *`password`* por el nombre de usuario y la contraseña que desee crear.

```
net user user-name password /add
```

5. Para añadir un usuario al grupo de administradores, ejecute el siguiente comando. Sustituya *`user-name`* por el nombre de usuario que desee añadir.

```
net localgroup SWE_ADMIN_GROUP user-name /add
```

Ahora puede usar el nombre de usuario y la contraseña para iniciar sesión en la puerta de enlace SiteWise Edge en la AWS IoT SiteWise aplicación AWS OpsHub for.

Administrar el certificado de la puerta de enlace SiteWise Edge

Puede usar SiteWise Monitor y aplicaciones de terceros, como Grafana, en sus dispositivos SiteWise Edge Gateway. Estas aplicaciones requieren una conexión TLS al servicio. SiteWise Las puertas de enlace Edge utilizan actualmente un certificado autofirmado. Si utiliza un navegador para abrir las aplicaciones, como un portal de SiteWise Monitor, es posible que reciba una advertencia sobre un certificado que no es de confianza.

A continuación, se muestra cómo descargar el certificado de confianza de AWS OpsHub la AWS IoT SiteWise aplicación.

1. Inicie sesión en la aplicación.
2. Elija Configuración.
3. En Autenticación, elija Descargar certificado.

A continuación se supone que utilizas Google Chrome o FireFox. Si utiliza un navegador diferente, consulte la documentación correspondiente al mismo. Para añadir el certificado que ha descargado en el paso anterior a un navegador, realice una de las siguientes acciones:

- Si utiliza Google Chrome, siga las instrucciones indicadas en Configuración de certificados de la Documentación de ayuda de Google Chrome Enterprise.

- Si utiliza Firefox, siga las instrucciones indicadas en Carga del certificado en el navegador Mozilla o Firefox de la Documentación de Oracle.

Cambiar la versión de los paquetes de componentes de SiteWise Edge Gateway

Puede usar la AWS IoT SiteWise consola para cambiar la versión de los paquetes de componentes en sus gateways SiteWise Edge.

Para cambiar la versión de un paquete de componentes de una puerta de enlace SiteWise Edge

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación izquierdo, seleccione Puertas de enlace.
3. Seleccione la puerta de enlace SiteWise Edge cuyas versiones del paquete desee cambiar.
4. En Configuración de Gateway, selecciona Ver versiones de software.
5. En la página Editar versiones de software, en el paquete del que desee actualizar la versión, seleccione la versión que desee implementar y elija Implementar.
6. Seleccione Listo.

Running SiteWise Edge en Siemens Industrial Edge

Puede transferir los datos de su dispositivo Siemens Industrial Edge al suyo Cuenta de AWS ejecutando una puerta de enlace SiteWise Edge en el dispositivo. Para ello, cree un recurso de puerta de enlace SiteWise Edge con un objetivo de despliegue del dispositivo Siemens Industrial Edge (nuevo), descargue el archivo de configuración y cárguelo en su aplicación Siemens a través del portal Siemens Industrial Edge Management (IEM). Para obtener más información sobre cómo ejecutar AWS IoT SiteWise Edge en Siemens Industrial Edge, incluida la forma de configurar los recursos de Siemens necesarios, consulte ¿Qué es Industrial Edge? en la documentación de Siemens.

> **Note**
>
> Siemens no es un vendedor o proveedor de AWS IoT SiteWise Edge. El Siemens Industrial Edge Marketplace es un mercado independiente.

Temas

Requisitos previos

Para ejecutar AWS IoT SiteWise Edge en Siemens Industrial Edge, necesita lo siguiente:

- Una cuenta de la plataforma Siemens Digital Exchange
- Una cuenta de Siemens Industrial Edge Hub (iehub)
- Una instancia de Siemens Industrial Edge Management (IEM)
- Un dispositivo industrial Edge (IED) de Siemens o un dispositivo virtual Siemens Industrial Edge (iEVD)
- Acceso al objetivo de despliegue del dispositivo Siemens Industrial Edge. Para acceder, vaya a la AWS IoT SiteWise consola y seleccione Solicitar acceso.

Seguridad

Como parte del modelo de responsabilidad compartida entre AWS nuestros clientes y nuestros socios, a continuación se describe quién es responsable de los diferentes aspectos de la seguridad:

Responsabilidad del cliente

- Investigar al socio.
- Configurar el acceso a la red otorgado al socio.
- Proteger físicamente el dispositivo en el que se ejecuta AWS IoT SiteWise Edge.

AWS responsabilidad

- Aislar al socio de los recursos en la AWS nube del cliente.

Responsabilidad del socio

- Uso de valores predeterminados seguros.
- Mantener la solución segura en el tiempo mediante parches y otras actualizaciones apropiadas.

- Mantener la confidencialidad de los datos de los clientes.
- Examinar otras aplicaciones disponibles en el mercado de socios.

Durante la fase de vista previa de esta función, el socio y otras aplicaciones instaladas a través del mercado de socios pueden acceder a los datos de los clientes que se almacenan en la memoria AWS IoT SiteWise caché del dispositivo asociado.

Creación del archivo de configuración

Una vez que tenga las cuentas de Siemens y las instancias de IEM adecuadas, podrá crear una pasarela SiteWise Edge para un dispositivo Siemens Industrial Edge de tipo despliegue.

Para crear el archivo de configuración

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Edge Gateways.
3. Seleccione Crear puerta de enlace.
4. En el tipo de implementación, elija el dispositivo Siemens Industrial Edge: nuevo.
5. Introduzca un nombre para su puerta de enlace SiteWise Edge o utilice el nombre generado por AWS IoT SiteWise.
6. (Opcional) En la configuración avanzada, haga lo siguiente:
   - Introduce un nombre para tu AWS IoT Core cosa o utiliza el nombre generado por AWS IoT SiteWise.
7. Seleccione Crear puerta de enlace.
8. En el cuadro de diálogo Generar el archivo de configuración de la puerta de enlace SiteWise Edge, seleccione Generar y descargar. AWS IoT SiteWise genera automáticamente un archivo de configuración que utilizará para configurar la aplicación AWS IoT SiteWise Edge.

> **Important**
>
> Asegúrese de guardar el archivo de configuración en un lugar seguro. Lo utilizará más adelante.

Ahora que ha creado la puerta de enlace SiteWise Edge, haga lo siguiente para terminar de configurar la puerta de enlace SiteWise Edge:

1. Agregue fuentes de datos
2. Configure el componente Publisher

Una vez que tenga el archivo de configuración y la puerta de enlace SiteWise Edge esté configurada, descargue la aplicación AWS IoT SiteWise Edge del Siemens Industrial Edge Marketplace e instálela mediante el portal Siemens Industrial Edge Management (IEM). A continuación, acceda a su dispositivo Siemens Industrial Edge a través del portal Siemens Industrial Edge Management (IEM) y cargue el archivo de configuración en el dispositivo en el que desee instalar la puerta de enlace SiteWise Edge.

Solución de problemas

Para solucionar los problemas relacionados con la pasarela SiteWise Edge de su dispositivo Siemens Industrial Edge, puede acceder a los registros de la aplicación a través de los portales Siemens Industrial Edge Management (IEM) o Siemens Industrial Edge Device (IED). Para obtener más información, consulte Descarga de registros en la documentación de Siemens.

Veo 'SESSION_TAKEN_OVER' o 'com.aws.greengrass.mqttclient. MqttClient: No se pudo publicar el mensaje a través de Spooler y lo volveré a intentar. ' en los registros

Si ve una advertencia que incluye `SESSION_TAKEN_OVER` o un error que incluye `com.aws.greengrass.mqttclient.MqttClient: Failed to publish the message via Spooler and will retry.` en sus registros`/greengrass/v2/logs/greengrass.log`, puede que esté intentando usar el mismo archivo de configuración para varias puertas de enlace SiteWise Edge en varios dispositivos. Cada puerta de enlace SiteWise Edge necesita un archivo de configuración único para conectarse a su Cuenta de AWS.

Veo «com.aws.greengrass.deployment». IotJobsHelper: No se encontró ningún trabajo de despliegue. o «El resultado del despliegue ya se ha informado». en los registros

Si ve `com.aws.greengrass.deployment.IotJobsHelper: No deployment job found.` o está `Deployment result already reported.` en sus registros en`/greengrass/v2/logs/greengrass.log`, puede que esté intentando reutilizar el mismo archivo de configuración.

Existen varias soluciones:

- Si desea volver a utilizar el archivo de configuración, haga lo siguiente:

  1. Vaya a la consola de AWS IoT SiteWise.
  2. En el panel de navegación, seleccione Puertas de enlace.
  3. Elija la puerta de enlace SiteWise Edge que desee reutilizar.
  4. Selecciona la pestaña Actualizaciones.
  5. Seleccione una versión de Publisher diferente y elija Implementar.

- Siga los pasos Creación del archivo de configuración que se indican para crear un nuevo archivo de configuración.

Veo «Falta AWS_REGION en el archivo de configuración» en los registros.

Si aparece `Config file missing AWS_REGION` en los registros de Siemens, el JSON del archivo de configuración está dañado. Deberá crear un nuevo archivo de configuración. Siga los pasos Creación del archivo de configuración que se indican para crear un nuevo archivo de configuración.

Contacto

- Si quieres solicitar acceso a la aplicación, ve a la AWS IoT SiteWise consola y selecciona Solicitar acceso.
- Si necesitas ayuda para solucionar los problemas de la aplicación, ve a la AWS IoT SiteWise consola, navega hasta la página de detalles de la puerta de enlace SiteWise Edge y selecciona Obtener asistencia.

Filtrado de activos en una puerta de enlace SiteWise Edge

Puede usar el filtrado perimetral para administrar sus activos de manera más eficiente enviando solo un subconjunto de activos a una puerta de enlace SiteWise Edge específica para su uso en el procesamiento de datos. Si sus activos están organizados en forma de árbol o estructura principal secundaria, puede configurar una política de IAM asociada a la función de IAM de una puerta de enlace de SiteWise Edge que solo permita enviar la raíz del árbol, o principal, y sus elementos secundarios a una puerta de enlace de Edge específica. SiteWise

> **Note**
>
> Si está organizando los activos existentes en una estructura de árbol, después de crear la estructura, vaya a cada activo existente que haya agregado a la estructura y elija Editar y, a continuación, seleccione Guardar para asegurarse de que AWS IoT SiteWise reconoce la nueva estructura.

Configuración del filtrado de periferia

Para configurar el filtrado de borde en la puerta de enlace de SiteWise Edge, añada la siguiente política de IAM a la función de IAM de la puerta de enlace de SiteWise Edge y *root-asset-idsustituya < >* por el ID del activo raíz que desee enviar a la puerta de enlace de 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>*"
                }
            }
        }
    ]
}
```

Si actualmente hay activos en su puerta de enlace de SiteWise Edge que desee eliminar, inicie sesión en su puerta de enlace de SiteWise Edge y ejecute el siguiente comando para forzar a la puerta de enlace de SiteWise Edge a sincronizarse con ellos AWS IoT SiteWise mediante la eliminación de la memoria caché.

```
sudo rm /greengrass/v2/work/aws.iot.SiteWiseEdgeProcessor/sync-app/
sync_resource_bundles/edge.json
```

Uso de las API de AWS IoT SiteWise en la periferia

Puede utilizar un subconjunto de las API de AWS IoT SiteWise disponibles junto con API específicas de periferia para interactuar con sus recursos y modelos de recursos en la periferia. Los modelos de activos deben configurarse para que se ejecuten en la periferia. Para obtener más información, consulte Procesamiento de datos en el borde.

Utilice estas API para recopilar datos sobre sus recursos y modelos de recursos, monitorear los portales implementados y las métricas del panel de control, y obtener datos de los recursos recopilados en la periferia. Esto proporciona un host central en su red para interactuar con AWS IoT SiteWise sin necesidad de realizar una llamada a la API web.

Temas

- Todas las API disponibles para su uso con dispositivos de periferia de AWS IoT SiteWise
- API de solo periferia para uso con dispositivos AWS IoT SiteWise de periferia
- Tutorial: Obtener una lista de modelos de activos en una puerta de enlace SiteWise Edge

Todas las API disponibles para su uso con dispositivos de periferia de AWS IoT SiteWise

Al trabajar con dispositivos en la periferia puede utilizar una variedad de API para interactuar con AWS IoT SiteWise y completar tareas de forma local en el dispositivo.

API de AWS IoT SiteWise disponibles

Las siguientes API de AWS IoT SiteWise están disponibles en los dispositivos de periferia:

- ListAssetModels
- DescribeAssetModel
- ListAssets
- DescribeAsset
- DescribeAssetProperty

- ListAssociatedAssets
- GetAssetPropertyAggregates
- GetAssetPropertyValue
- GetAssetPropertyValueHistory
- ListDashboards
- ListPortals
- ListProjectAssets
- ListProjects
- DescribeDashboard
- DescribePortal
- DescribeProject

API de solo periferia disponibles

Las siguientes API se utilizan localmente en dispositivos en la periferia:

- Autenticación: utilice esta API para obtener las credenciales temporales SigV4 que utilizará para realizar llamadas a la API.

API de solo periferia para uso con dispositivos AWS IoT SiteWise de periferia

Además de las API de AWS IoT SiteWise que están disponibles en la periferia, hay otras específicas de periferia. A continuación se describen esas API específicas de periferia.

Autenticación

Obtiene las credenciales de la puerta de enlace SiteWise Edge. Tendrá que añadir usuarios locales o conectarse a su sistema utilizando LDAP o un grupo de usuarios de Linux. Para obtener más información sobre cómo añadir usuarios, consulte LDAP o Grupo de usuarios de Linux.

Sintaxis de la solicitud

```
POST /authenticate HTTP/1.1
Content-type: application/json
{
```

```
  "username": "string",
  "password": "string",
  "authMechanism": "string"
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

username

El nombre de usuario utilizado para validar la llamada de solicitud.

Tipo: cadena

Obligatorio: sí

password

La contraseña del usuario que solicita las credenciales.

Tipo: cadena

Obligatorio: sí

authMechanism

El método de autenticación para validar a este usuario en el host.

Tipo: cadena

Valores válidos: `ldap`, `linux`, `winnt`

Obligatorio: sí

Sintaxis de la respuesta

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

```
  "accessKeyId": "string",
  "secretAccessKey": "string",
  "sessionToken": "string",
  "region": "edge"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

Los siguientes datos se devuelven en formato JSON.

accessKeyId

El ID de clave de acceso que identifica las credenciales de seguridad temporales.

Restricciones de longitud: longitud mínima de 16. La longitud máxima es de 128.

Patrón: `[\w]*`

secretAccessKey

La clave de acceso secreta que se puede utilizar para firmar las solicitudes.

Tipo: cadena

sessionToken

El token que los usuarios deben pasar a la API de servicio para utilizar las credenciales temporales.

Tipo: cadena

región

La región a la que se dirigen las llamadas a la API.

Tipo: CONSTANT - `edge`

Errores

IllegalArgumentException

La solicitud ha sido rechazada porque el formato del cuerpo del documento proporcionado no era correcto. El mensaje de error describe el error específico.

Código de estado HTTP: 400

AccessDeniedException

El usuario no tiene credenciales válidas basadas en el proveedor de identidad actual. El mensaje de error describe el mecanismo de autenticación.

Código de estado HTTP: 403

TooManyRequestsException

La solicitud ha alcanzado su límite de intentos de autenticación. El mensaje de error contiene la cantidad de tiempo de espera hasta que se realicen nuevos intentos de autenticación.

Código de estado HTTP: 429

Tutorial: Obtener una lista de modelos de activos en una puerta de enlace SiteWise Edge

Puede utilizar un subconjunto de las API de AWS IoT SiteWise disponibles junto con API específicas de periferia para interactuar con sus recursos y modelos de recursos en la periferia. En este tutorial, se explica cómo obtener credenciales temporales para una puerta de enlace AWS IoT SiteWise Edge y cómo obtener una lista de los modelos de activos de la puerta de enlace SiteWise Edge.

Requisitos previos

En los pasos de este tutorial puede utilizar diversas herramientas. Para utilizar estas herramientas, asegúrese de tener instalados los requisitos previos correspondientes.

Necesitará lo siguiente para completar este tutorial:

- Un SiteWise Requisitos de Edge Gateway implementado y en ejecución
- Acceda a su puerta de enlace SiteWise Edge en la misma red a través del puerto 443.
- OpenSSL instalado
- (AWS OpsHubparaAWS IoT SiteWise) La AWS IoT SiteWiseaplicación AWS OpsHub para
- (curl) curl instalado
- (Python) urllib3 instalado
- (Python) Python3 instalado
- (Python) Boto3 instalado

- (Python) BotoCoreinstalado

Paso 1: Obtenga un certificado firmado por el servicio SiteWise Edge Gateway

Para establecer una conexión TLS con las API disponibles en la puerta de enlace SiteWise Edge, necesita un certificado de confianza. Puede generar este certificado mediante OpenSSL AWS OpsHub o for. AWS IoT SiteWise

OpenSSL

> **Note**
>
> Necesita tener instalado OpenSSL para ejecutar este comando.

Abre una terminal y ejecuta el siguiente comando para obtener un certificado firmado desde la puerta de enlace de SiteWise Edge. `<sitewise_gateway_ip>`Sustitúyalo por la IP de la puerta de enlace 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

Puede utilizar AWS OpsHub para AWS IoT SiteWise. Para obtener más información, consulte Administración de puertas de enlace SiteWise perimetrales.

En este tutorial se utiliza la ruta absoluta al certificado de puerta de enlace SiteWise Edge descargado. Ejecute el siguiente comando para exportar la ruta completa de su certificado, sustituyendo `<absolute_path_to_certificate>` por la ruta al certificado:

```
export PATH_TO_CERTIFICATE='<absolute_path_to_certificate>'
```

Paso 2: Obtenga el nombre de host de la puerta de enlace SiteWise Edge

> **Note**
>
> Necesita tener instalado OpenSSL para ejecutar este comando.

Para completar el tutorial, necesitará el nombre de host de su puerta de enlace SiteWise Edge. Para obtener el nombre de host de la puerta de enlace SiteWise Edge, ejecute lo siguiente y sustitúyalo por <sitewise_gateway_ip> la IP de la puerta de enlace SiteWise Edge:

```
openssl s_client -connect <sitewise_gateway_ip>:443 </dev/null 2>/dev/null | grep -Po
 'CN = \K.*'| head -1
```

Ejecute el siguiente comando para exportar el nombre de host para usarlo más adelante y <your_edge_gateway_hostname> sustitúyalo por el nombre de host de su SiteWise puerta de enlace Edge:

```
export GATEWAY_HOSTNAME='<your_edge_gateway_hostname>'
```

Paso 3: Obtenga credenciales temporales para su SiteWise puerta de enlace Edge

Ahora que tiene el certificado firmado y el nombre de host de su puerta de enlace SiteWise Edge, necesita obtener credenciales temporales para poder ejecutar las API en la puerta de enlace. Puede obtener estas credenciales a través de la puerta AWS OpsHub de enlace de SiteWise Edge AWS IoT SiteWise o directamente desde ella mediante las API.

> **Important**
>
> Las credenciales caducan cada 4 horas, por lo que debe obtenerlas justo antes de usar las API de su puerta de enlace SiteWise Edge. No almacene las credenciales en caché durante más de 4 horas.

Obtenga credenciales temporales utilizando AWS OpsHub para AWS IoT SiteWise

> **Note**
>
> Necesita tener instalada la aplicación AWS OpsHub para AWS IoT SiteWise.

Para utilizar la aplicación AWS OpsHub para AWS IoT SiteWise a fin de obtener sus credenciales temporales, haga lo siguiente:

1. Inicie sesión en la aplicación.
2. Elija Configuración.

3. En Autenticación, elija Copiar credenciales.
4. Amplíe la opción que se adapte a su entorno y elija Copiar.
5. Guarde las credenciales para utilizarlas más tarde.

Obtenga credenciales temporales mediante la API de SiteWise Edge Gateway

Para usar la API de puerta de enlace de SiteWise Edge para obtener las credenciales temporales, puede usar un script de Python o un curl, primero necesitará tener un nombre de usuario y una contraseña para su puerta de enlace de SiteWise Edge. Las puertas de enlace SiteWise Edge utilizan la autenticación y la autorización SigV4. Para obtener más información sobre cómo añadir usuarios, consulte LDAP o Grupo de usuarios de Linux. Estas credenciales se utilizarán en los siguientes pasos para obtener las credenciales locales en su puerta de enlace SiteWise Edge que se necesitan para usar las AWS IoT SiteWise API.

Python

> **Note**
>
> Necesita tener urllib3 y Python3 instalados.

Para obtener las credenciales mediante Python

1. Cree un archivo llamado get_credentials.py y copie en él el siguiente código.

```
'''
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. Ejecute get_credentials.py desde el terminal sustituyendo <gateway_username> y <gateway_password> por las credenciales que ha creado.

```
python3 get_credentials.py -e https://$GATEWAY_HOSTNAME -c $PATH_TO_CERTIFICATE
 -u '<gateway_username>' -p '<gateway_password>' -m 'linux'
```

curl

> **Note**
>
> Necesita tener curl instalado.

Para obtener las credenciales mediante curl

1. Ejecute el siguiente comando desde el terminal sustituyendo <gateway_username> y <gateway_password> por las credenciales que ha creado.

```
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 respuesta debe ser similar a la siguiente:

```
{
    "username": "sweuser",
    "accessKeyId": "<accessKeyId>",
    "secretAccessKey": "<secretAccessKey>",
    "sessionToken": "<sessionToken>",
    "sessionExpiryTime": "2022-11-17T04:51:40.927095Z",
    "authMechanism": "linux",
    "role": "edge-user"
}
```

2. Ejecute el siguiente comando desde el terminal.

```
export AWS_ACCESS_KEY_ID=<accessKeyId>
export AWS_SECRET_ACCESS_KEY=<secretAccessKey>
export AWS_SESSION_TOKEN=<sessionToken>
export AWS_REGION=edge
```

Paso 4: Obtenga una lista de los modelos de activos de la puerta de enlace SiteWise Edge

Ahora que tiene un certificado firmado, el nombre de host de la puerta de enlace SiteWise Edge y las credenciales temporales de la puerta de enlace SiteWise Edge, puede usar la `ListAssetModels` API para obtener una lista de los modelos de activos de la puerta de enlace SiteWise Edge.

Python

> **Note**
>
> Necesitas tener instalado Python3 y Boto3. BotoCore

Para obtener la lista de modelos de recursos mediante Python

1. Cree un archivo llamado list_asset_model.py y copie el siguiente código en él.

```
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. Ejecute list_asset_model.py desde el terminal.

```
python3 list_asset_model.py
```

curl

> **Note**
>
> Necesita tener curl instalado.

Para obtener la lista de modelos de recursos mediante curl

Ejecute el siguiente comando desde el terminal.

```
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 respuesta debe ser similar a la siguiente:

```
{
    "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 y restauración de gateways SiteWise Edge

En este tema se explica cómo restaurar las puertas de enlace de SiteWise Edge y hacer copias de seguridad de los datos métricos. Si tiene problemas con una puerta de enlace SiteWise Edge averiada en la misma máquina y necesita solucionar el problema, lea la AWS IoT SiteWise documentación Solución de problemas con la puerta de enlace SiteWise Edge.

> **Note**
>
> La guía que se trata en este tema es para las puertas de enlace SiteWise Edge instaladas en la AWS IoT Greengrass V2 versión 2.1.0 o superior.

Copias de seguridad diarias de los datos de métricas

Crear una copia de seguridad es importante si desea transferir o restaurar los datos en una nueva máquina. Hacer una copia de seguridad de sus datos reduce en gran medida el riesgo de pérdida de datos operativos durante un proceso de transferencia o restauración.

La ruta de la carpeta influxdb es la siguiente:

Linux

```
/greengrass/v2/work/aws.iot.SiteWiseEdgeProcessor/influxdb
```

Windows

```
C:\greengrass\v2\work\aws.iot.SiteWiseEdgeProcessor\influxdb
```

Le recomendamos que haga una copia de seguridad de toda la carpeta con todo lo que contenga.

Le recomendamos que haga copias de seguridad periódicas de sus datos métricos desde la versión 1.0 SiteWise Edge en un disco duro externo o en la AWS nube.

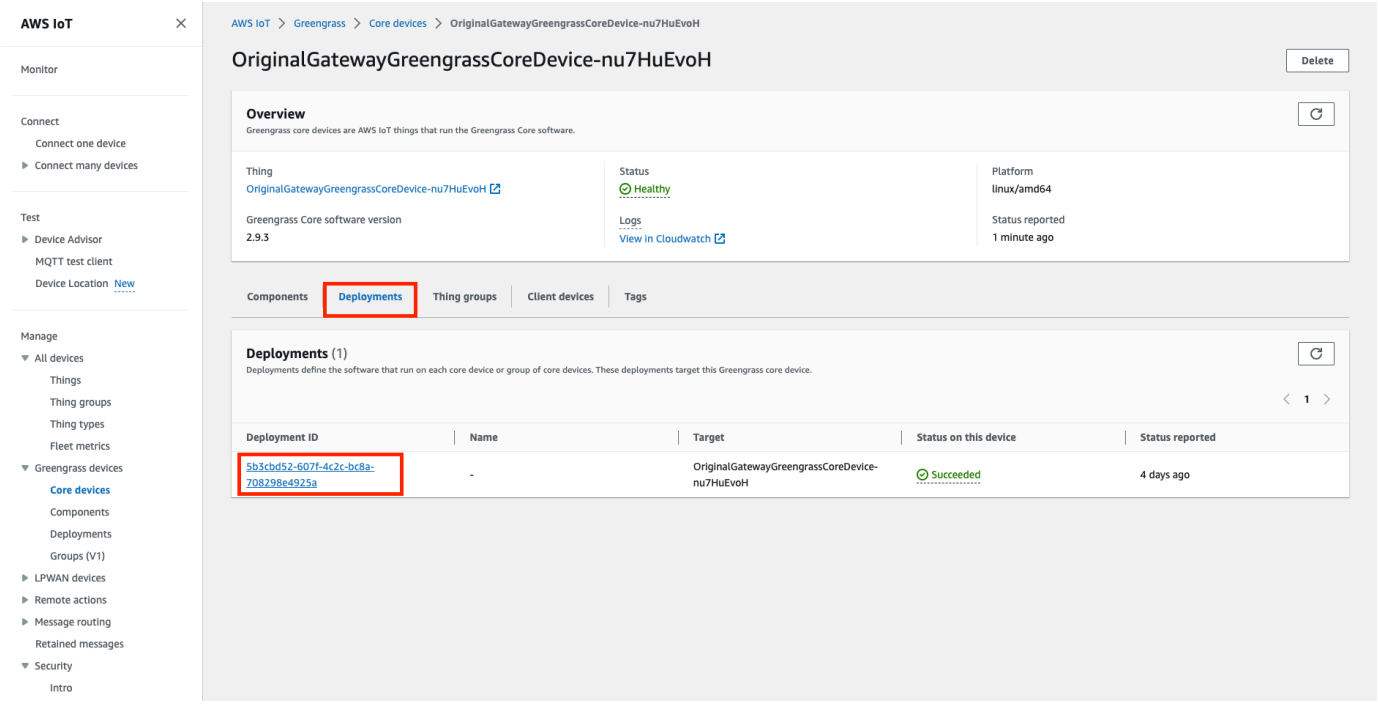
Restaure una puerta de enlace SiteWise Edge

Utilice el siguiente procedimiento para restaurar una puerta de enlace SiteWise Edge:

1. Utilice el script de instalación descargado al crear la puerta de enlace SiteWise Edge para restaurar la puerta de enlace SiteWise Edge en la nueva máquina. Lea el procedimiento de instalación del software de puerta de enlace SiteWise Edge en su dispositivo local para configurar la puerta de enlace SiteWise Edge.

   Si hubiera perdido o no pudiera encontrar el script de instalación, póngase en contacto con el servicio de atención al cliente de AWS.
2. Una vez instalada la puerta de enlace SiteWise Edge, inicie sesión en la AWS IoT Greengrass consola.

3. Para volver a implementar los componentes, vaya a Administrar y, a continuación, en Dispositivos AWS IoT Greengrass , seleccione Dispositivos centrales.
4. En la tabla de dispositivos AWS IoT Greengrass principales, seleccione el dispositivo principal correspondiente a su puerta de enlace SiteWise Edge.
5. Una vez en la página de dispositivos, abra la pestaña Implementaciones y seleccione su ID de implementación. Esto abre la página Implementaciones con su ID seleccionado.



6. Una vez en la página Implementaciones, en la parte superior derecha pulse el botón Acciones y seleccione la opción Revisar para iniciar una nueva implementación. Configure la implementación. Si desea mantener la implementación tal como está, pase a Revisar y Desplegar.
7. Espere a que el Estado de la implementación cambie a `Completed`.

> **Note**
>
> Además, todos los componentes del SiteWise Edge tardarán unos minutos en configurarse y funcionar por completo.

Restaure AWS IoT SiteWise los datos

Utilice el siguiente procedimiento para restaurar los datos en una máquina nueva.

1. Copie la carpeta `influxdb` en la nueva máquina.
2. Detenga el SiteWise EdgeProcessor componente ejecutando el siguiente comando en su terminal:

   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. Localice la ruta en la que realizó la copia de seguridad de los datos y ejecute el siguiente 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. Reinicie el SiteWiseEdgeProcessor componente:

   Linux

   ```
   sudo /greengrass/v2/bin/greengrass-cli component restart -n
   aws.iot.SiteWiseEdgeProcessor
   ```

Windows

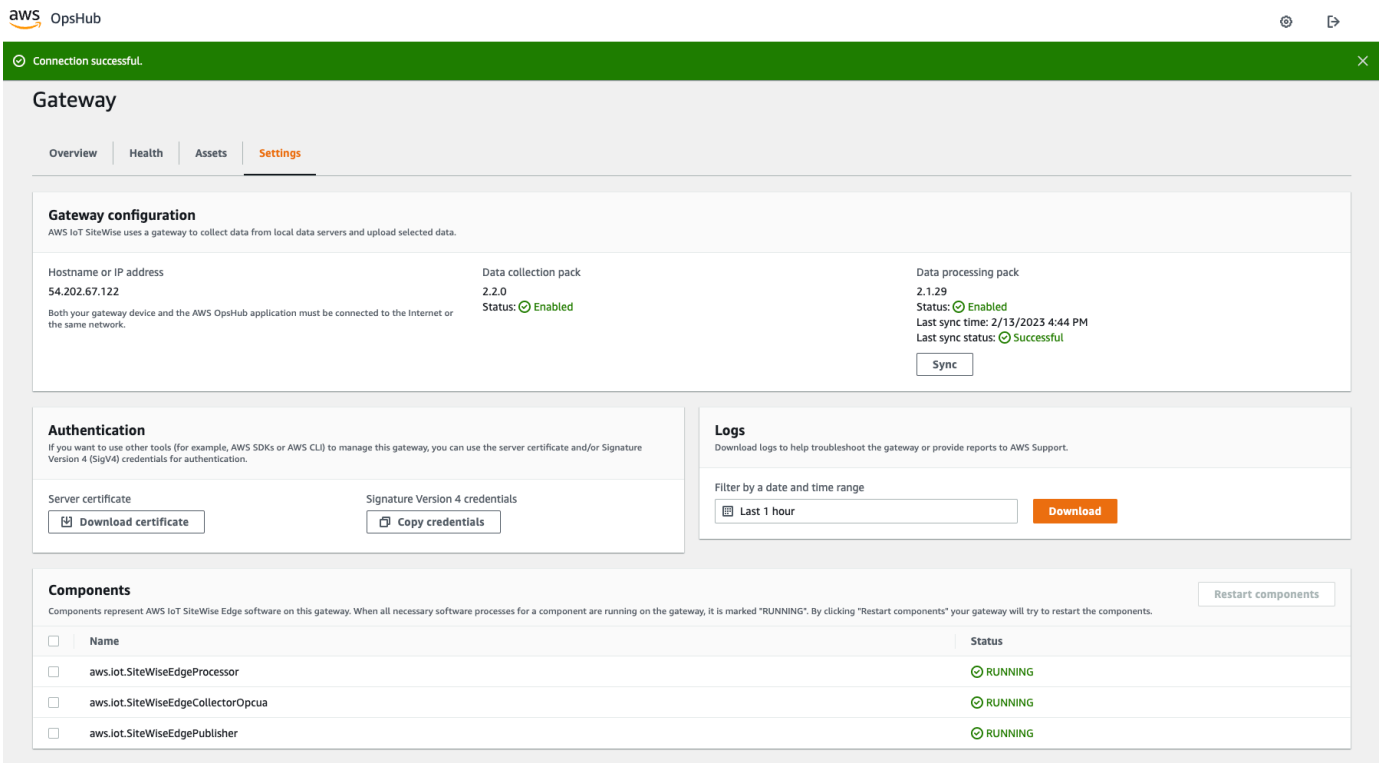
```
C:\greengrass\v2\bin\greengrass-cli component restart -n
aws.iot.SiteWiseEdgeProcessor
```

Validación de copias de seguridad y restauraciones correctas

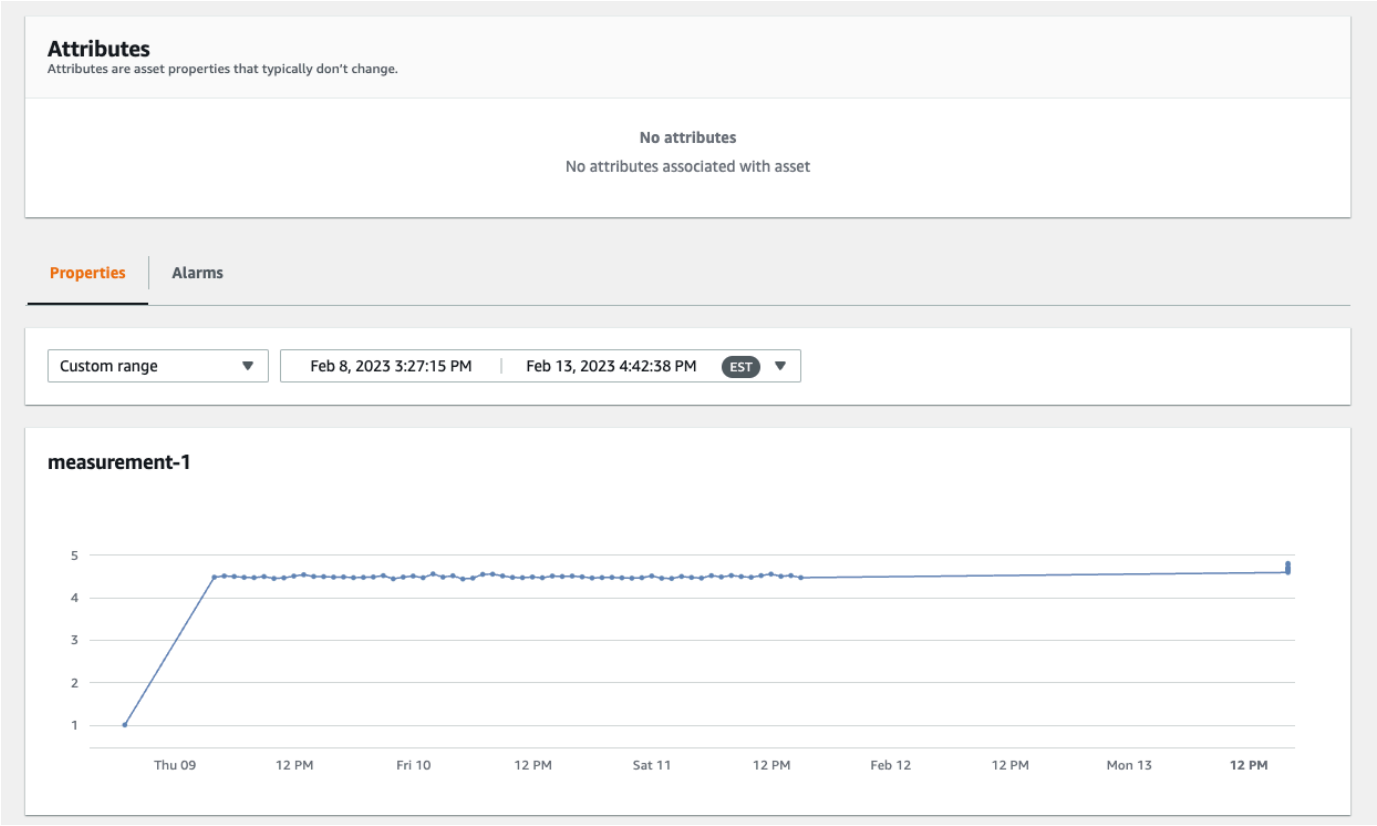
Utilice este procedimiento para validar los datos respaldados y las restauraciones de la puerta de enlace Edge. SiteWise

> **Note**
>
> Este procedimiento requiere que haya instalado para. AWS OpsHub AWS IoT SiteWise Para obtener más información, consulte Administración de puertas de enlace SiteWise Edge mediante AWS OpsHub for AWS IoT SiteWise.

1. Abierto AWS OpsHub para. AWS IoT SiteWise
2. En la página de configuración de SiteWise Edge Gateway, compruebe el estado de cada componente que aparece en la tabla de componentes. Compruebe que el color del estado sea verde y que la lectura indique RUNNING.



3. Valide los datos pasados en el panel de control del portal para comprobar que tanto los datos pasados como los nuevos estén configurados correctamente. Habrá un tiempo de inactividad entre los datos pasados y nuevos. Debería esperar ver un periodo en el que no se recopilaran puntos de datos.



Si tiene problemas al realizar una copia de seguridad o restaurar una puerta de enlace SiteWise Edge, consulte los siguientes temas de solución de problemas: Solución de problemas de una puerta de enlace AWS IoT SiteWise Edge.

Configuración de puertas de enlace SiteWise Edge ()AWS IoT Greengrass Version 1

> **Note**
>
> SiteWise Las puertas de enlace perimetrales que se ejecutan solo AWS IoT Greengrass V1 están disponibles si comenzó a usar esta función antes del 29 de julio de 2021. De lo contrario, debe configurar las puertas de enlace SiteWise Edge que se ejecuten en. AWS IoT Greengrass V2

Puede enviar datos industriales AWS IoT SiteWise mediante una puerta de enlace SiteWise Edge para cargar datos desde equipos industriales. La puerta de enlace SiteWise Edge sirve

de intermediario entre AWS IoT SiteWise sus equipos industriales de datos. AWS IoT SiteWise proporciona AWS IoT Greengrass componentes que puede implementar en cualquier dispositivo que pueda funcionar AWS IoT Greengrass para configurar una puerta de enlace SiteWise Edge. AWS IoT SiteWise admite la vinculación con el protocolo de servidor OPC-UA.

Si tiene puertas de enlace AWS IoT SiteWise Edge que se ejecuten AWS IoT Greengrass V1, puede actualizar sus puertas de enlace SiteWise Edge a. AWS IoT Greengrass V2 Para obtener más información, consulte las instrucciones para actualizar las puertas de enlace SiteWise Edge de a. AWS IoT Greengrass V1 AWS IoT Greengrass V2

Temas

Elegir un dispositivo de puerta de enlace AWS IoT Greengrass V1 SiteWise Edge

Elija el dispositivo local que mejor se adapte a su operación industrial. Puede configurar una puerta de enlace SiteWise Edge en cualquier dispositivo que pueda funcionar AWS IoT Greengrass. Todos los dispositivos locales deben cumplir los siguientes requisitos:

- Es compatible con el software AWS IoT Greengrass Core v1.10.2 o posterior. Para obtener más información, consulte Plataformas admitidas y requisitos en la Guía para desarrolladores de AWS IoT Greengrass Version 1 .
- Tiene al menos 4 GB de RAM.
- Tiene al menos 10 GB de espacio libre en disco.
- Admite una máquina virtual Java 8 (JVM).

Si planea procesar datos de forma perimetral AWS IoT SiteWise, su dispositivo local también debe cumplir los siguientes requisitos:

- Tener un procesador x86 de 64 bits y cuatro núcleos.
- Tener al menos 16 GB de RAM.

- Tiene al menos 32 GB de RAM si utiliza Windows.
- Tener al menos 256 GB de espacio libre en disco.

El espacio en disco necesario para almacenar en caché los datos para una conectividad a Internet intermitente depende de los siguientes factores:

- Número de flujos de datos cargados
- Puntos de datos por flujo de datos por segundo
- Tamaño de cada punto de datos
- Velocidades de comunicación
- Tiempo de inactividad de red esperado

La capacidad de cómputo necesaria para sondear y cargar los datos depende de los siguientes factores:

- Número de flujos de datos cargados
- Puntos de datos por flujo de datos por segundo

Configuración de una puerta de enlace AWS IoT Greengrass V1 SiteWise Edge

Una puerta de enlace AWS IoT SiteWise Edge sirve de intermediario entre su equipo industrial y AWS IoT SiteWise. Puede implementar el software de puerta de enlace SiteWise Edge en cualquier dispositivo que pueda funcionar AWS IoT Greengrass. Para obtener más información, consulte Elegir un dispositivo de puerta de enlace AWS IoT Greengrass V1 SiteWise Edge.

Puede AWS IoT SiteWise habilitar el procesamiento de datos de forma local en sus dispositivos Edge mediante el paquete de procesamiento de datos de su puerta de enlace SiteWise Edge. Para ello, añada su puerta de enlace SiteWise Edge a AWS IoT SiteWise. Para obtener más información sobre el procesamiento de datos en la periferia, consulte the section called “Habilitación del procesamiento de datos de la periferia”.

> **Note**
>
> Le recomendamos que complete los siguientes pasos junto a alguien que tenga acceso informático de administrador a sus redes local y corporativa. Estos pasos pueden requerir

que alguien que conozca tu equipo industrial y esté autorizado a configurar los ajustes del firewall.

Temas

- Configuración del entorno de puerta de enlace SiteWise Edge
- Creación de una política de IAM y un rol
- Configuración de un grupo AWS IoT Greengrass
- Configuración del AWS IoT SiteWise conector
- Añadir la puerta de enlace SiteWise Edge a AWS IoT SiteWise

Configuración del entorno de puerta de enlace SiteWise Edge

En este procedimiento, debe instalar AWS IoT Greengrass y configurar la puerta de enlace SiteWise Edge para usarla con AWS IoT SiteWise.

> **Note**
>
> Esta sección incluye instrucciones para instalar paquetes mediante el comando de `apt`. Esto es aplicable a sistemas que ejecutan Ubuntu o similar. Si no utiliza un sistema similar, consulte la documentación de su distribución y utilice el instalador de paquetes recomendado.

Para configurar la puerta de enlace SiteWise Edge

1. Según corresponda, modifique la configuración de la BIOS de la puerta de enlace SiteWise Edge de la siguiente manera.
   a. Asegúrese de que la puerta de enlace SiteWise Edge se reinicie automáticamente después de un posible corte de energía, si corresponde.
   b. Asegúrese de que la puerta de enlace SiteWise Edge no hiberne ni duerma, si corresponde.
2. Asegúrese de que la puerta de enlace SiteWise Edge se conecte a Internet.
3. (Opcional) Para usar la puerta de enlace SiteWise Edge sin el ratón, el teclado y el monitor, realice los siguientes pasos para configurarla `ssh` en la puerta de enlace SiteWise Edge:

a. Si aún no ha instalado el paquete SSH, ejecute el siguiente comando.

```
sudo apt install ssh
```

b. Ejecute el siguiente comando de la .

```
service ssh status
```

c. Busque `Active: active (running)` en el resultado para confirmar que el servidor SSH se esté ejecutando.

d. Pulse Q para salir.

Ejecute el siguiente comando para usar SSH para conectarse a la puerta de enlace SiteWise Edge desde otra computadora. Sustituya el *`nombre`* de usuario por el nombre de usuario y la *`IP`* por la dirección IP de la puerta de enlace SiteWise Edge.

```
ssh username@IP
```

Puede utilizar el argumento `-p` *`port-number`* para conectarse a un puerto distinto del puerto predeterminado 22.

4. Descargue e instale el software AWS IoT Greengrass Core v1.10.2 o posterior y cree un AWS IoT Greengrass grupo para su puerta de enlace SiteWise Edge. Para ello, siga las instrucciones de Introducción a AWS IoT Greengrass en la Guía del desarrollador de AWS IoT Greengrass .

   Le recomendamos que ejecute el script de configuración del dispositivo de AWS IoT Greengrass para comenzar rápidamente. Si quieres revisar AWS IoT Greengrass los requisitos y los procesos con más detenimiento, puedes seguir los pasos del Módulo 1 y el Módulo 2 para configurarlos. AWS IoT Greengrass

   > **Important**
   >
   > Revise las AWS regiones en las que AWS IoT SiteWise está disponible. Cuando elijas una región AWS IoT Greengrass, asegúrate de que la región también sea compatible AWS IoT SiteWise. De lo contrario, no podrás conectar tu puerta de enlace SiteWise Edge a AWS IoT SiteWise.

Antes de continuar con el siguiente paso, debes tener instalado el software AWS IoT Greengrass Core en tu puerta de enlace SiteWise Edge.

5. Ejecute los siguientes comandos para instalar Java 8.

```
sudo apt update
      sudo apt install openjdk-8-jre
```

El software de puerta de enlace SiteWise Edge que se instala más adelante en esta guía utiliza un entorno de ejecución de Java 8.

6. Ejecute los siguientes comandos para comprobar que Java se ha instalado correctamente.

```
java -version
```

7. El software AWS IoT Greengrass Core asume un `java8` directorio. Ejecute el siguiente comando para vincular su instalación de Java a ese directorio de `java8`.

```
sudo ln -s /usr/bin/java /usr/bin/java8
```

8. Ejecute el siguiente comando para crear un directorio de `/var/sitewise` datos y conceder los `ggc_user` permisos para ese directorio. AWS IoT SiteWise almacena los datos en este directorio. Creó el `ggc_user` al configurarlo AWS IoT Greengrass anteriormente en este procedimiento.

```
sudo mkdir /var/sitewise
      sudo chown ggc_user /var/sitewise
      sudo chmod 700 /var/sitewise
```

`/var/sitewise`Es el directorio predeterminado que AWS IoT SiteWise utiliza. Puede personalizar la ruta del directorio (por ejemplo, `/var/sitewise` reemplazarla por`/var/`*`custom`*`/`*`path`*`/`), pero hacerlo requiere pasos adicionales una vez creada la puerta de enlace SiteWise Edge. Para obtener más información, consulte el paso 6 en Configuración del AWS IoT SiteWise conector.

9. Si es necesario, pida al administrador de TI que añada los siguientes puntos de conexión y puertos a la lista blanca de la red local:

   - Puertos 443, 8443 y 8883.

> **Important**
>
> Puede configurar AWS IoT Greengrass Core para que use solo el puerto 443 para todas las comunicaciones de red. Para obtener más información, consulte esta sección acerca de cómo conectarse utilizando el puerto 443 o a través de un proxy de red en la Guía del desarrollador de AWS IoT Greengrass .

- La dirección IP de su puerta de enlace SiteWise Edge (puerto 443). Para obtener la dirección IP, ejecute el comando `ip address` o `ifconfig` y anote el valor de `inet` (como `203.0.113.0`).
- El punto final de AWS IoT SiteWise datos: `data.iotsitewise.`*`region`*`.amazonaws.com` (puerto 443).
- Los siguientes AWS puntos finales que utiliza la puerta de enlace SiteWise Edge. Puede encontrarlos en el archivo `/`*`greengrass-root`*`/config/config.json`. Reemplace *`greengrass-root`* por el directorio raíz de su instalación de AWS IoT Greengrass .
  - ggHost: `greengrass-ats.iot.`*`region`*`.amazonaws.com` (puertos 443, 8443 y 8883).
  - iotHost: *`prefix`*`-ats.iot.`*`region`*`.amazonaws.com` (puertos 443, 8443 y 8883).

  Para obtener más información, consulte Puntos de conexión y cuotas de AWS IoT Greengrass.

10. Si el software AWS IoT Greengrass Core aún no se está ejecutando, ejecute el siguiente comando para iniciar el software AWS IoT Greengrass Core. Sustituya *`greengrass-root`* por la raíz de la instalación. AWS IoT Greengrass El directorio *`greengrass-root`* predeterminado es `/greengrass`.

    ```
    cd /greengrass-root/ggc/core
          sudo ./greengrassd start
    ```

    Debería ver este mensaje: `Greengrass successfully started with PID:` *`some-PID-number`*

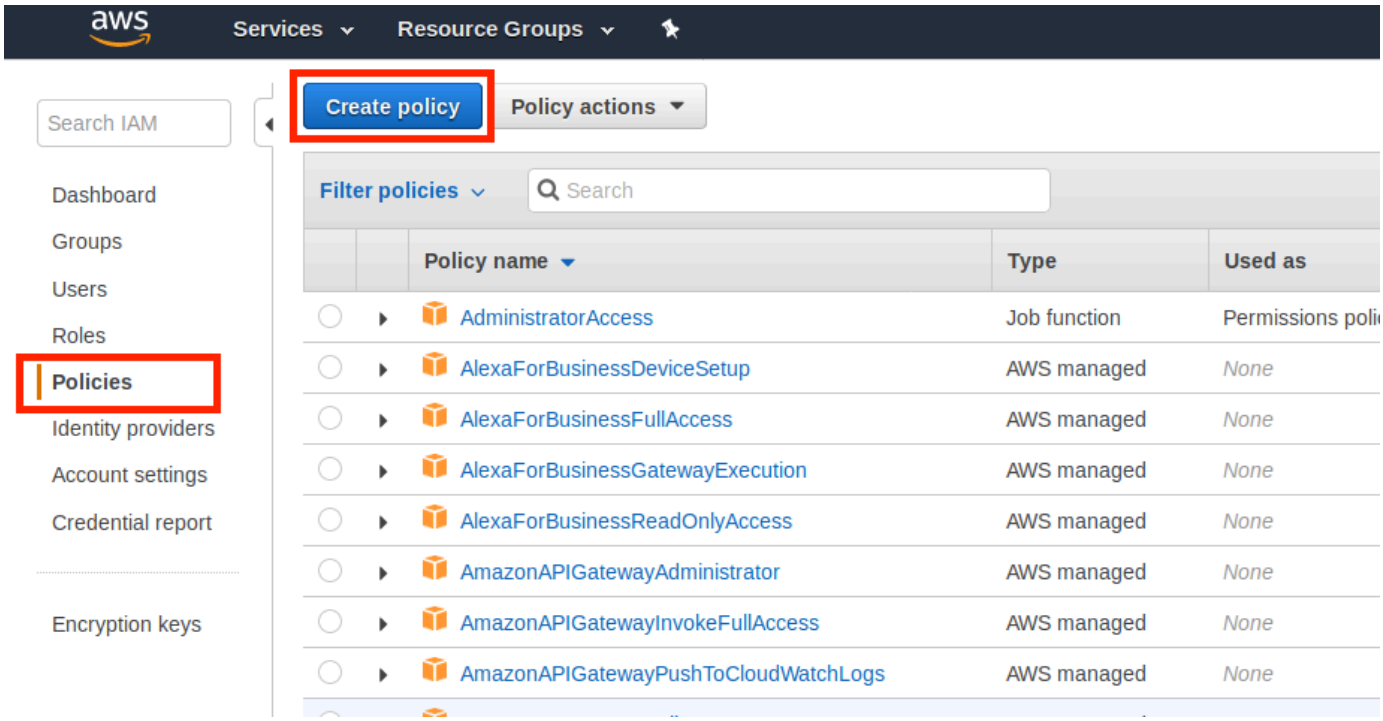
11. Configura el software AWS IoT Greengrass Core para que se inicie automáticamente cuando se encienda la puerta de enlace SiteWise Edge. Consulte la documentación del sistema operativo de su puerta de enlace SiteWise Edge.

Creación de una política de IAM y un rol

Debe crear una política y un rol AWS Identity and Access Management (de IAM) para permitir que la puerta de enlace de SiteWise Edge acceda AWS IoT SiteWise en su nombre.

Para crear una política y un rol de IAM

1. Vaya a la consola de IAM.
2. En el panel de navegación, seleccione Políticas y, a continuación, Crear política.



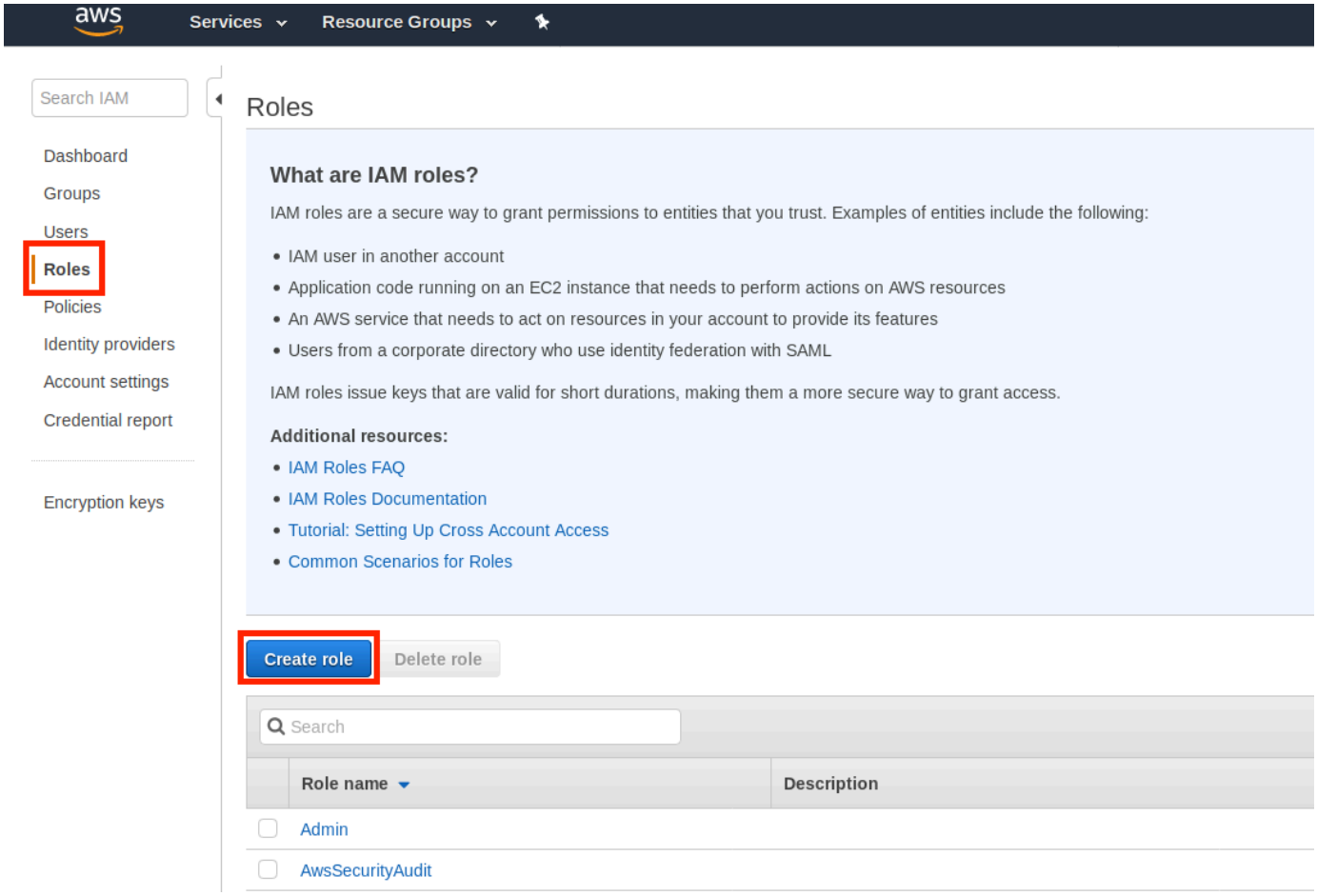
3. En la pestaña JSON, elimine el contenido actual del campo de política y pegue la siguiente política en el campo.

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

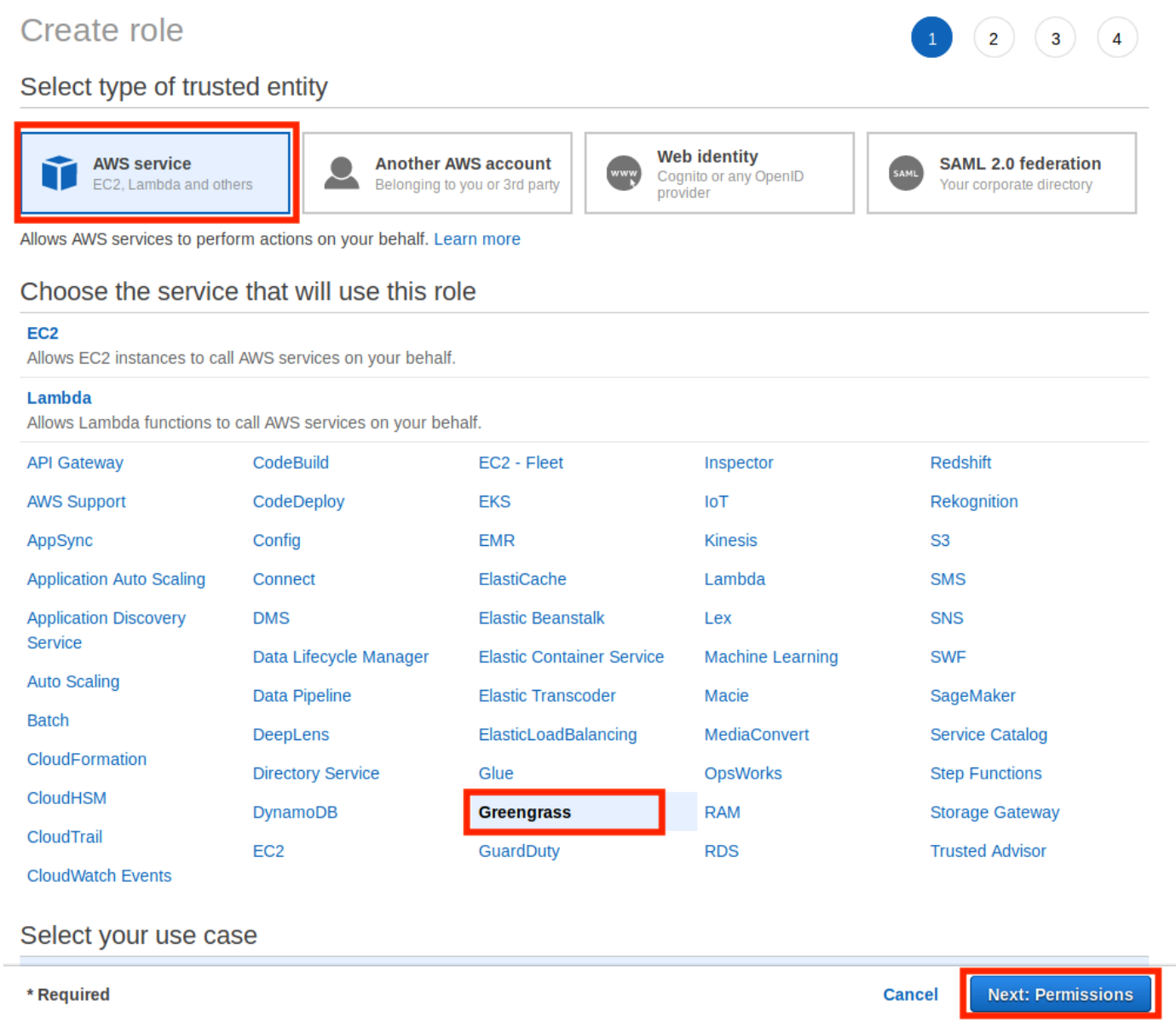
> **Note**
>
> Para mejorar la seguridad, puedes especificar una ruta jerárquica de AWS IoT SiteWise activos en la `Condition` propiedad. El siguiente ejemplo es una política de confianza que especifica una ruta jerárquica de activos.

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

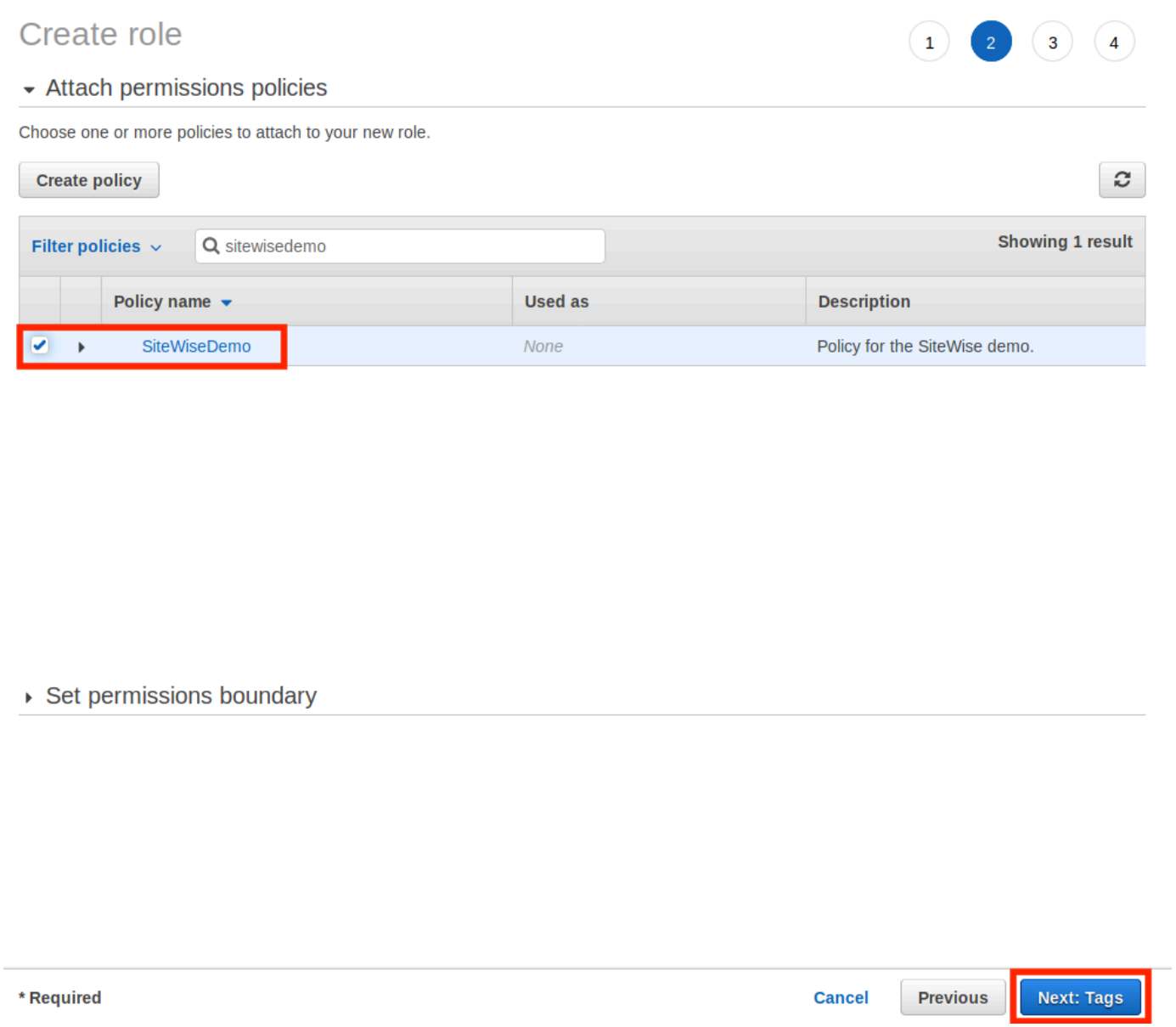
4. Elija Revisar política.
5. Escriba un nombre y una descripción para la política y, a continuación, elija Crear política.
6. En el panel de navegación, seleccione Roles y, a continuación, Crear rol.



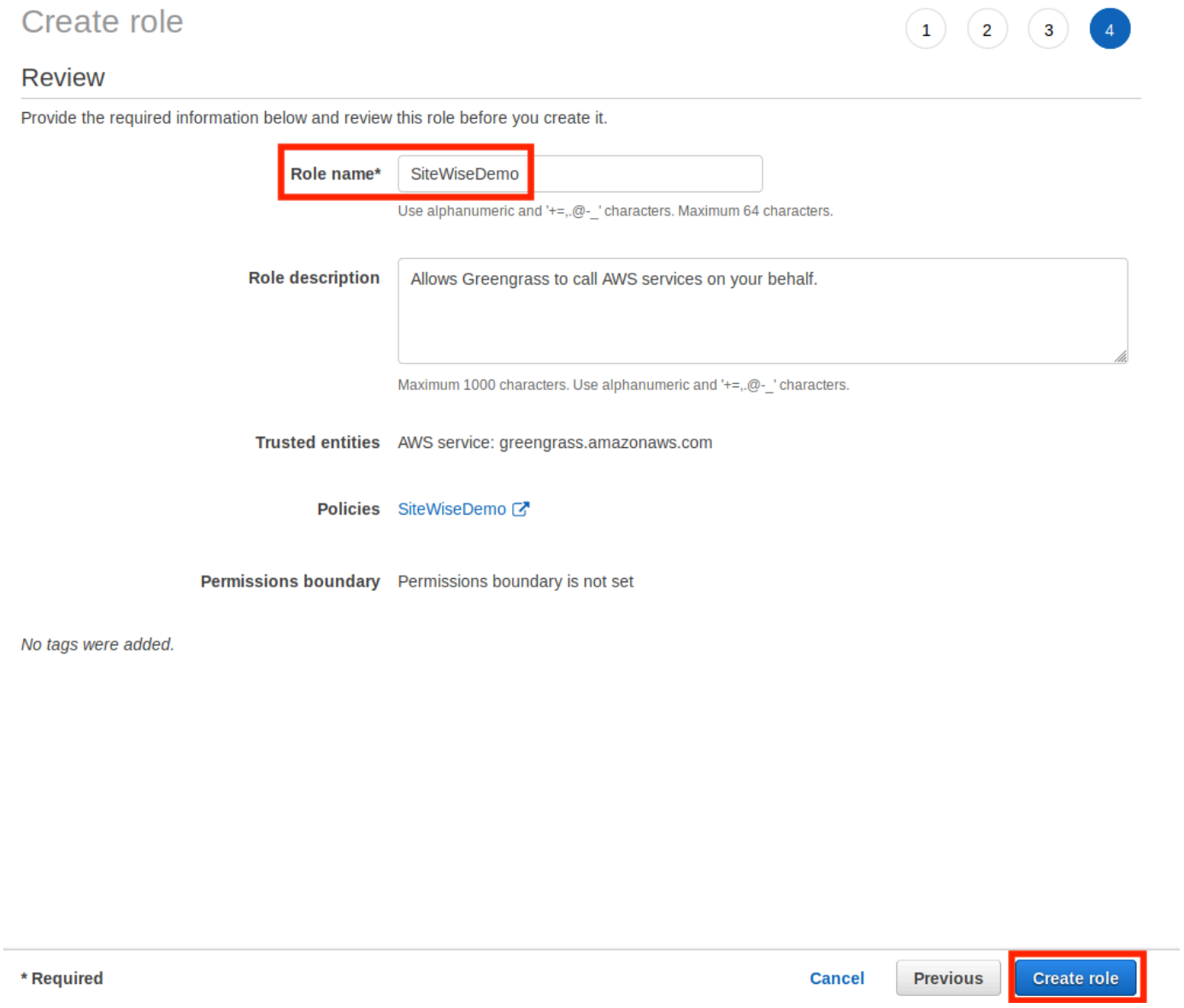
7. En Seleccionar tipo de entidad de confianza, seleccione Servicio de AWS . En Elegir el servicio que utilizará el rol, seleccione Greengrass como el servicio que utilizará el rol y, a continuación, Siguiente: Permisos.



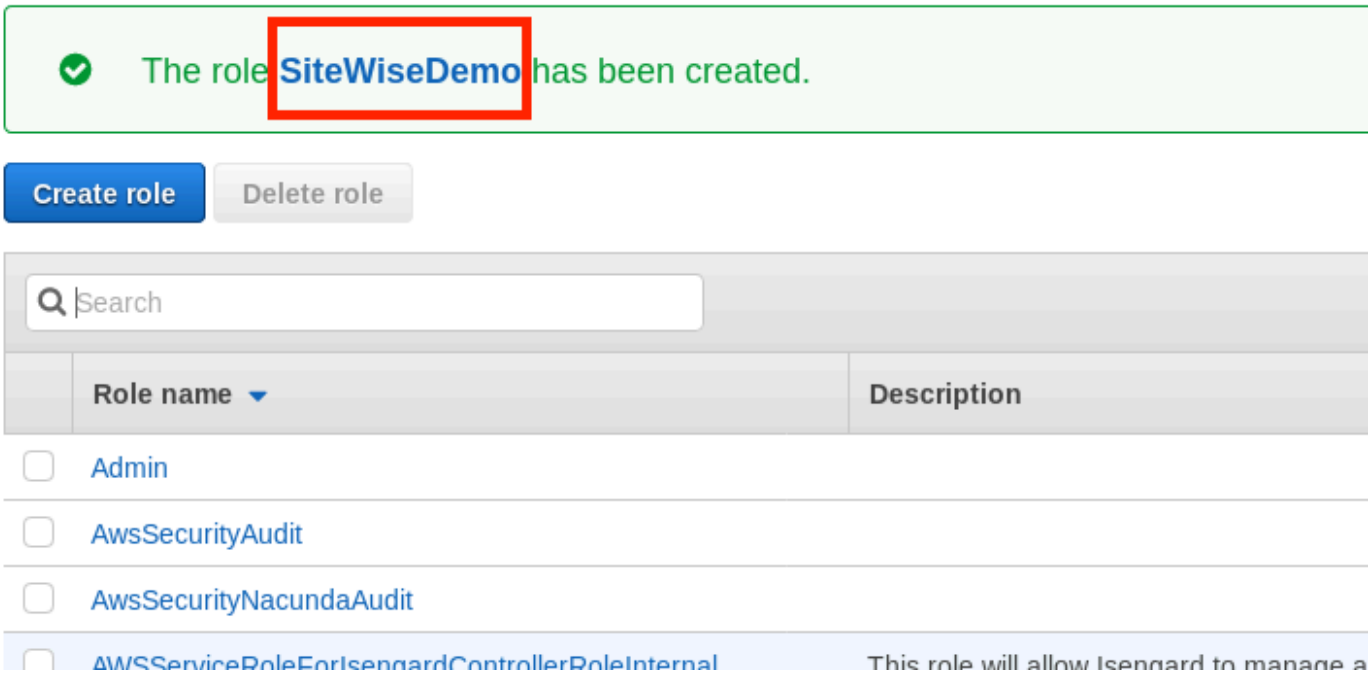
8. Busque la política que ha creado, seleccione la casilla de verificación y, a continuación, seleccione Siguiente: Etiquetas.



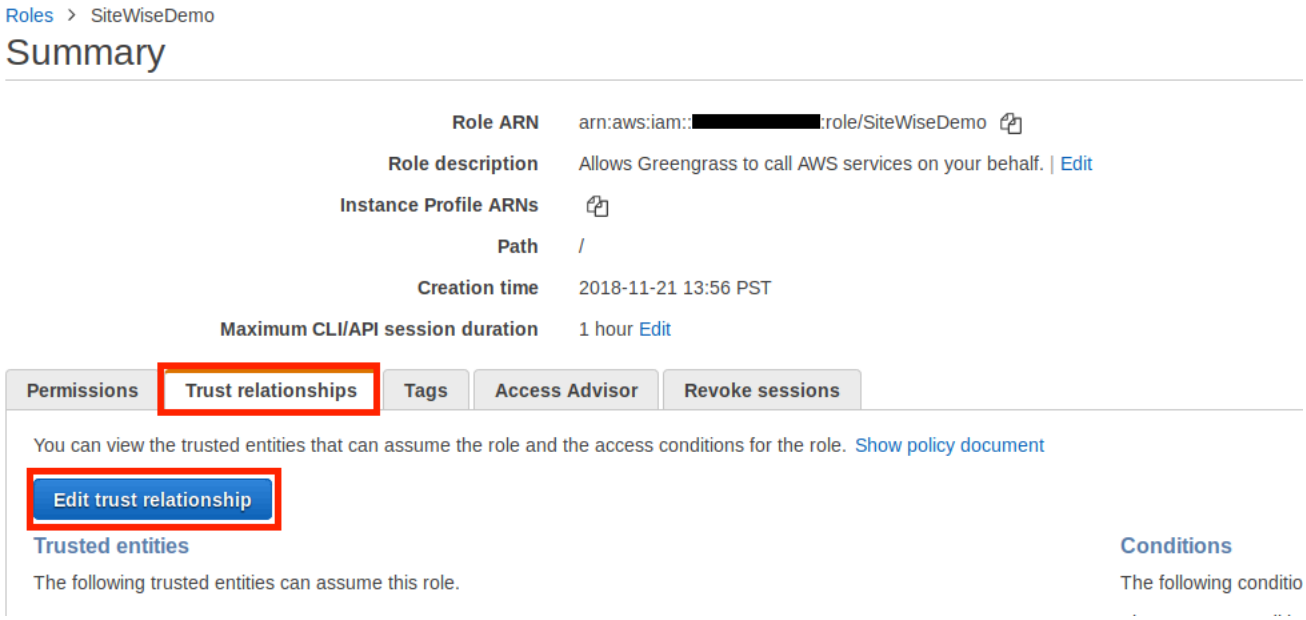
9. (Opcional) Añada etiquetas al rol y, a continuación, seleccione Siguiente: Revisar.
10. Escriba un nombre y una descripción para el rol y, a continuación, seleccione Crear rol.



11. En el banner verde, seleccione el enlace a su nuevo rol. También puede utilizar el campo de búsqueda para buscar el rol.



12. Elija la pestaña Relaciones de confianza y, a continuación, Editar relación de confianza.



13. Sustituya el contenido actual del campo de la política por lo siguiente y, a continuación, seleccione Actualizar política de confianza.

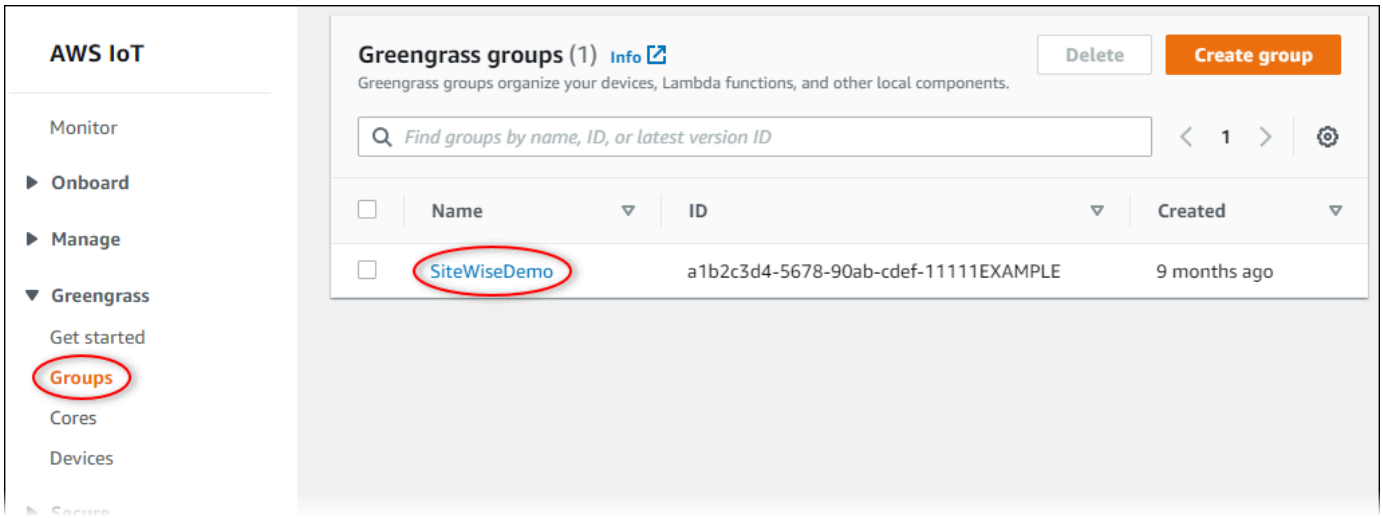
```
{
        "Version": "2012-10-17",
        "Statement": [
          {
            "Effect": "Allow",
```

```
            "Principal": {
              "Service": "greengrass.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
          }
        ]
      }
```

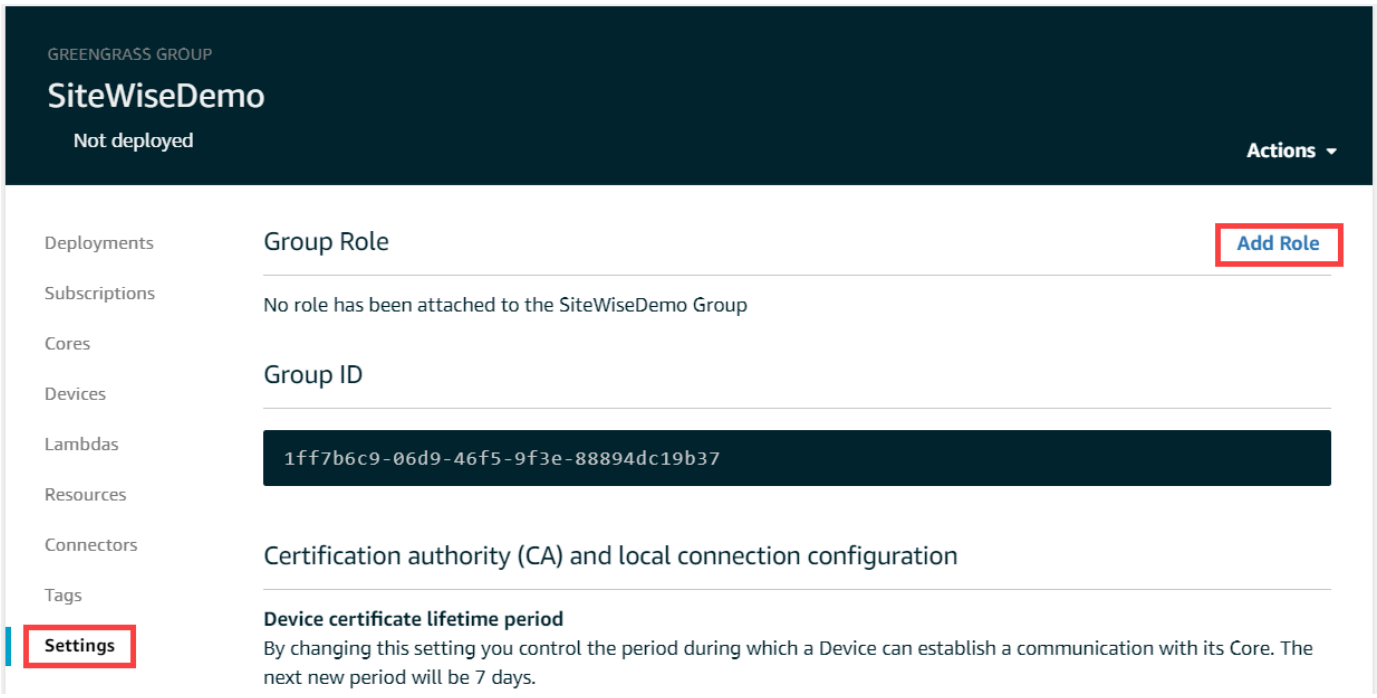
Configuración de un grupo AWS IoT Greengrass

Para asociar un rol de IAM a un grupo y habilitar el administrador de flujos

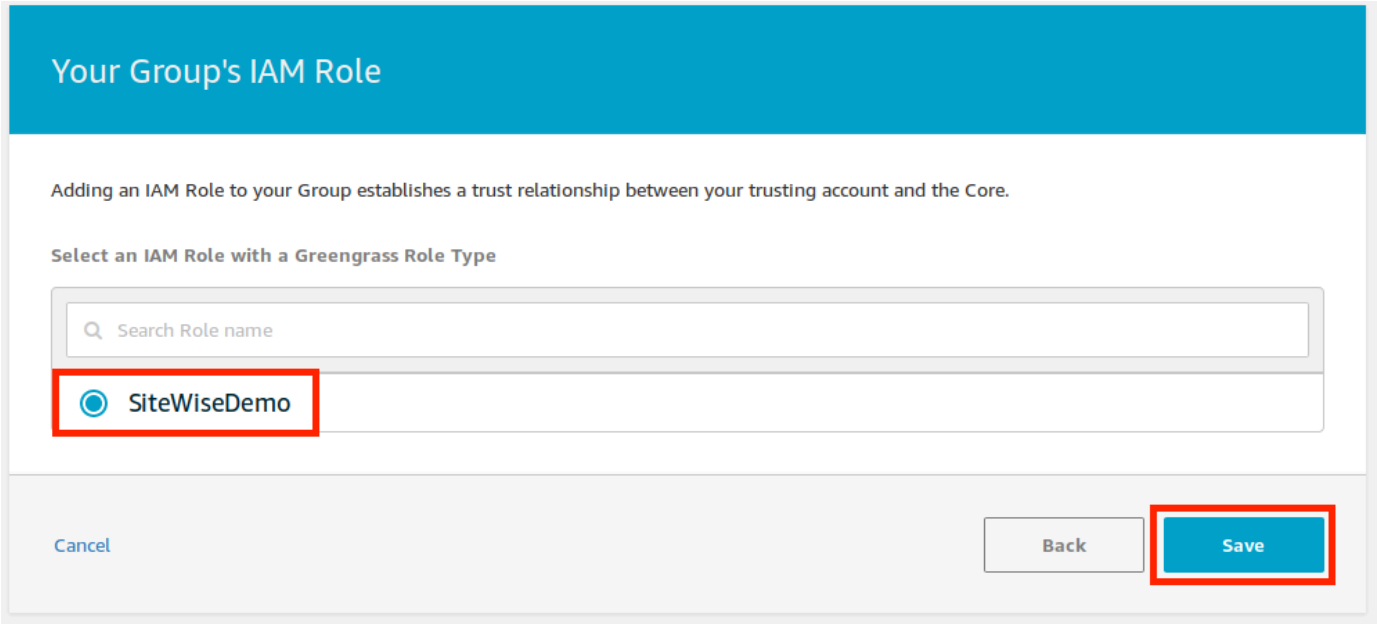
1. Vaya a la consola de AWS IoT Greengrass.
2. En el panel de navegación izquierdo, en Greengrass, elija Grupos y, a continuación, elija el grupo que creó en Configuración del entorno de puerta de enlace SiteWise Edge.



3. En el panel de navegación izquierdo, elija Configuración. En la sección Rol de grupo elija Añadir rol.



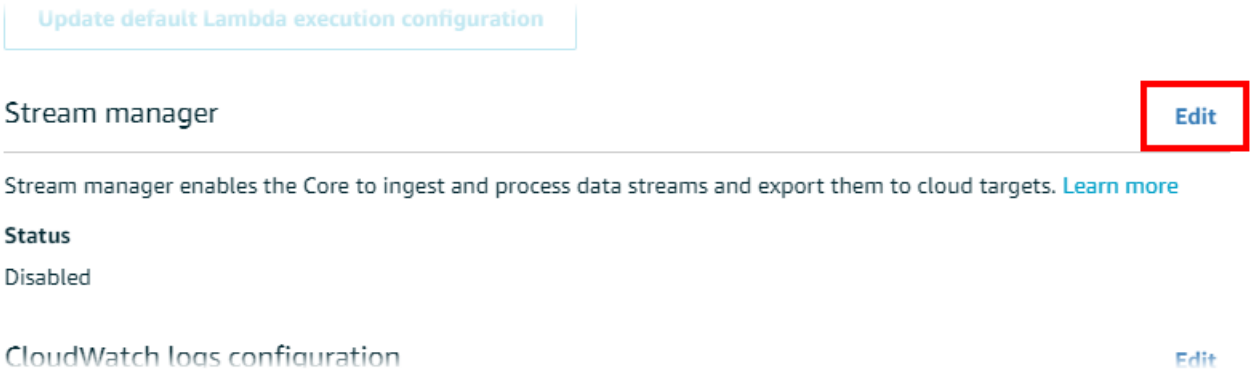
4. Elija el rol que creó en Creación de una política de IAM y un rol y, a continuación, seleccione Guardar.



5. En la página Ajustes, en la sección Administrador de secuencias elija Editar.

   El administrador de transmisiones es una función AWS IoT Greengrass que permite a su AWS IoT Greengrass núcleo transmitir datos a la AWS nube. SiteWise Las pasarelas perimetrales requieren que el administrador de transmisiones esté habilitado. Para obtener más información,

consulte Administrar flujos de datos en el AWS IoT Greengrass núcleo de la Guía para AWS IoT Greengrass Version 1 desarrolladores.



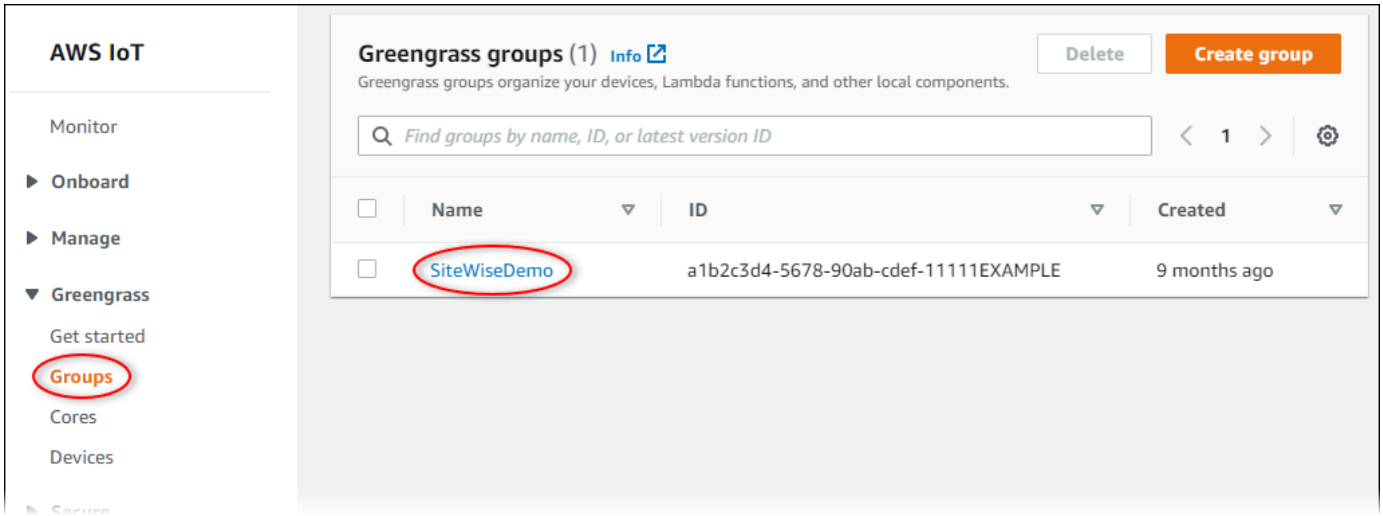
6. Seleccione Habilitado y, a continuación, elija Guardar.
7. En la esquina superior izquierda, seleccione Servicios para prepararse para el siguiente procedimiento.

Configuración del AWS IoT SiteWise conector

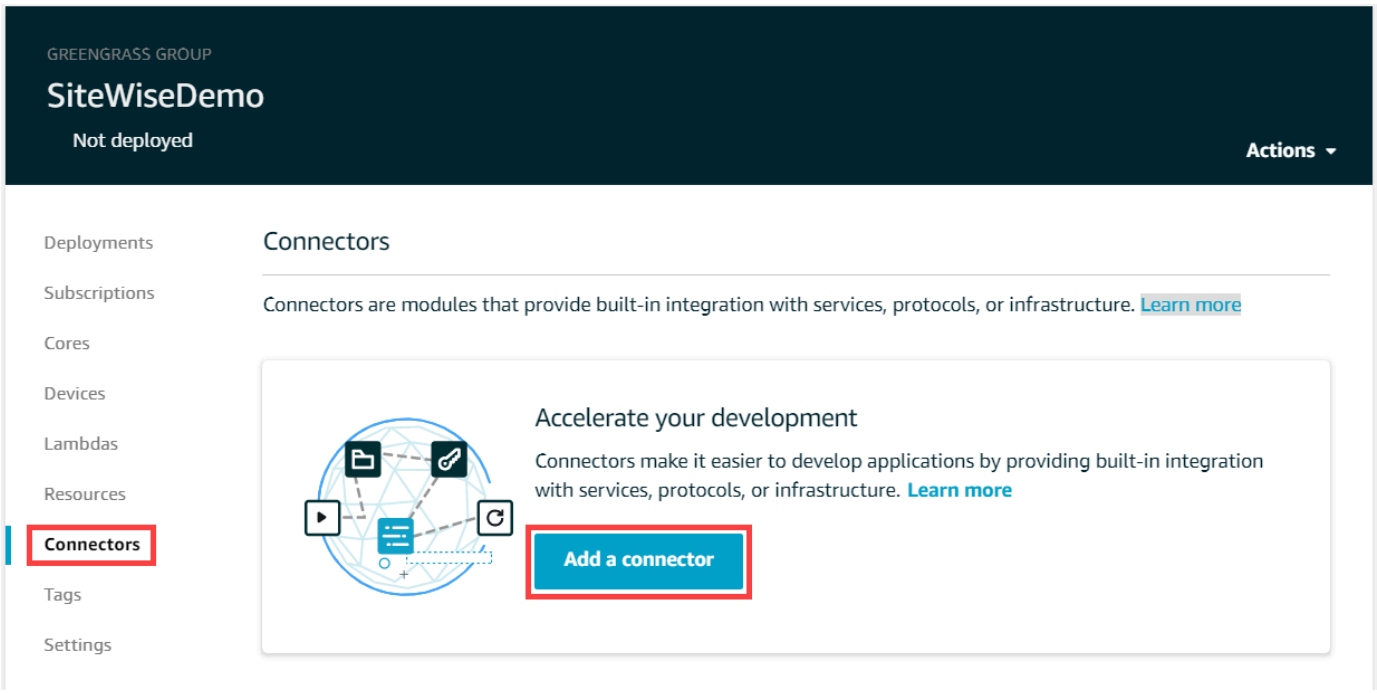
En este procedimiento, configurará el AWS IoT SiteWise conector en su grupo de Greengrass. Los componentes son módulos prediseñados que aceleran el ciclo de vida del desarrollo en escenarios perimetrales comunes. Para obtener más información, consulte Conectores AWS IoT Greengrass en la Guía para desarrolladores de AWS IoT Greengrass Version 1 .

Para configurar el conector AWS IoT SiteWise

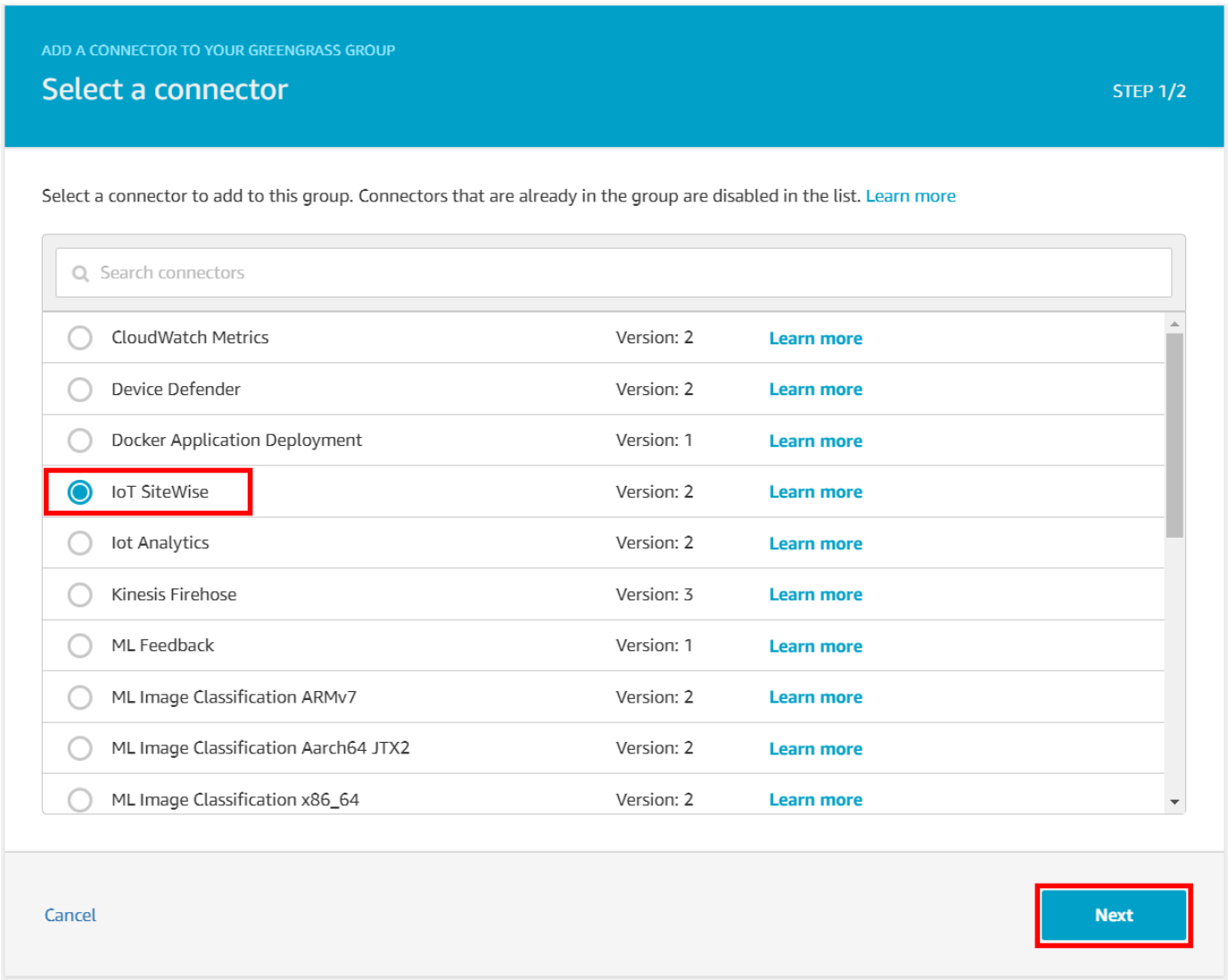
1. Vaya a la consola de AWS IoT Greengrass.
2. En el panel de navegación izquierdo, en Greengrass, elija Grupos y, a continuación, elija el grupo que creó en Configuración del entorno de puerta de enlace SiteWise Edge.



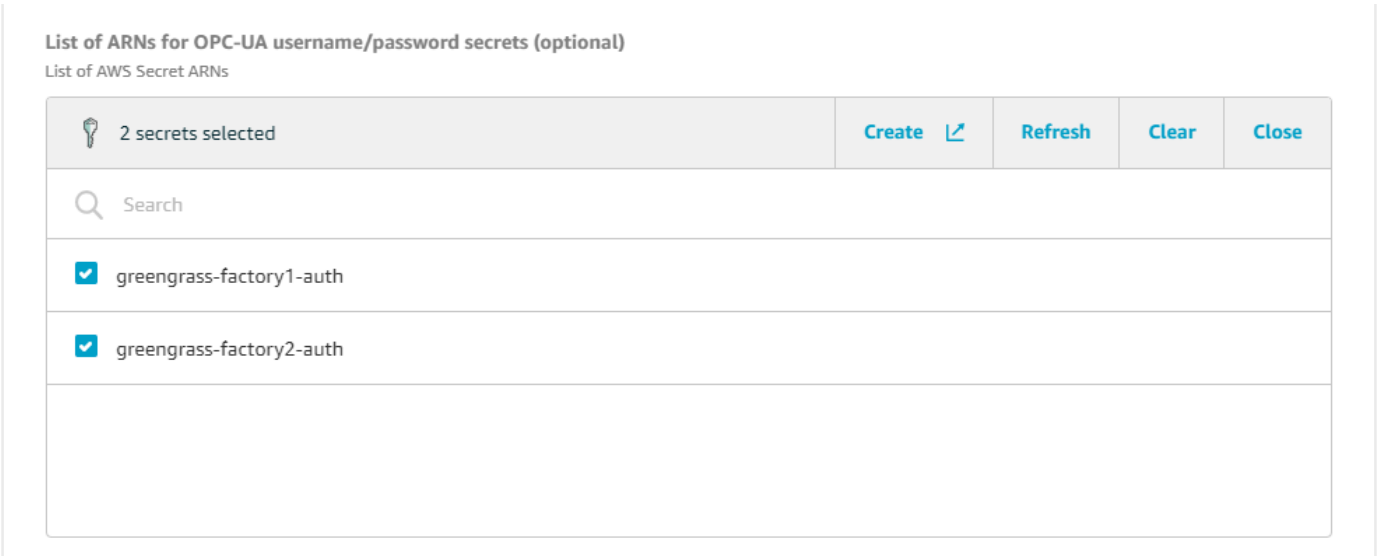
3. En la página de navegación izquierda, seleccione Conectores. En la página Conectores, seleccione Añadir un conector.



4. Elija IoT SiteWise de la lista y elija Siguiente.



5. Si su servidor requiere autenticación, puede crear AWS Secrets Manager secretos con el nombre de usuario y la contraseña del servidor. A continuación, puede adjuntar cada secreto a su grupo de Greengrass y elegirlos en Lista de ARN de secretos de nombre de usuario/contraseña. Para obtener más información acerca de cómo crear y configurar secretos, consulte Configuración de la autenticación de origen. También puede agregar secretos al conector más adelante.



6. Si configuró su puerta de enlace SiteWise Edge con una ruta diferente a la`/var/sitewise`, introdúzcala como ruta de almacenamiento local.
7. (Opcional) Introduzca un tamaño máximo de búfer de disco para el conector. Si el AWS IoT Greengrass núcleo pierde la conexión con la AWS nube, el conector almacena los datos en caché hasta que se pueda conectar correctamente. Si el tamaño de la caché excede el tamaño máximo del búfer de disco, el conector descartará los datos más antiguos de la cola.
8. Elija Añadir.
9. En la esquina superior derecha, en el menú Acciones, seleccione Implementación.
10. Seleccione Detección automática para iniciar la implementación.

    Si se produce un error en la implementación, elija Implementar de nuevo. Si la implementación sigue sin funcionar, consulte la sección de problemas de implementación de AWS IoT Greengrass.

Añadir la puerta de enlace SiteWise Edge a AWS IoT SiteWise

En este procedimiento, añada el grupo Greengrass de su puerta de enlace SiteWise Edge a. AWS IoT SiteWise Después de registrar la puerta de enlace SiteWise Edge AWS IoT SiteWise, el servicio puede implementar las configuraciones de las fuentes de datos en la puerta de enlace SiteWise Edge.

Para agregar la puerta de enlace SiteWise Edge a AWS IoT SiteWise

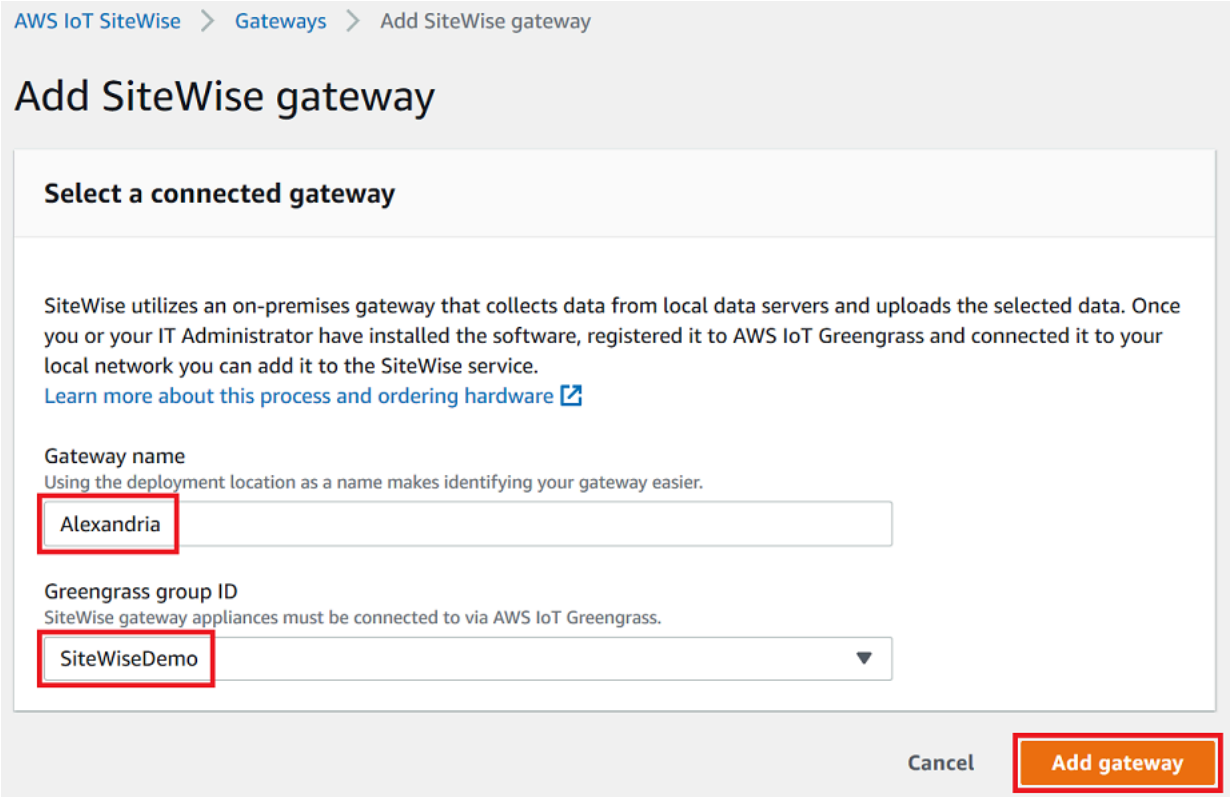
1. Vaya a la consola de AWS IoT SiteWise.

2. Seleccione Añadir puerta de enlace.
3. En la página Agregar SiteWise puerta de enlace, haga lo siguiente:

   a. Introduzca un nombre para la puerta de enlace SiteWise Edge. Considere incluir la ubicación de la puerta de enlace SiteWise Edge en el nombre para poder identificarla fácilmente.

   b. En ID de grupo de Greengrass, seleccione el grupo Greengrass que creó anteriormente.

      Example



   c. (Opcional) En Capacidades de la periferia, seleccione Paquete de procesamiento de datos. Esto permite la comunicación entre su puerta de enlace SiteWise Edge y cualquier modelo de activo y activo configurado para el Edge. Para obtener más información, consulte the section called “Habilitación del procesamiento de datos de la periferia”.

> **Important**
>
> Si agrega el paquete de procesamiento de datos a su puerta de enlace SiteWise Edge, debe configurar e implementar el conector SiteWise Edge en su AWS IoT Greengrass grupo. Realice los pasos siguientes.

   d. Seleccione Añadir puerta de enlace.

4. Si agrega el paquete de procesamiento de datos a su puerta de enlace SiteWise Edge, configure e implemente el conector del procesador de AWS IoT SiteWise datos en su AWS IoT Greengrass grupo. Siga los pasos the section called “Configuración del AWS IoT SiteWise conector” que se indican para configurar el conector del procesador de AWS IoT SiteWise datos:

   a. En Seleccione un conector en la AWS IoT Greengrass consola, elija Procesador AWS IoT SiteWise de datos.
   b. En Ruta de almacenamiento local, introduzca la ruta a su puerta de enlace SiteWise Edge.
   c. Elija Añadir.
   d. En la esquina superior derecha, en el menú Acciones, seleccione Despliegue y, a continuación, Detección automática para iniciar la implementación.

Una vez implementada la puerta de enlace SiteWise Edge, puede agregar una fuente para cada equipo industrial desde el que desee que la puerta de enlace SiteWise Edge ingiera datos. Para obtener más información, consulte Configuración de orígenes de datos.

Puedes ver CloudWatch las métricas de Amazon para verificar a qué se conecta tu puerta de enlace SiteWise Edge AWS IoT SiteWise. Para obtener más información, consulte AWS IoT Greengrass Version 1 métricas de puerta de enlace.

Configuración de las fuentes de datos en las puertas de enlace AWS IoT Greengrass V1 SiteWise Edge

Después de configurar una puerta de enlace AWS IoT SiteWise Edge, puede configurar las fuentes de datos para que la puerta de enlace SiteWise Edge pueda ingerir datos de equipos industriales locales a otros. AWS IoT SiteWise Cada fuente representa un servidor local, como un servidor OPC-UA, al que la puerta de enlace SiteWise Edge conecta y recupera los flujos de datos industriales. Para obtener más información sobre la configuración de una puerta de enlace SiteWise Edge, consulte. Configuración de una puerta de enlace AWS IoT Greengrass V1 SiteWise Edge

> **Note**
>
> AWS IoT SiteWise reinicia la puerta de enlace SiteWise Edge cada vez que agrega o edita una fuente. La puerta de enlace SiteWise Edge no ingiere datos mientras se reinicia. El tiempo necesario para reiniciar la puerta de enlace SiteWise Edge depende de la cantidad de etiquetas que haya en las fuentes de la puerta de enlace SiteWise Edge. El tiempo de

reinicio puede oscilar entre unos segundos (para una puerta de enlace SiteWise Edge con pocas etiquetas) y varios minutos (para una puerta de enlace SiteWise Edge con muchas etiquetas).

Después de crear los orígenes, puede asociar sus flujos de datos a las propiedades de los activos. Para obtener más información sobre cómo crear y utilizar activos, consulte Crear modelos de activos industriales y Asignación de flujos de datos industriales a propiedades de activos.

Puede ver CloudWatch las métricas para comprobar a qué fuente de datos está conectada AWS IoT SiteWise. Para obtener más información, consulte AWS IoT Greengrass Version 1 métricas de puerta de enlace.

Actualmente, AWS IoT SiteWise es compatible con los siguientes protocolos de fuente de datos:

- OPC-UA: protocolo de comunicación machine-to-machine (M2M) para la automatización industrial.
- Modbus TCP: un protocolo de comunicación de datos utilizado para interactuar con controladores lógicos programables (PLC).
- Ethernet/IP (EIP): un protocolo de red industrial que adapta el Protocolo Industrial Común (CIP) a Ethernet estándar.

> **Note**
>
> SiteWise Las pasarelas perimetrales que se ejecutan AWS IoT Greengrass V2 actualmente no son compatibles con las fuentes IP Modbus TCP y Ethernet.

Temas

- Configuración de un origen Modbus TCP
- Configuración de un origen Ethernet/IP (EIP)
- Configuración de la autenticación de origen
- Actualización de un conector

Configuración de un origen Modbus TCP

Puede usar la AWS IoT SiteWise consola o la capacidad de una puerta de enlace AWS IoT SiteWise Edge para definir y agregar una fuente Modbus TCP a su puerta de enlace SiteWise Edge. Este origen representa un servidor Modbus TCP local.

> **Note**
>
> - SiteWise Las puertas de enlace Edge que se ejecutan AWS IoT Greengrass V2 actualmente no son compatibles con las fuentes Modbus TCP.
> - Debe instalar el AWS IoT SiteWise conector para utilizar una fuente Modbus TCP.

Puede usar la fuente Modbus TCP para convertir el tipo de datos de su fuente en un tipo de datos diferente cuando se reciba en su puerta de enlace SiteWise Edge. El tipo de datos de origen determina los tipos de datos que puede elegir para sus datos de destino. También puede optar por intercambiar bytes utilizando el origen Modbus TCP. En la siguiente tabla se ofrece más información sobre los tipos de datos de origen, los tipos de datos de destino y los modos de intercambio compatibles.

Para obtener más información sobre modos de intercambio, consulte el artículo Cómo se codifican los datos reales (coma flotante) y de 32 bits en los mensajes Modbus RTU sobre codificación de mensajes Modbus.

Tipo de datos de origen	Tipos de datos de destino compatibles	Modos de intercambio compatibles	Versiones de conectores compatibles
ASCII	Cadena	noSwap	2
UTF8	Cadena	noSwap	2
ISO8859	Cadena	noSwap	2
Int16	Entero, doble, cadena	noSwap	1 y 2

Tipo de datos de origen	Tipos de datos de destino compatibles	Modos de intercambio compatibles	Versiones de conectores compatibles
Int32	Entero, doble, cadena	NoSwap, ByteSwap byteWordSwap, WordSwap	1 y 2
Flotante	Doble, cadena	Sin Swap, ByteSwap, WordSwap byteWordSwap	1 y 2
Booleano	Booleano	noSwap	1 y 2
Volcado hexadecimal	Cadena	noSwap	1 y 2

Temas

- Configuración de un origen Modbus TCP (consola)
- Configuración de un origen Modbus TCP (CLI)

Configuración de un origen Modbus TCP (consola)

Para configurar un origen Modbus TCP

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación izquierdo, seleccione Puertas de enlace.
3. En la puerta de enlace SiteWise Edge para la que desea crear una fuente, elija Administrar y, a continuación, elija Ver detalles.
4. Seleccione Nuevo origen en la esquina superior derecha.
5. En Opciones de protocolo, elija Modbus TCP.
6. En Configuración del origen Modbus TCP, introduzca un Nombre para el origen.
7. En Dirección IP, introduzca la dirección IP del servidor de origen de datos.
8. (Opcional) Introduzca el Puerto e ID de unidad del servidor de origen.
9. (Opcional) En Duración mínima entre peticiones, introduzca el intervalo de tiempo entre peticiones sucesivas enviadas a su servidor. La puerta de enlace SiteWise Edge calcula

automáticamente el intervalo mínimo permitido en función del dispositivo y del número de registros que tenga.

10. En Grupos de propiedades, introduzca un Nombre.
11. En Propiedades:

    a. En Etiqueta, introduzca un alias de propiedad para su conjunto de registros. Por ejemplo, **`TT-001`**.

    b. En Dirección de registro, introduzca la dirección de registro que inicia el conjunto de registros.

    c. En Tipo de datos de origen, elija el tipo de datos Modbus TCP del que desea convertir los datos. Esto está predeterminado a Volcado hexadecimal.

    > **Note**
    >
    > El tipo de datos de origen que elija determina el tamaño de los datos, el tipo de datos de destino y el modo de intercambio que puede elegir. Para obtener más información, consulte the section called “Configuración de un origen Modbus TCP”.

    d. En Tamaño de datos, introduzca el número de registros por leer al comenzar desde la Dirección de registro. Esto viene determinado por el tipo de datos de origen que elija para este origen.

    e. En Tipo de datos de destino, elige el tipo de AWS IoT SiteWise datos al que quieres que se conviertan los datos. El predeterminado es Cadena. El tipo de destino debe ser compatible con el tipo de datos de origen que elija para este origen. Para obtener más información, consulte the section called “Configuración de un origen Modbus TCP”.

    f. En Modo de intercambio, elija el modo de intercambio de datos que desea utilizar para leer los datos de su conjunto de registros. El modo de intercambio debe ser compatible con el tipo de datos de origen que elija para este origen. Para obtener más información, consulte the section called “Configuración de un origen Modbus TCP”.

12. En Velocidad de escaneo, actualice la velocidad a la que desea que la puerta de enlace SiteWise Edge lea sus registros. AWS IoT SiteWise calcula automáticamente la velocidad de escaneo mínima permitida para su puerta de enlace SiteWise Edge.
13. (Opcional) En Destino, elija adonde se envían los datos del origen. De forma predeterminada, la fuente envía los datos a AWS IoT SiteWise. Puede utilizar una AWS IoT Greengrass transmisión para exportar los datos a un destino local o, en su lugar, a la AWS nube.

> **Note**
>
> Debe elegir AWS IoT SiteWise el destino de los datos de origen si quiere procesar los datos de esta fuente de forma perimetral. AWS IoT SiteWise Para obtener más información sobre el procesamiento de datos en la periferia, consulte the section called “Habilitación del procesamiento de datos de la periferia”.

Para enviar sus datos a otro destino:

a. En Opciones de destino, seleccione Otros destinos.

b. En el nombre de la transmisión de Greengrass, introduce el nombre exacto de la transmisión. AWS IoT Greengrass

> **Note**
>
> Puede utilizar un flujo que ya haya creado o crear un nuevo flujo de AWS IoT Greengrass para exportar sus datos. Si desea utilizar un flujo existente, debe introducir el nombre exacto del flujo o se creará uno nuevo.
> Para obtener más información sobre cómo trabajar con AWS IoT Greengrass transmisiones, consulte Administrar transmisiones de datos en la guía para AWS IoT Greengrass desarrolladores.

14. Elija Añadir origen.

AWS IoT SiteWise implementa la configuración de la puerta de enlace SiteWise Edge en su AWS IoT Greengrass núcleo. No es necesario iniciar una implementación manualmente.

Configuración de un origen Modbus TCP (CLI)

Puede definir las fuentes de datos TCP de Modbus con una función de puerta de enlace SiteWise Edge. Debe definir todos los orígenes Modbus TCP en una única configuración de capacidad.

Para obtener más información sobre cómo definir las fuentes con AWS CLI, consultethe section called “Configuración de orígenes de datos (AWS CLI)”.

> **Note**
>
> Debe instalar el AWS IoT SiteWise conector para utilizar una fuente Modbus TCP.

Esta capacidad tiene las siguientes versiones.

Versión	Espacio de nombres
1	`iotsitewise:modbuscollector:1`

Parámetros de configuración de capacidad de Modbus TCP

Al definir orígenes Modbus TCP en una configuración de capacidad, debe especificar la siguiente información en el documento JSON `capabilityConfiguration`:

fuentes

Lista de estructuras de definición de orígenes Modbus-TCP que contiene cada una la siguiente información:

name

Un nombre único y sencillo para el origen.

measurementDataStreamPrefijo

(Opcional) Cadena que se debe anteponer a todos los flujos de datos del origen. La puerta de enlace SiteWise Edge agrega este prefijo a todos los flujos de datos de esta fuente. Utilice un prefijo de flujo de datos para distinguir entre flujos de datos que tienen el mismo nombre y orígenes diferentes. Cada flujo de datos debe tener un nombre único en su cuenta.

destino

Una estructura de destino que contiene la siguiente información:

type

El tipo del destino.

Nombre de transmisión

El nombre de la AWS IoT Greengrass transmisión.

streamBufferSize

El tamaño del búfer de flujo.

punto de conexión

Una estructura de punto de conexión que contiene la siguiente información:

IPaddress

La dirección IP del origen Modbus TCP.

puerto

(Opcional) El puerto del origen Modbus TCP.

ID de unidad

(Opcional) El unitId. El valor predeterminado es 1.

minimumInterRequestDuración

La duración mínima entre solicitudes en milisegundos.

Grupos de propiedades

La lista de grupos de propiedades que definen la definición de la etiqueta solicitada por el protocolo.

name

El nombre del grupo de propiedades. Debe ser un identificador único.

tagPathDefinitions

La ubicación de la medición dentro del origen. Por ejemplo, el orden de bytes y palabras, la dirección y el tipo de transformación. La estructura de cada `MeasurementPathDefinition` está definida por el conector.

Modo de escaneo

Define el comportamiento del modo de escaneo y los parámetros configurables del origen.

Configuración de un origen Ethernet/IP (EIP)

Puede usar la AWS IoT SiteWise consola o la capacidad de una puerta de enlace SiteWise Edge para definir y agregar una fuente IP Ethernet a su puerta de enlace SiteWise Edge. Este origen representa un servidor IP Ethernet local.

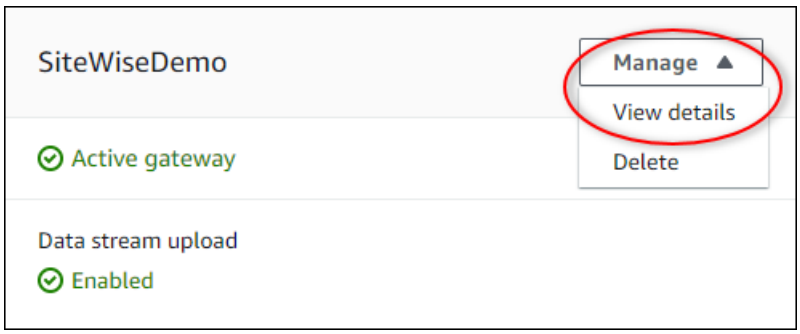
> **Note**
>
> - SiteWise Las puertas de enlace perimetrales que se ejecutan AWS IoT Greengrass V2 actualmente no admiten fuentes IP Ethernet.
> - Debe instalar el AWS IoT SiteWise conector para utilizar una fuente IP Ethernet.

Temas

Configuración de un origen Ethernet/IP (consola)

Para configurar un origen Ethernet/IP

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación izquierdo, seleccione Puertas de enlace.
3. En la puerta de enlace de SiteWise Edge para la que desea crear una fuente, elija Administrar y, a continuación, elija Ver detalles.



4. Seleccione Nuevo origen en la esquina superior derecha.
5. En Opciones de protocolo, elija EtherNet/IP (EIP).
6. Para la configuración de la fuente EtherNet /IP, introduzca un nombre para la fuente.
7. En Dirección IP, introduzca la dirección IP del servidor de origen de datos.
8. (Opcional) Introduzca el Puerto del servidor de origen.
9. En Duración mínima entre peticiones, introduzca el intervalo de tiempo entre peticiones sucesivas enviadas a su servidor. La puerta de enlace SiteWise Edge calcula automáticamente el intervalo mínimo permitido en función del dispositivo y del número de registros que tenga.

10. En Grupos de propiedades, introduzca un Nombre.
11. En Propiedades:

    a. En Etiqueta, introduzca el alias de propiedad para su conjunto de registros. Por ejemplo, **`boiler.inlet.temperature.value`**.

    b. En Tipo de datos de destino, elige el tipo de AWS IoT SiteWise datos al que quieres que se conviertan los datos. El predeterminado es Cadena.
12. En Velocidad de escaneo, actualice la velocidad a la que desea que la puerta de enlace SiteWise Edge lea sus registros. AWS IoT SiteWise calcula automáticamente la velocidad de escaneo mínima permitida para su puerta de enlace SiteWise Edge.
13. (Opcional) En Destino, elija adonde se envían los datos del origen. De forma predeterminada, la fuente envía los datos a AWS IoT SiteWise. Puede utilizar una AWS IoT Greengrass transmisión para exportar los datos a un destino local o, en su lugar, a la AWS nube.

    > **Note**
    >
    > Debe elegir AWS IoT SiteWise el destino de los datos de origen si quiere procesar los datos de esta fuente de forma perimetral. AWS IoT SiteWise Para obtener más información sobre el procesamiento de datos en la periferia, consulte the section called “Habilitación del procesamiento de datos de la periferia”.

    Para enviar sus datos a otro destino:

    a. En Opciones de destino, seleccione Otros destinos.

    b. En el nombre de la transmisión de Greengrass, introduce el nombre exacto de la transmisión. AWS IoT Greengrass

    > **Note**
    >
    > Puede utilizar un flujo que ya haya creado o crear un nuevo flujo de AWS IoT Greengrass para exportar sus datos. Si desea utilizar un flujo existente, debe introducir el nombre exacto del flujo o se creará uno nuevo.
    > Para obtener más información sobre cómo trabajar con AWS IoT Greengrass transmisiones, consulte Administrar transmisiones de datos en la guía para AWS IoT Greengrass desarrolladores.

14. Elija Añadir origen.

    AWS IoT SiteWise implementa la configuración de la puerta de enlace SiteWise Edge en su AWS IoT Greengrass núcleo. No es necesario iniciar una implementación manualmente.

Configuración de un origen Ethernet/IP (CLI)

Puede definir las fuentes de datos EIP en una función de puerta de enlace SiteWise perimetral. Debe definir todos los orígenes EIP en una única configuración de capacidad.

Para obtener más información sobre cómo definir las fuentes con AWS CLI, consultethe section called “Configuración de orígenes de datos (AWS CLI)”.

> **Note**
>
> Debe instalar el AWS IoT SiteWise conector para utilizar una fuente IP Ethernet.

Esta capacidad tiene las siguientes versiones.

Versión	Espacio de nombres
1	`iotsitewise:eipcollector:1`

Parámetros de configuración de capacidad EIP

Al definir orígenes EIP en una configuración de capacidad, debe especificar la siguiente información en el documento JSON `capabilityConfiguration`:

fuentes

Una lista de estructuras de definición de origen EIP que contengan la siguiente información:

name

Un nombre único y sencillo para el origen. Puede tener hasta 256 caracteres.

destinationPathPrefix

(Opcional) Cadena que se debe anteponer a todos los flujos de datos del origen. La puerta de enlace SiteWise Edge agrega este prefijo a todos los flujos de datos de esta fuente. Utilice

un prefijo de flujo de datos para distinguir entre flujos de datos que tienen el mismo nombre y orígenes diferentes. Cada flujo de datos debe tener un nombre único en su cuenta.

destino

Una estructura de destino que contiene la siguiente información:

type

El tipo del destino.

Nombre de transmisión

El nombre de la AWS IoT Greengrass transmisión.

streamBufferSize

El tamaño del búfer de flujo.

punto de conexión

Una estructura de punto de conexión que contiene la siguiente información:

IPaddress

La dirección IP del origen EIP.

puerto

(Opcional) El puerto del origen EIP. Los valores aceptados son números entre 1 y 65535.

minimumInterRequestDuración

(Opcional) La duración mínima entre solicitudes en milisegundos.

Grupos de propiedades

La lista de grupos de propiedades que definen la definición de la etiqueta solicitada por el protocolo. Cada origen puede tener un único grupo de propiedades.

name

El nombre del grupo de propiedades. Debe ser un identificador único con una longitud máxima de 256 caracteres.

tagPathDefinitions

La lista de estructuras que especifican los datos que hay que recopilar del dispositivo Ethernet/IP y cómo transformarlos para la salida.

type

El tipo de `tagPathDefinition`. Por ejemplo, `EIPTagPath`.

path

La ruta de la `tagPathDefinition`. Cada etiqueta de una ruta puede tener una longitud máxima de 40 caracteres y puede empezar por una letra o un guion bajo. Las etiquetas no pueden contener guiones bajos consecutivos ni finales. La ruta tiene el prefijo de cualquier valor de. destinationPathPrefix

dstDataType

El tipo de datos para la salida de los datos de la etiqueta. Los valores aceptados son `integer`, `double`, `string` y `boolean`.

ScanMode

Define el comportamiento del modo de escaneo y los parámetros configurables del origen.

type

El tipo de comportamiento del modo de escaneo. Los valores aceptados son `POLL`.

tasa

La velocidad en milisegundos a la que el conector debería leer las etiquetas desde el origen Ethernet/IP.

Configuración de la autenticación de origen

Si los servidores OPC-UA requieren credenciales de autenticación para conectarse, puede definir un nombre de usuario y una contraseña en un secreto para cada origen de AWS Secrets Manager. Luego, agrega el secreto a su grupo de Greengrass y al SiteWise conector de IoT para que esté disponible en su puerta de enlace SiteWise Edge. Para obtener más información, consulte Implementar secretos hasta el AWS IoT Greengrass núcleo en la Guía para AWS IoT Greengrass Version 1 desarrolladores.

Cuando haya un secreto disponible en su puerta de enlace SiteWise Edge, podrá elegirlo al configurar una fuente. A continuación, la puerta de enlace SiteWise Edge utiliza las credenciales de autenticación del secreto cuando se conecta a la fuente. Para obtener más información, consulte Configuración de orígenes de datos.

Temas

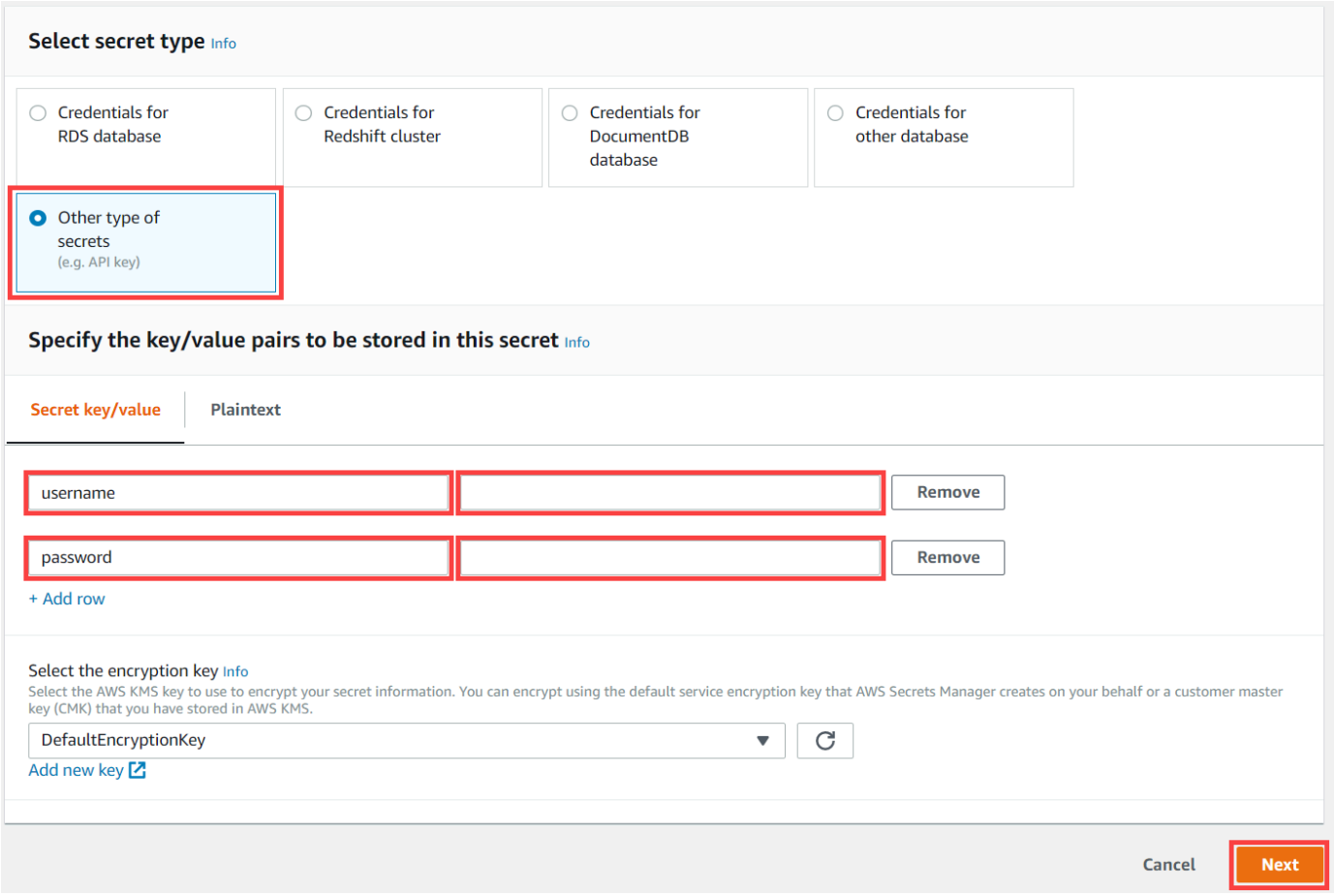
- Creación de secretos de autenticación de origen
- Adición de secretos a un grupo de Greengrass
- Añadir secretos a un SiteWise conector de IoT

Creación de secretos de autenticación de origen

En este procedimiento, usted crea un secreto de autenticación para su fuente en el administrador de secretos. En el secreto, defina pares clave-valor **`username`** y **`password`** que contengan detalles de autenticación para su origen.

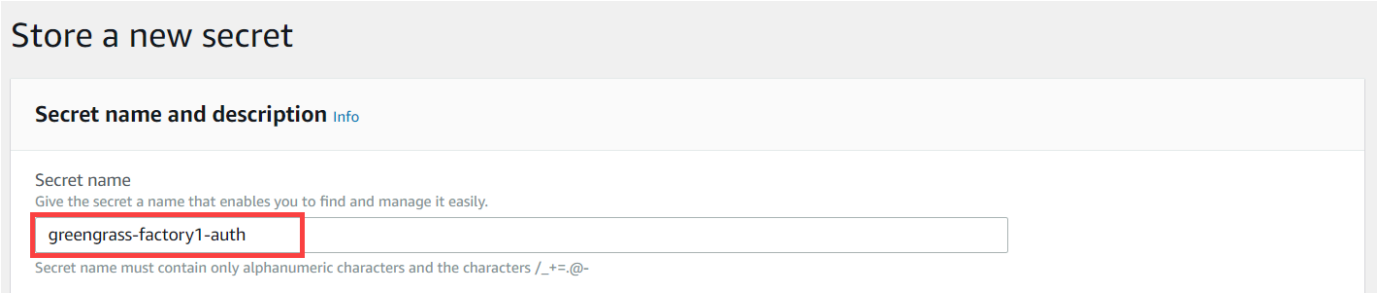
Para crear un secreto de autenticación de origen

1. Vaya a la consola del administrador de secretos.
2. Elija Almacenar un secreto nuevo.
3. En Seleccionar tipo de secreto, elija Otro tipo de secretos.
4. Introduzca pares clave-valor de **`username`** y **`password`** para los valores de autenticación del servidor OPC-UA y, a continuación, seleccione Siguiente.



5. Escriba un Nombre de secreto que comience por `greengrass-`, como **`greengrass-factory1-auth`**.

> **Important**
>
> Debe utilizar el prefijo `greengrass-` para que el rol de servicio predeterminado AWS IoT Greengrass acceda a sus secretos. Si quieres nombrar tus secretos sin este prefijo, debes conceder permisos AWS IoT Greengrass personalizados para acceder a ellos. Para obtener más información, consulta Permitir AWS IoT Greengrass obtener valores secretos en la Guía para AWS IoT Greengrass Version 1 desarrolladores.



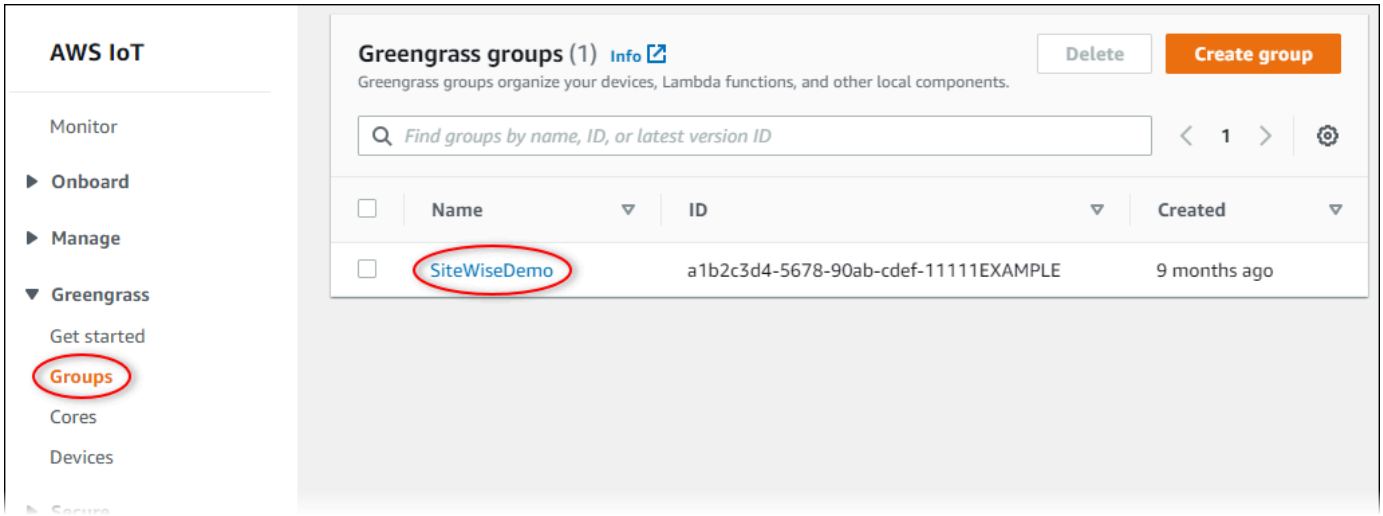
6. Introduzca una Descripción y seleccione Siguiente.
7. (Opcional) En la página Configurar rotación automática, configure la rotación automática para sus secretos. Si configura la rotación automática, debe volver a implementar su grupo de Greengrass cada vez que rote un secreto.
8. En la página Configurar rotación automática, seleccione Siguiente.
9. Revise su nuevo secreto y seleccione Tienda.

Adición de secretos a un grupo de Greengrass

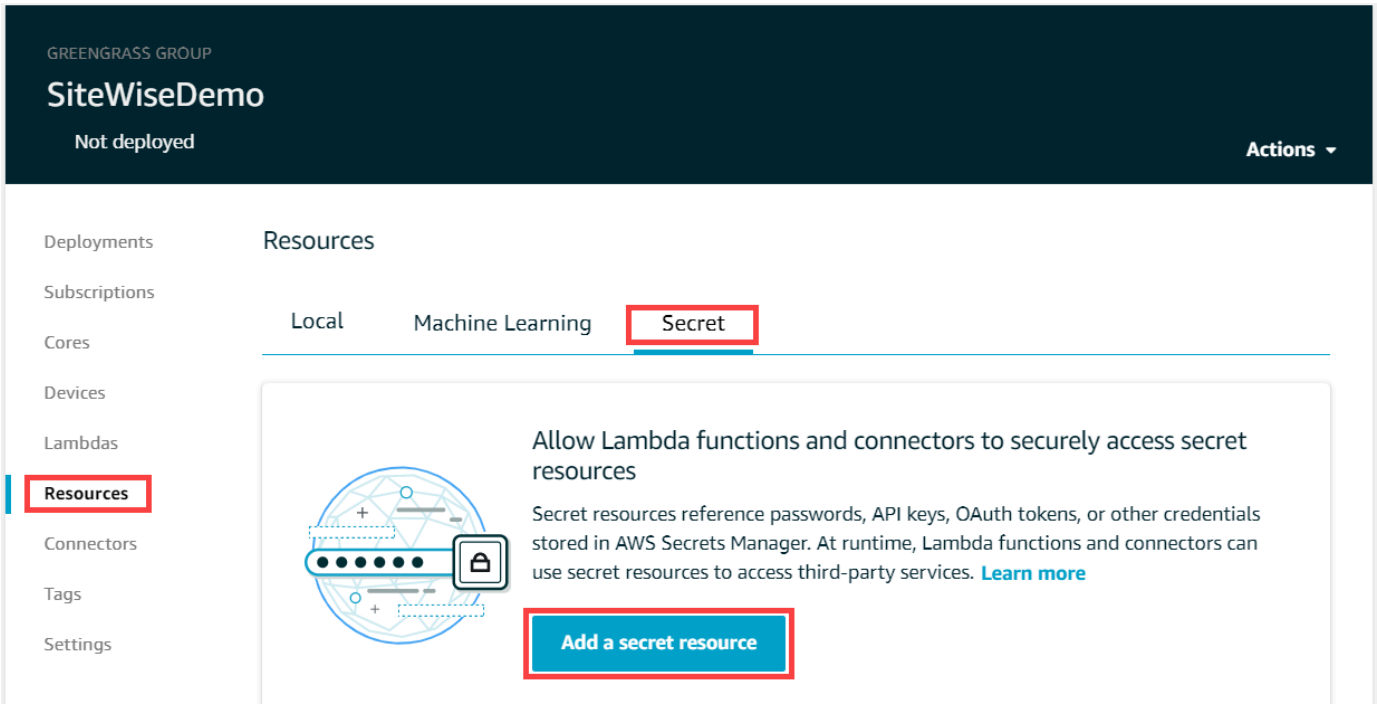
En este procedimiento, agrega los secretos de autenticación de origen a su AWS IoT Greengrass grupo para que estén disponibles en su SiteWise conector de IoT.

Para añadir un secreto a su grupo de Greengrass

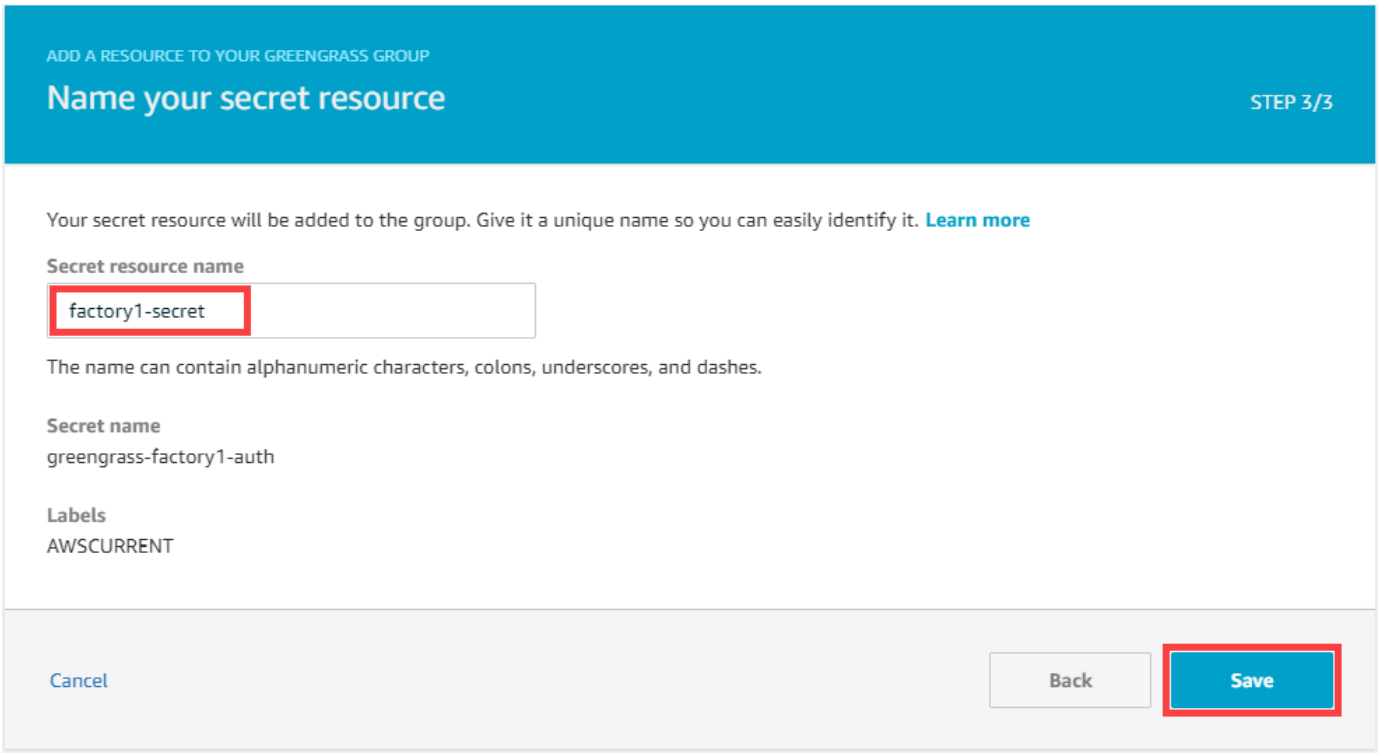
1. Vaya a la consola de AWS IoT Greengrass.
2. En el panel de navegación, en Greengrass, seleccione Grupos y, a continuación, su grupo.



3. En la página de navegación, Seleccione Recursos.
4. En la página Recursos, elija la pestaña Secreto y, a continuación, Agregar un recurso secreto.



5. Elija Seleccionar y escoja su secreto de la lista.
6. Elija Siguiente.
7. En Nombre de recurso secreto, escriba un nombre para el recurso secreto y seleccione Guardar.

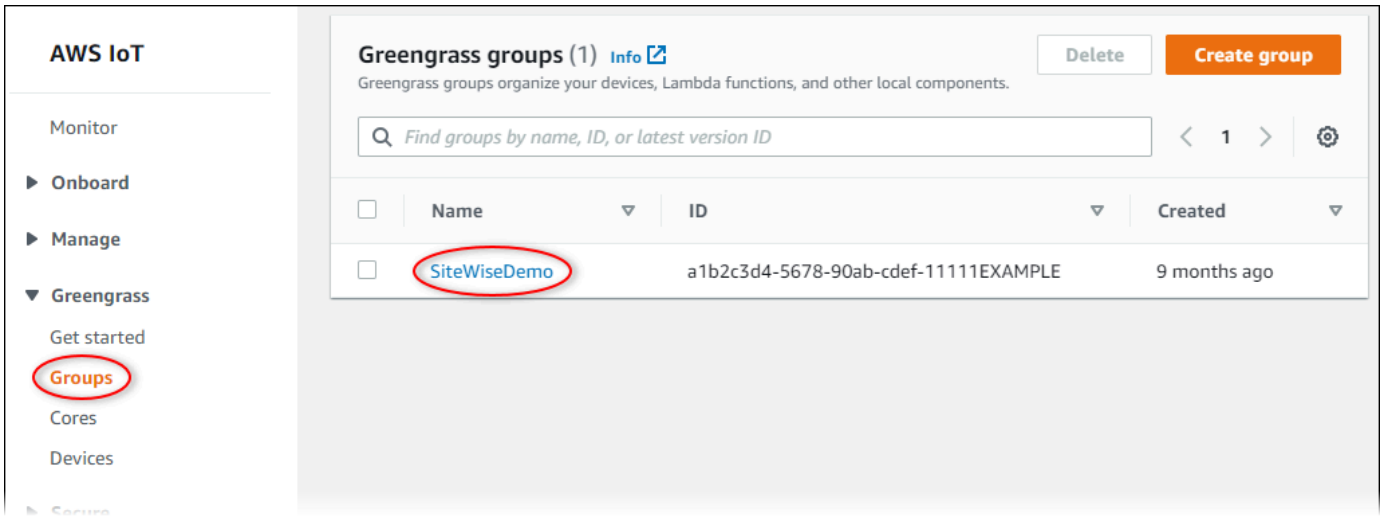


Añadir secretos a un SiteWise conector de IoT

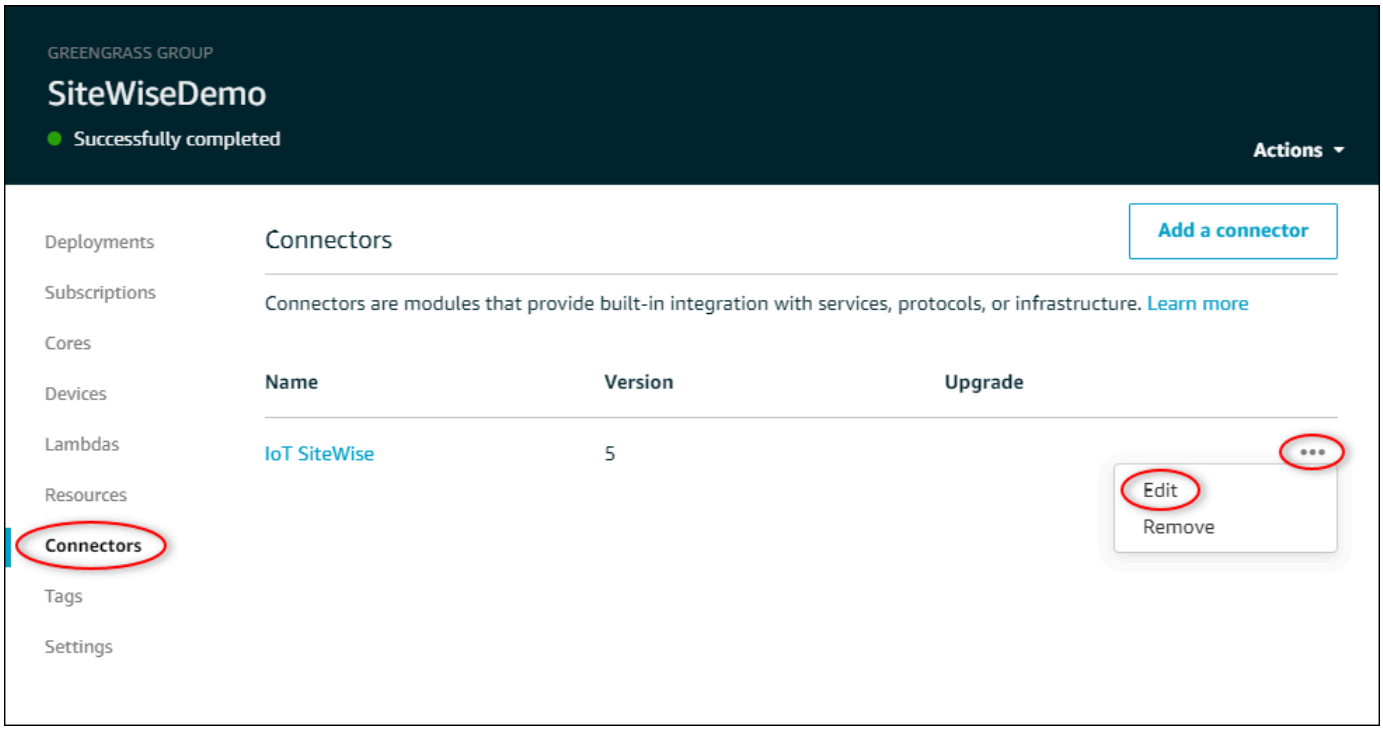
En este procedimiento, agrega los secretos de autenticación de origen a su SiteWise conector de IoT para que estén disponibles en su puerta de enlace SiteWise Edge. AWS IoT SiteWise

Para añadir un secreto a tu SiteWise conector de IoT

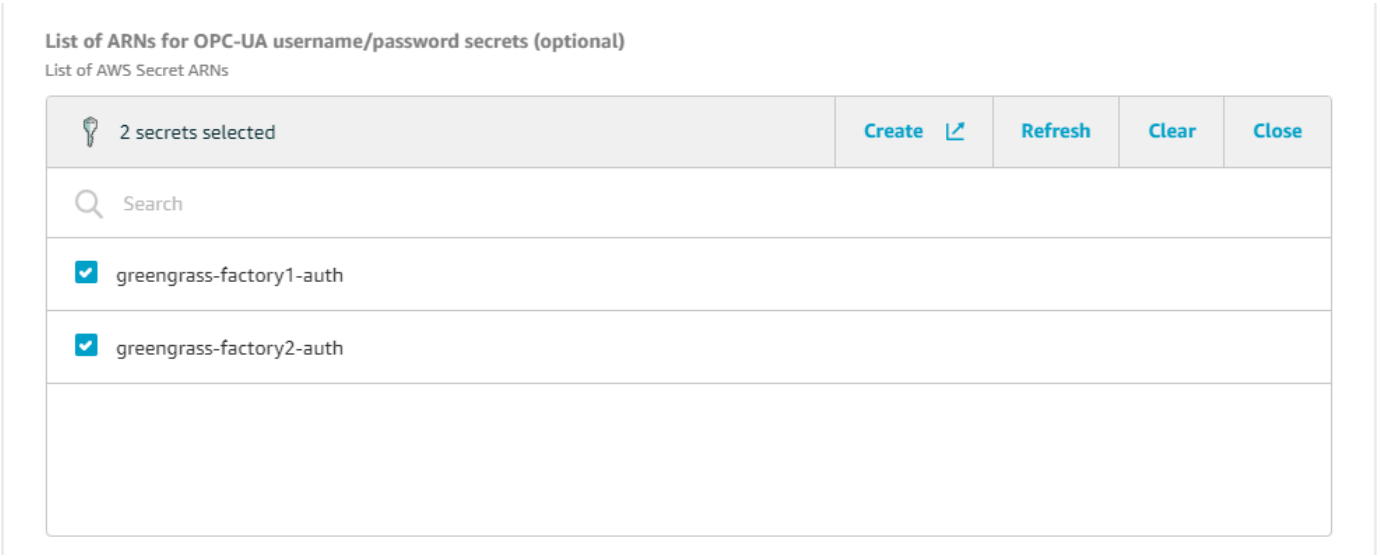
1. Vaya a la consola de AWS IoT Greengrass.
2. En el panel de navegación, en Greengrass, seleccione Grupos y, a continuación, su grupo.



3. En la página de navegación, seleccione Conectores.
4. Elija el icono de puntos suspensivos del SiteWise conector IoT para abrir el menú de opciones y, a continuación, seleccione Editar.



5. En la lista de ARN para los nombres de usuario y contraseñas secretos del OPC-UA, selecciona Seleccionar y, a continuación, selecciona cada secreto para añadirlo a esta puerta de enlace Edge. SiteWise Si tiene que crear secretos, consulte Creación de secretos de autenticación de origen.



Si el secreto no aparece, elija Actualizar. Si el secreto sigue sin aparecer, compruebe haber añadido el secreto a su grupo Greengrass.

6. Seleccione Guardar.
7. En la esquina superior derecha, en el menú Acciones, seleccione Implementación.
8. Seleccione Detección automática para iniciar la implementación.

   Si se produce un error en la implementación, elija Implementar de nuevo. Si la implementación sigue sin funcionar, consulte la sección de problemas de implementación de AWS IoT Greengrass.

   Después de que el grupo se implemente, puede configurar un origen que utilice el nuevo secreto. Para obtener más información, consulte Configuración de orígenes de datos.

Actualización de un conector

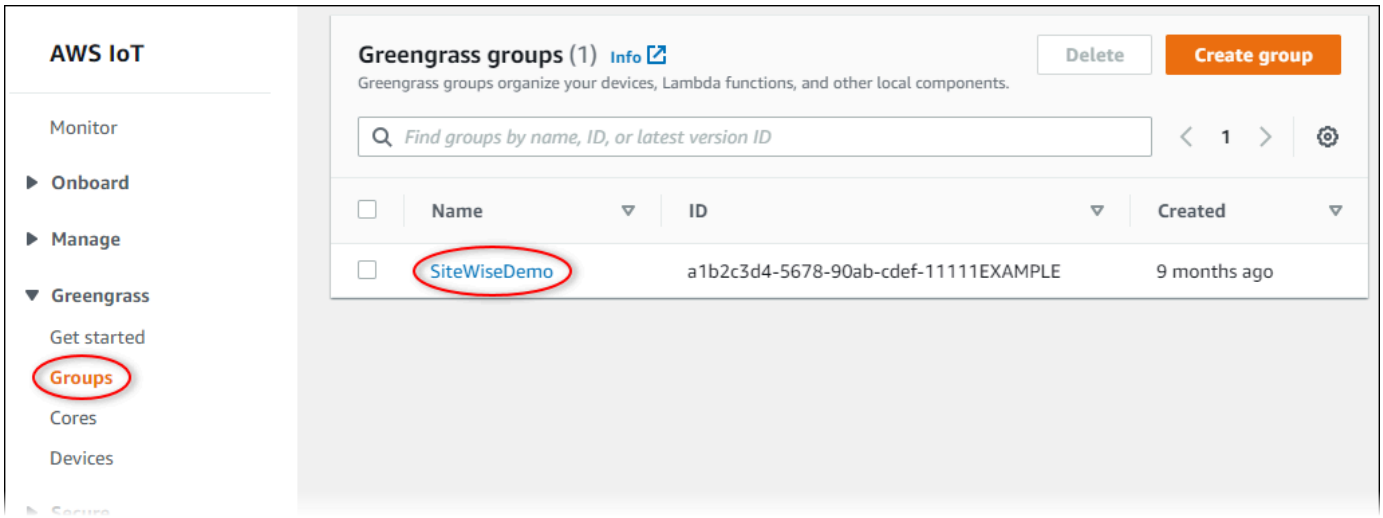
> **Important**
>
> La versión 6 del SiteWise conector IoT presenta nuevos requisitos: el software AWS IoT Greengrass principal v1.10.0 y el administrador de flujos. Antes de actualizar el conector, compruebe que la puerta de enlace SiteWise Edge cumpla estos requisitos o no podrá implementar la puerta de enlace Edge. SiteWise

Puede actualizar fácilmente el conector de su puerta de enlace SiteWise Edge después del lanzamiento de una nueva versión SiteWise del conector de IoT.

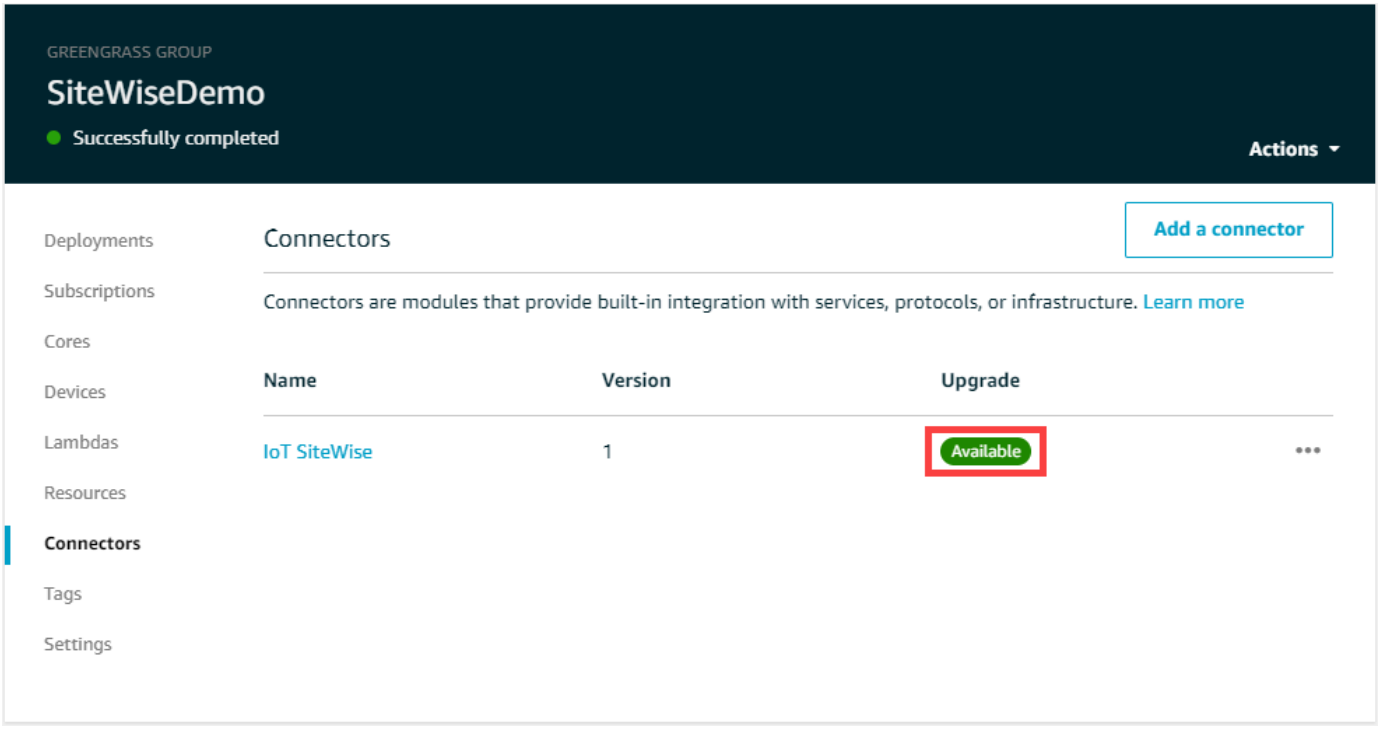
> **Note**
>
> En este procedimiento, se vuelve a implementar el grupo de Greengrass y se reinicia la puerta de enlace de Edge. SiteWise La puerta de enlace SiteWise Edge no ingiere datos mientras se reinicia. El tiempo necesario para reiniciar la puerta de enlace SiteWise Edge depende de la cantidad de etiquetas que haya en las fuentes de la puerta de enlace SiteWise Edge. El tiempo de reinicio puede oscilar entre unos segundos (para una puerta de enlace SiteWise Edge con pocas etiquetas) y varios minutos (para una puerta de enlace SiteWise Edge con muchas etiquetas).

Para actualizar un SiteWise conector de IoT

1. Vaya a la consola de AWS IoT Greengrass.
2. En el panel de navegación, en Greengrass, elija Grupos y, a continuación, elija el grupo que creó al configurar la puerta de enlace SiteWise Edge.



3. En el panel de navegación, elija Conectores.
4. En la página Conectores, selecciona Disponible junto al SiteWise conector IoT.



Si no ve el elemento Disponible, ya tiene la versión más reciente del conector.

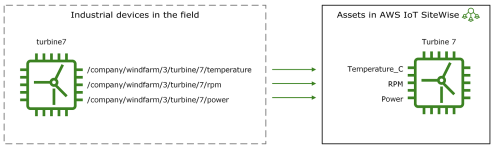
5. En la página Actualizar conector, introduzca los parámetros del conector y, a continuación, seleccione Actualizar.
6. En la esquina superior derecha, en el menú Acciones, seleccione Implementación.
7. Seleccione Detección automática para iniciar la implementación.

   Si se produce un error en la implementación, elija Implementar de nuevo. Si la implementación sigue sin funcionar, consulte la sección de problemas de implementación de AWS IoT Greengrass.

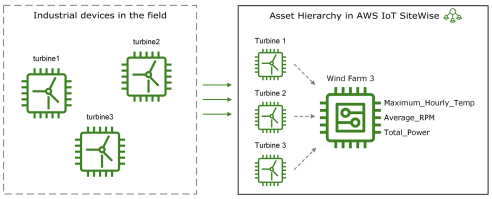
Crear modelos de activos industriales

Puede crear representaciones virtuales de su operación industrial con AWS IoT SiteWise activos. Un activo representa un dispositivo, un equipo o un proceso que carga uno o más flujos de datos al Nube de AWS. Por ejemplo, un dispositivo puede ser una turbina eólica que envía mediciones de la temperatura del aire, la velocidad de rotación de la hélice y series temporales de salida de potencia a las propiedades de activos en AWS IoT SiteWise.

Cada secuencia de datos corresponde a un alias de propiedad único. Por ejemplo, el alias `/company/windfarm/3/turbine/7/temperature` identifica de forma exclusiva el flujo de datos de temperatura procedente de la turbina número 7 en el parque eólico número 3. Puede configurar AWS IoT SiteWise los activos para transformar los datos de medición entrantes mediante expresiones matemáticas, como convertir los datos de temperatura de grados Celsius a Fahrenheit.



Un activo también puede representar una agrupación lógica de dispositivos, como un parque eólico completo. Puede asociar activos a otros activos para crear jerarquías de activos que representen operaciones industriales complejas. Los activos pueden acceder a los datos de sus activos secundarios asociados. De este modo, puede utilizar AWS IoT SiteWise expresiones para calcular métricas agregadas, como la producción neta de energía de un parque eólico.



Debe crear todos los activos a partir de un modelo de activos. Los modelos de activos son estructuras declarativas que normalizan el formato de los activos. Los modelos de activos exigen una información coherente en varios activos del mismo tipo para que pueda procesar los datos de los activos que representan grupos de dispositivos. En el diagrama anterior, se utiliza el mismo modelo de activos para las tres turbinas porque todas las turbinas comparten un conjunto común de propiedades.

También puede crear modelos de componentes. Un modelo de componentes es un tipo especial de modelo de activos que se puede incluir en los modelos de activos u otros modelos de componentes.

Puede utilizar los modelos de componentes para definir subconjuntos reutilizables comunes, como sensores, motores, etc., que pueda compartir en varios modelos de activos.

Después de definir los modelos de activos, puede crear los activos industriales. Para crear un activo, seleccione un modelo de activos `ACTIVE` para crear un activo a partir de ese modelo. A continuación, puede rellenar información específica del activo, como alias y atributos de flujo de datos. En el diagrama anterior, se crean tres activos de turbina a partir de un modelo de activos y, a continuación, se asocian alias de flujo de datos como `/company/windfarm/3/turbine/7/temperature` para cada turbina.

También puede actualizar y eliminar los activos, modelos de activos y modelos de componentes existentes. Al actualizar un modelo de activos, todos los activos basados en ese modelo de activos reflejan los cambios que realice en el modelo subyacente. Al actualizar un modelo de componentes, esto se aplica a todos los activos en función de todos los modelos de activos que hacen referencia al modelo de componentes.

Sus modelos de activos pueden ser muy complejos, por ejemplo, al modelar un equipo complicado que tiene muchos subcomponentes. Para ayudar a mantener estos modelos de activos organizados y fáciles de mantener, puede utilizar modelos compuestos personalizados para agrupar propiedades relacionadas o reutilizar componentes compartidos. Para obtener más información, consulte Modelos compuestos personalizados (componentes).

Temas

Estados de activos y modelos

Al crear, actualizar o eliminar un activo, un modelo de activo o un modelo de componentes, los cambios tardan en propagarse. AWS IoT SiteWise resuelve estas operaciones de forma asíncrona y actualiza el estado de cada recurso. Cada activo, modelo de activo y modelo de componente tiene un campo de estado que contiene el estado del recurso y cualquier mensaje de error, si corresponde. El estado puede ser uno de los siguientes valores:

- `ACTIVE`— El recurso está activo. Este es el único estado en el que puede consultar activos, modelos de activos y modelos de componentes e interactuar con ellos.
- `CREATING`— Se está creando el recurso.
- `UPDATING`— El recurso se está actualizando.
- `DELETING`— Se está eliminando el recurso.
- `PROPAGATING`— (Solo modelos de activos y modelos de componentes) Los cambios se están propagando a todos los recursos dependientes (del modelo de activos a los activos o del modelo de componentes a los modelos de activos).
- `FAILED`— El recurso no se pudo validar durante una operación de creación o actualización, posiblemente debido a una referencia circular en una expresión. Puede eliminar los recursos que estén en ese `FAILED` estado.

Algunas de las operaciones de creación, actualización y eliminación AWS IoT SiteWise colocan un activo, un modelo de activo o un modelo de componente en un estado distinto `ACTIVE` al de cuando se resuelve la operación. Para consultar un recurso o interactuar con él después de realizar una de estas operaciones, debe esperar a que el estado cambie a`ACTIVE`. De lo contrario, sus solicitudes fallan.

Temas

Comprobación del estado de un activo

Puede usar la AWS IoT SiteWise consola o la API para comprobar el estado de un activo.

Temas

- Comprobación del estado de un activo (consola)
- Comprobar el estado de un activo (AWS CLI)

Comprobación del estado de un activo (consola)

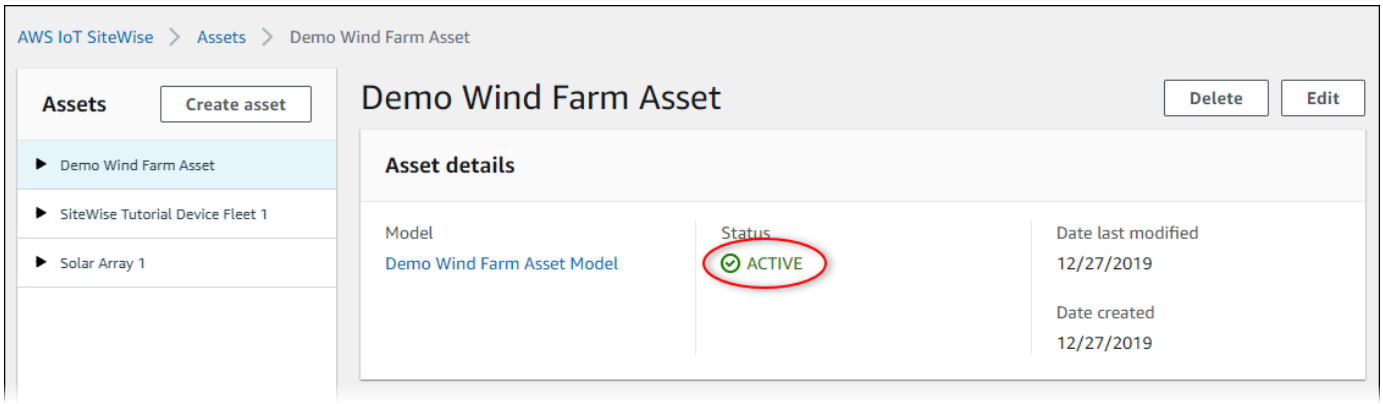
Utilice el procedimiento siguiente para comprobar el estado de un activo en la consola de AWS IoT SiteWise .

Para comprobar el estado de un activo (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Activos.
3. Elija el activo que desea comprobar.

> **Tip**
>
> Puede elegir el icono de flecha para expandir una jerarquía de activos y encontrar su activo.

4. Busque Estado en el panel Detalles del activo.



Comprobar el estado de un activo (AWS CLI)

Puede usar AWS Command Line Interface (AWS CLI) para comprobar el estado de un activo.

Para comprobar el estado de un activo, utilice la DescribeAssetoperación con el `assetId` parámetro.

Para comprobar el estado de un activo (AWS CLI)

- Ejecute el siguiente comando para describir el activo. *Sustituya el identificador del* activo por el identificador del activo o el identificador externo. El ID externo es un ID definido por el usuario. Para obtener más información, consulte Hacer referencia a objetos con identificadores externos en la Guía del usuario de AWS IoT SiteWise .

  ```
  aws iotsitewise describe-asset --asset-id asset-id
  ```

  La operación devuelve una respuesta que contiene los detalles del activo. La respuesta contiene un `assetStatus` objeto que tiene la siguiente estructura:

  ```
  {
      ...
      "assetStatus": {
        "state": "String",
        "error": {
           "code": "String",
           "message": "String"
        }
      }
    }
  ```

  El estado del activo está en `assetStatus.state` en el objeto JSON.

Comprobar el estado de un modelo de activos o un modelo de componentes

Puede utilizar la AWS IoT SiteWise consola o la API para comprobar el estado de un modelo de activos o un modelo de componentes.

Temas

- Comprobar el estado de un modelo de activos o un modelo de componentes (consola)
- Comprobar el estado de un modelo de activos o un modelo de componentes (AWS CLI)

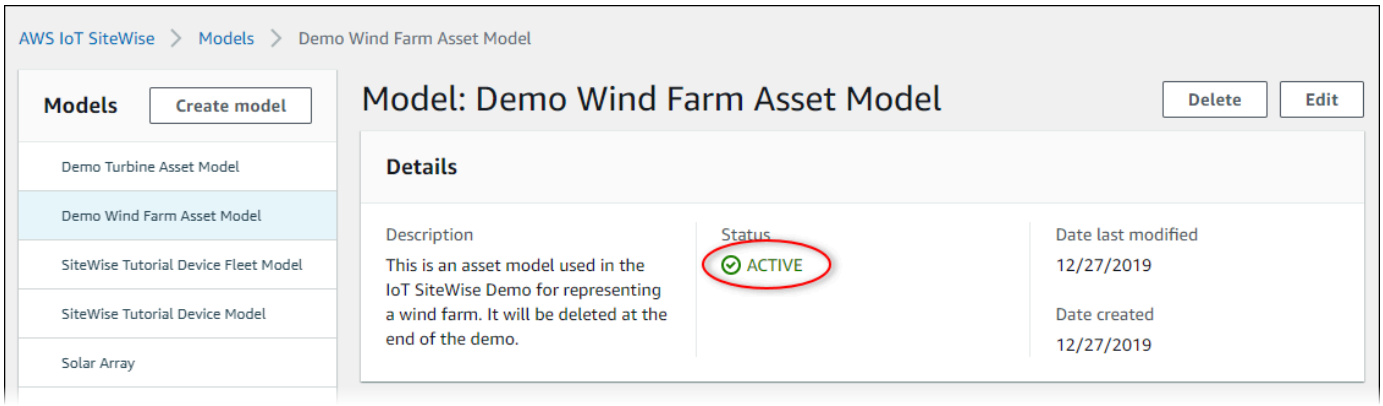
Comprobar el estado de un modelo de activos o un modelo de componentes (consola)

Utilice el siguiente procedimiento para comprobar el estado de un modelo de activos o un modelo de componentes en la AWS IoT SiteWise consola.

> **Tip**
>
> Tanto los modelos de activos como los modelos de componentes se muestran en la sección Modelos del panel de navegación. El panel de detalles del modelo de activo o modelo de componente seleccionado indica de qué tipo se trata.

Para comprobar el estado de un modelo de activos o un modelo de componentes (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Models (Modelos).
3. Seleccione el modelo que desee comprobar.
4. Busque Estado en el panel Detalles.



Comprobar el estado de un modelo de activos o un modelo de componentes (AWS CLI)

Puede utilizar el AWS CLI para comprobar el estado de un modelo de activos o un modelo de componentes.

Para comprobar el estado de un modelo de activos o un modelo de componentes, utilice la DescribeAssetModeloperación con el `assetModelId` parámetro.

> **Tip**
>
> AWS CLI Define los modelos de componentes como un tipo de modelo de activos. Por lo tanto, se utiliza la misma DescribeAssetModeloperación para ambos tipos de modelo. El `assetModelType` campo de la respuesta indica si es un `ASSET_MODEL` o un`COMPONENT_MODEL`.

Para comprobar el estado de un modelo de activos o un modelo de componentes (AWS CLI)

- Ejecute el siguiente comando para describir el modelo. *`asset-model-id`*Sustitúyalo por el ID o el ID externo del modelo de activos o del modelo de componentes. El ID externo es un ID definido por el usuario. Para obtener más información, consulte Hacer referencia a objetos con identificadores externos en la Guía del usuario de AWS IoT SiteWise .

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

  La operación devuelve una respuesta que contiene los detalles del modelo. La respuesta contiene un objeto `assetModelStatus` que tiene la siguiente estructura.

  ```
  {
      ...
      "assetModelStatus": {
        "state": "String",
        "error": {
           "code": "String",
           "message": "String"
        }
      }
    }
  ```

  El estado del modelo se encuentra `assetModelStatus.state` en el objeto JSON.

Modelos compuestos personalizados (componentes)

Al modelar un activo industrial especialmente complejo, como una pieza de maquinaria complicada que consta de muchas piezas, mantener los modelos de activos organizados y fáciles de mantener puede convertirse en un desafío.

En esos casos, puede añadir modelos compuestos personalizados, o componentes si utiliza la consola, a sus modelos de activos y componentes existentes. Esto le ayuda a mantenerse organizado al agrupar las propiedades relacionadas y reutilizar las definiciones de los subcomponentes.

Hay dos tipos de modelos compuestos personalizados:

- Los modelos compuestos personalizados en línea definen un conjunto de propiedades agrupadas que se aplican al modelo de activos o al modelo de componentes al que pertenece el modelo compuesto personalizado. Se utilizan para agrupar propiedades relacionadas. Constan de un nombre, una descripción y un conjunto de propiedades del modelo de activos. No son reutilizables.
- Los modelos compuestos omponent-model-based personalizados en C hacen referencia a un modelo de componentes que desee incluir en su modelo de activos o modelo de componentes. Se utilizan para incluir subconjuntos estándar en el modelo. Constan de un nombre, una descripción y el identificador del modelo de componente al que hace referencia. No tienen propiedades propias; el modelo de componentes al que se hace referencia proporciona las propiedades asociadas a todos los activos creados.

Las siguientes secciones ilustran cómo utilizar modelos compuestos personalizados en sus diseños.

Temas

Modelos compuestos personalizados en línea

Los modelos compuestos personalizados en línea proporcionan una forma de organizar el modelo de activos agrupando las propiedades relacionadas.

Por ejemplo, supongamos que quiere modelar un activo robótico. El robot incluye un servomotor, una fuente de alimentación y una batería. Cada una de esas partes constitutivas tiene sus propias propiedades que desea incluir en el modelo. Puede definir un modelo de activos denominado `robot_model` que tenga propiedades como las siguientes.

```
• robot_model
```

- `servo_status` (entero)
- `servo_position` (doble)
- `powersupply_status` (entero)
- `powersupply_temperature` (doble)
- `battery_status` (entero)
- `battery_charge` (doble)

Sin embargo, en algunos casos, es posible que haya muchos subensamblajes o que los propios subensamblajes tengan muchas propiedades. En estos casos, es posible que haya tantas propiedades que resulte engorroso consultarlas y mantenerlas en una sola lista plana en la raíz del modelo, como en el ejemplo anterior.

Para hacer frente a estas situaciones, puede utilizar un modelo compuesto personalizado en línea para agrupar las propiedades. Un modelo compuesto personalizado en línea es un modelo compuesto personalizado que define sus propias propiedades. Por ejemplo, puede modelar su robot de la siguiente manera.

- `robot_model`
  - `servo`
    - `status`(entero)
    - `position`(doble)
  - `powersupply`
    - `status`(entero)
    - `temperature` (doble)
  - `battery`
    - `status`(entero)
    - `charge`(doble)

En el ejemplo anterior `servopowersupply`, y `battery` son los nombres de los modelos compuestos personalizados en línea definidos en el modelo de `robot_model` activos. A continuación, cada uno de estos modelos compuestos define sus propias propiedades.

> **Note**
>
> En este caso, cada modelo compuesto personalizado define sus propias propiedades, de modo que todas las propiedades forman parte del propio modelo de activos (`robot_model`en este caso). Estas propiedades no se comparten con ningún otro modelo de activos o de componentes. Por ejemplo, si creó algún otro modelo de activos que también tuviera un modelo compuesto personalizado en línea denominado`servo`, realizar un cambio interno no `robot_model` afectaría a la `servo` `servo` definición del otro modelo de activos. Si desea implementar este tipo de compartición (por ejemplo, tener solo una definición para un servo, que puedan compartir todos sus modelos de activos), debería crear un modelo de componentes para ese servo y, a continuación, crear modelos component-model-basedcompuestos que hagan referencia a él. Consulte la siguiente sección para obtener más información.

Para obtener información sobre cómo crear modelos compuestos personalizados en línea, consulteCreación de modelos compuestos personalizados (componentes).

C: omponent-model-based modelos compuestos personalizados

Puede crear un modelo de componente AWS IoT SiteWise para definir un subensamblaje estándar y reutilizable. Una vez creado un modelo de componente, puede añadir referencias al mismo en sus otros modelos de activos y modelos de componentes. Para ello, añada un modelo compuesto component-model-based personalizado a cualquier modelo en el que desee hacer referencia al componente. Puede añadir referencias a su componente desde varios modelos o varias veces dentro del mismo modelo.

De esta forma, puede evitar duplicar las mismas definiciones en todos los modelos. También simplifica el mantenimiento de los modelos, ya que cualquier cambio que realice en un modelo de componentes se reflejará en todos los modelos de activos que lo utilicen.

Por ejemplo, supongamos que su instalación industrial tiene muchos tipos de equipos y todos utilizan el mismo tipo de servomotor. Algunos de ellos tienen muchos servomotores en un solo equipo. Creas un modelo de activos para cada tipo de equipo, pero no querrás duplicar la definición `servo` cada vez. Quieres modelarlo solo una vez y usarlo en tus distintos modelos de activos. Si más adelante cambias la definición de`servo`, se actualizará en todos tus modelos y activos.

Para modelar el robot del ejemplo anterior de esta manera, podría definir los servomotores, las fuentes de alimentación y las baterías como modelos de componentes, como este.

- `servo_component_model`
  - `status`(entero)
  - `position`(doble)

- `powersupply_component_model`
  - `status`(entero)
  - `temperature` (doble)

- `battery__component_model`
  - `status`(entero)
  - `charge`(doble)

A continuación, podría definir modelos de activos, por ejemplo`robot_model`, que hagan referencia a estos componentes. Varios modelos de activos pueden hacer referencia al mismo modelo de componentes. También puede hacer referencia al mismo modelo de componentes varias veces en un modelo de activo, por ejemplo, si su robot tiene varios servomotores.

- `robot_model`
  - `servo1`(referencia:) `servo_component_model`
  - `servo2`(referencia:`servo_component_model`)
  - `servo3`(referencia:`servo_component_model`)
  - `powersupply` (referencia:`powersupply_component_model`)
  - `battery`(referencia:`battery_component_model`)

Para obtener información sobre cómo crear modelos de componentes, consulteCreación de modelos de componentes.

Para obtener información sobre cómo hacer referencia a sus modelos de componentes en otros modelos, consulteCreación de modelos compuestos personalizados (componentes).

Uso de rutas para hacer referencia a las propiedades de los modelos compuestos personalizados

Al crear una propiedad en un modelo de activos, un modelo de componentes o un modelo compuesto personalizado, puede hacer referencia a ella desde otras propiedades que utilizan su valor, como las transformaciones y las métricas.

AWS IoT SiteWise proporciona diferentes formas de hacer referencia a su propiedad. La forma más sencilla suele ser utilizar su identificador de propiedad. Sin embargo, si la propiedad a la que desea hacer referencia está en un modelo compuesto personalizado, puede que le resulte más útil hacer referencia a ella mediante una ruta.

Una ruta es una secuencia ordenada de segmentos de ruta que especifica una propiedad en términos de su posición entre los modelos compuestos anidados dentro de un modelo de activos y un modelo compuesto.

Obtención de rutas de propiedades

Puede obtener la ruta de una propiedad desde el `path` campo de su propiedad AssetModelProperty.

Por ejemplo, supongamos que tiene un modelo de activos `robot_model` que contiene un modelo compuesto personalizado`servo`, que tiene una propiedad`position`. Si llama`servo`, DescribeAssetModelCompositeModella `position` propiedad mostrará un `path` campo similar al siguiente:

```
"path": [
    {
       "id": "asset model ID",
       "name": "robot_model"
    },
    {
       "id": "composite model ID",
       "name": "servo"
    },
    {
       "id": "property ID",
       "name": "position"
    }
]
```

Uso de rutas de propiedades

Puede usar una ruta de propiedad al definir una propiedad que haga referencia a otras propiedades, como una transformación o una métrica.

Una propiedad usa una variable para hacer referencia a otra propiedad. Para obtener más información sobre cómo trabajar con variables, consulteUso de variables en las expresiones de fórmula.

Al definir una variable para hacer referencia a una propiedad, puede utilizar el identificador de la propiedad o su ruta.

Para definir una variable que utilice la ruta de la propiedad a la que se hace referencia, especifique el `propertyPath` campo de su valor.

Por ejemplo, para definir un modelo de activos que tenga una métrica que haga referencia a una propiedad mediante una ruta, puede pasar una carga útil como esta a CreateAssetModel:

```
{
    ...
    "assetModelProperties": [
        {
            ...
            "type": {
                "metric": {
                    ...
                    "variables": [
                        {
                            "name": "variable name",
                            "value": {
                                "propertyPath": [
                                    path segments
                                ]
                            }
                        }
                    ],
                    ...
                }
            },
            ...
        },
        ...
```

```
    ],
    ...
}
```

Trabajar con identificadores de objetos

AWS IoT SiteWise define varios tipos de objetos persistentes, como activos, modelos de activos, propiedades y jerarquías. Todos estos objetos tienen identificadores únicos que puede utilizar para recuperarlos, actualizarlos y eliminarlos.

AWS IoT SiteWise tiene diferentes opciones para los clientes a la hora de crear identificaciones. AWS IoT SiteWise genera uno por defecto en el momento de la creación del objeto. Los usuarios también pueden proporcionar sus propios identificadores a sus objetos.

Temas

Trabajar con los UUID de objetos

Cada objeto persistente AWS IoT SiteWise tiene un UUID para identificarlo. Por ejemplo, los modelos de activos tienen un ID de modelo de activo, los activos tienen un ID de activo, etc. Este identificador se asigna en el momento de crear el objeto y permanece inalterado durante la vida útil del objeto.

Cuando creas un objeto nuevo, AWS IoT SiteWise genera un identificador único para ti de forma predeterminada. También puedes proporcionar tu propio ID en el momento de la creación en formato UUID.

> **Note**
>
> Los UUID deben ser únicos a nivel mundial en la AWS región en la que se crearon y para el mismo tipo de objeto. Cuando se AWS IoT SiteWise genera automáticamente un ID para ti, siempre es único. Si eliges tu propio identificador, asegúrate de que sea único.

Por ejemplo, si llamas para crear un nuevo modelo de activos CreateAssetModel, puedes proporcionar tu propio UUID en el `assetModelId` campo opcional de la solicitud.

Por el contrario, si lo omites `assetModelId` en la solicitud, AWS IoT SiteWise genera un UUID para el nuevo modelo de activos.

Uso de identificadores externos

Para definir su propio ID en un formato que no sea el UUID, puede asignar un ID externo. Por ejemplo, puedes hacerlo si reutilizas un ID que estás utilizando en un sistema que no lo está AWS, o si quieres que sea más legible para los humanos. Los ID externos tienen un formato más flexible. Puedes utilizarlos para hacer referencia a tus objetos en las operaciones de la AWS IoT SiteWise API en las que, de otro modo, utilizarías el UUID.

Al igual que los UUID, cada ID externo debe ser único en su contexto. Por ejemplo, no puede tener dos modelos de activos con el mismo ID externo. Además, al igual que los UUID, un objeto solo puede tener un ID externo durante su vida útil, lo que no puede cambiar.

Diferencias entre los ID externos y los UUID

Los ID externos se diferencian de los UUID en los siguientes aspectos:

- Cada objeto tiene un UUID, pero los ID externos son opcionales.
- AWS IoT SiteWise nunca genera identificadores externos. Los proporciona usted mismo.
- Si el objeto aún no tiene uno, puedes asignarle un identificador externo en cualquier momento.

Formato de los identificadores externos

Un identificador externo válido tiene las siguientes propiedades:

- Tiene una longitud de entre 2 y 128 caracteres.
- El primer y el último carácter deben ser alfanuméricos (A-Z, a-z, 0-9).
- Los caracteres que no sean el primero y el último deben ser alfanuméricos o bien alguno de los siguientes caracteres: `_-.:`

Por ejemplo, un identificador externo debe ajustarse a la siguiente expresión regular:

```
[a-zA-Z0-9][a-zA-Z0-9_\-.:]*[a-zA-Z0-9]+
```

Hacer referencia a objetos con identificadores externos

En muchos lugares en los que puede hacer referencia a un objeto mediante su UUID, puede utilizar su ID externo en su lugar, si lo tiene. Para ello, añade el ID externo a la cadena. `externalId:`

Por ejemplo, supongamos que tiene un modelo de activos cuyo UUID (ID del modelo de activo) es `a1b2c3d4-5678-90ab-cdef-11111EXAMPLE` y que también tiene el ID externo. `myExternalId` Llame DescribeAssetModelpara obtener más información al respecto. Puede utilizar cualquiera de los siguientes valores como valor de`assetModelId`:

- Con el propio ID del modelo de activo (UUID): `a1b2c3d4-5678-90ab-cdef-11111EXAMPLE`
- Con el ID externo: `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**
>
> El `externalId:` prefijo no forma parte, en sí mismo, del identificador externo. Solo debes proporcionar el prefijo cuando proporciones un ID externo a una operación de API que acepte UUID o ID externos. Por ejemplo, proporciona el prefijo cuando consultes o actualices un objeto existente.
> Al definir un identificador externo para un objeto, por ejemplo, al crear un modelo de activos, no incluya el prefijo.

De este modo, puedes usar identificadores externos en lugar de UUID para muchas operaciones de API AWS IoT SiteWise, pero no para todas. Por ejemplo, el GetAssetPropertyValue, debe usar UUID; no admite el uso de ID externos.

Para determinar si una operación de API en particular admite este uso, consulta la referencia de la API.

Creación de modelos de activos y modelos de componentes

AWS IoT SiteWise los modelos de activos y los modelos de componentes impulsan la estandarización de sus datos industriales. Un modelo de activos o un modelo de componentes

contiene un nombre, una descripción, propiedades de los activos y (opcionalmente) modelos compuestos personalizados que agrupan propiedades o que hacen referencia a modelos de componentes para subconjuntos.

- Se utiliza un modelo de activos para crear activos. Además de las características enumeradas anteriormente, un modelo de activos también puede contener definiciones jerárquicas que definan las relaciones entre los activos.
- Un modelo de componentes representa un subconjunto dentro de un modelo de activos u otro modelo de componentes. Al crear un modelo de componente, puede añadir referencias al mismo en los modelos de activos y en otros modelos de componentes. Sin embargo, no puede crear activos directamente a partir de los modelos de componentes.

Tras crear un modelo de activos o un modelo de componentes, puede crear modelos compuestos personalizados para agrupar propiedades o hacer referencia a los modelos de componentes existentes.

Para obtener información detallada sobre cómo crear modelos de activos y modelos de componentes, consulte las siguientes secciones.

Temas

Creación de modelos de activos

AWS IoT SiteWise los modelos de activos impulsan la estandarización de sus datos industriales. Un modelo de activos contiene el nombre, la descripción, las propiedades de activos y las definiciones de jerarquía de activos. Por ejemplo, puede definir un modelo de turbina eólica con propiedades de temperatura, rotaciones por minuto (RPM) y potencia. A continuación, puede definir un modelo de parque eólico con una propiedad de salida de potencia neta y una definición de jerarquía de turbina eólica.

> **Note**
>
> - Le recomendamos que modele su operación comenzando con los nodos de nivel más bajo. Por ejemplo, cree el modelo de turbina eólica antes de crear el modelo de parque eólico. Las definiciones de jerarquía de activos contienen referencias a modelos de activos existentes. Con este enfoque, puede definir jerarquías de activos a medida que crea sus modelos.
> - Los modelos de activos no pueden contener otros modelos de activos. Si debe definir un modelo al que pueda hacer referencia como subensamblaje dentro de otro modelo, debe crear un modelo de component--> en su lugar. Para obtener más información, consulte Creación de modelos de componentes.

En las siguientes secciones se describe cómo utilizar la AWS IoT SiteWise consola o la API para crear modelos de activos. En las secciones siguientes también se describen los diferentes tipos de propiedades y jerarquías de activos que se pueden utilizar para crear modelos.

Temas

Creación de un modelo de activos (consola)

Puede usar la AWS IoT SiteWise consola para crear un modelo de activos. La AWS IoT SiteWise consola ofrece varias funciones, como el autocompletado de fórmulas, que pueden ayudarle a definir modelos de activos válidos.

Para crear un modelo de activos (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Models (Modelos).
3. Seleccione Crear modelo.
4. En la página Crear un modelo, haga lo siguiente:

a. Escriba un Nombre para el modelo de activos, como **`Wind Turbine`** o **`Wind Turbine Model`**. Este nombre debe ser único en todos los modelos de su cuenta en esta región.

b. (Opcional) Añada un identificador externo para el modelo. Se trata de un identificador definido por el usuario. Para obtener más información, consulte Hacer referencia a objetos con identificadores externos en la Guía del usuario de AWS IoT SiteWise .

c. (Opcional) Agregue Definiciones de mediciones para el modelo. Las mediciones representan flujos de datos de su equipo. Para obtener más información, consulte Definición de flujos de datos procedentes del equipo (mediciones).

d. (Opcional) Agregue Definiciones de transformación para el modelo. Las transformaciones son fórmulas que asignan datos de un formulario a otro. Para obtener más información, consulte Transformación de datos (transformaciones).

e. (Opcional) Agregue Definiciones de métricas para el modelo. Las métricas son fórmulas que agregan datos a lo largo de intervalos de tiempo. Las métricas pueden agregar datos de entrada de activos asociados, de modo que puede calcular valores que representan la operación o un subconjunto de la operación. Para obtener más información, consulte Agregación de datos de propiedades y otros activos (métricas).

f. (Opcional) Agregue Definiciones de la jerarquía para el modelo. Las jerarquías son relaciones entre activos. Para obtener más información, consulte Definición de jerarquías de modelos de activos.

g. (Opcional) Agregue etiquetas para el modelo de activos. Para obtener más información, consulte Etiquetar sus recursos AWS IoT SiteWise.

h. Seleccione Crear modelo.

Al crear un modelo de activos, la AWS IoT SiteWise consola navega hasta la página del nuevo modelo. En esta página, puede consultar el Estado del modelo, que inicialmente es CREANDO. Esta página se actualiza automáticamente, por lo que puede esperar a que se actualice el estado del modelo.

> **Note**
>
> El proceso de creación de un modelo de activos puede tardar unos minutos para modelos complejos. Una vez que el estado del modelo de activos sea ACTIVO, puede utilizar el modelo de activos para crear activos. Para obtener más información, consulte Estados de activos y modelos.

5. (Opcional) Tras crear el modelo de activo, puede configurarlo para la periferia. Para obtener más información sobre SiteWise Edge, consulteHabilitación del procesamiento de datos de la periferia.

   a. En la página del modelo, elija Configurar para Edge.

   b. En la página de configuración del modelo, elija la configuración de periferia para el modelo. Esto controla dónde se AWS IoT SiteWise pueden calcular y almacenar las propiedades asociadas a este modelo de activos. Para obtener más información acerca de la configuración del modelo para la periferia, consulte the section called “Configuración de la capacidad de periferia”.

   c. Para la configuración perimetral personalizada, elija la ubicación en la que desee AWS IoT SiteWise calcular y almacenar cada una de las propiedades del modelo de activos.

      > **Note**
      >
      > Las transformaciones y las métricas asociadas deben configurarse para la misma ubicación. Para obtener más información acerca de la configuración del modelo para la periferia, consulte the section called “Configuración de la capacidad de periferia”.

   d. Seleccione Guardar. En la página del modelo, su Configuración de periferia ahora debería estar Configurada.

Crear un modelo de activos (AWS CLI)

Puede usar AWS Command Line Interface (AWS CLI) para crear un modelo de activos.

Utilice la CreateAssetModeloperación para crear un modelo de activos con propiedades y jerarquías. Esta operación espera una carga con la siguiente estructura.

```
{
  "assetModelType": "ASSET_MODEL",
  "assetModelName": "String",
  "assetModelDescription": "String",
  "assetModelProperties": Array of AssetModelProperty,
  "assetModelHierarchies": Array of AssetModelHierarchyDefinition
}
```

Para crear un modelo de activos ()AWS CLI

1. Cree un archivo llamado `asset-model-payload.json` y, a continuación, copie el siguiente objeto JSON en el archivo.

```
{
  "assetModelType": "ASSET_MODEL",
  "assetModelName": "",
  "assetModelDescription": "",
  "assetModelProperties": [

  ],
  "assetModelHierarchies": [

  ],
  "assetModelCompositeModels": [

  ]
}
```

2. Use su editor de texto JSON preferido para editar el archivo `asset-model-payload.json` para lo que se muestra a continuación:

   a. Escriba un nombre (`assetModelName`) para el modelo de activos, como **`Wind Turbine`** o **`Wind Turbine Model`**. Este nombre debe ser único en todos los modelos de activos y modelos de componentes de su cuenta Región de AWS.

   b. (Opcional) Introduzca un identificador externo (`assetModelExternalId`) para el modelo de activos. Se trata de un ID definido por el usuario. Para obtener más información, consulte Hacer referencia a objetos con identificadores externos en la Guía del usuario de AWS IoT SiteWise .

   c. (Opcional) Escriba una descripción (`assetModelDescription`) para el modelo de activos o elimine el par de clave-valor `assetModelDescription`.

   d. (Opcional) Defina las propiedades del activo (`assetModelProperties`) para el modelo. Para obtener más información, consulte Definición de las propiedades de datos.

   e. (Opcional) Defina jerarquías de activos (`assetModelHierarchies`) para el modelo. Para obtener más información, consulte Definición de jerarquías de modelos de activos.

   f. (Opcional) Defina las alarmas para el modelo. Las alarmas monitorean otras propiedades para que pueda identificar cuándo requieren atención los equipos o procesos. Cada definición de alarma es un modelo compuesto (`assetModelCompositeModels`) que

estandariza el conjunto de propiedades que utiliza la alarma. Para obtener más información, consulte Monitoreo de datos con alarmas y Definición de alarmas en los modelos de activos.

g. (Opcional) Agregue etiquetas (`tags`) para el modelo de activos. Para obtener más información, consulte Etiquetar sus recursos AWS IoT SiteWise.

3. Ejecute el siguiente comando para crear un modelo de activos a partir de la definición en el archivo JSON.

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

La operación devuelve una respuesta que contiene `assetModelId` al que hace referencia al crear un activo. La respuesta también contiene el estado del modelo (`assetModelStatus.state`), que es inicialmente `CREATING`. El estado del modelo de activos es `CREATING` hasta que se propagan los cambios.

> **Note**
>
> El proceso de creación de un modelo de activos puede tardar unos minutos para modelos complejos. Para comprobar el estado actual de su modelo de activos, utilice la DescribeAssetModeloperación especificando el`assetModelId`. Una vez que el estado del modelo de activos sea `ACTIVE`, puede utilizarlo para crear activos. Para obtener más información, consulte Estados de activos y modelos.

4. (Opcional) Cree modelos compuestos personalizados para su modelo de activos. Con los modelos compuestos personalizados, puede agrupar propiedades dentro del modelo o incluir un subensamblaje haciendo referencia a un modelo de componente. Para obtener más información, consulte Creación de modelos compuestos personalizados (componentes).

Modelos de activos de ejemplo

Esta sección contiene ejemplos de definiciones de modelos de activos que puede utilizar para crear modelos de activos con los SDK AWS CLI y AWS IoT SiteWise . Estos modelos de activos representan una turbina eólica y un parque eólico. Los activos de las turbinas eólicas ingieren datos sin procesar de los sensores y calculan valores como la potencia y la velocidad media del viento. Los activos del parque eólico calculan valores como la potencia total de todas las turbinas eólicas del parque eólico.

Temas

- Modelo de activos de turbina eólica
- Modelo de activos de parque eólico

Modelo de activos de turbina eólica

El siguiente modelo de activos representa una turbina en un parque eólico. La turbina eólica ingiere los datos de los sensores para calcular valores como la potencia y la velocidad media del viento.

> **Note**
>
> Este modelo de ejemplo se parece al modelo de aerogenerador de la AWS IoT SiteWise demostración. Para obtener más información, consulte Uso de la AWS IoT SiteWise demostración.

```
{
  "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": []
}
```

Modelo de activos de parque eólico

El siguiente modelo de activos representa un parque eólico que comprende varias turbinas eólicas. Este modelo de activos define una jerarquía con respecto al modelo de turbinas eólicas. Esto permite

al parque eólico calcular valores (como la potencia media) a partir de los datos de todas las turbinas eólicas del parque eólico.

> **Note**
>
> Este modelo de ejemplo se parece al modelo de parque eólico de la AWS IoT SiteWise demostración. Para obtener más información, consulte Uso de la AWS IoT SiteWise demostración.

Este modelo de activos depende de Modelo de activos de turbina eólica. Sustituya los valores `propertyId` y `childAssetModelId` por los de un modelo de activos de turbina eólica existente.

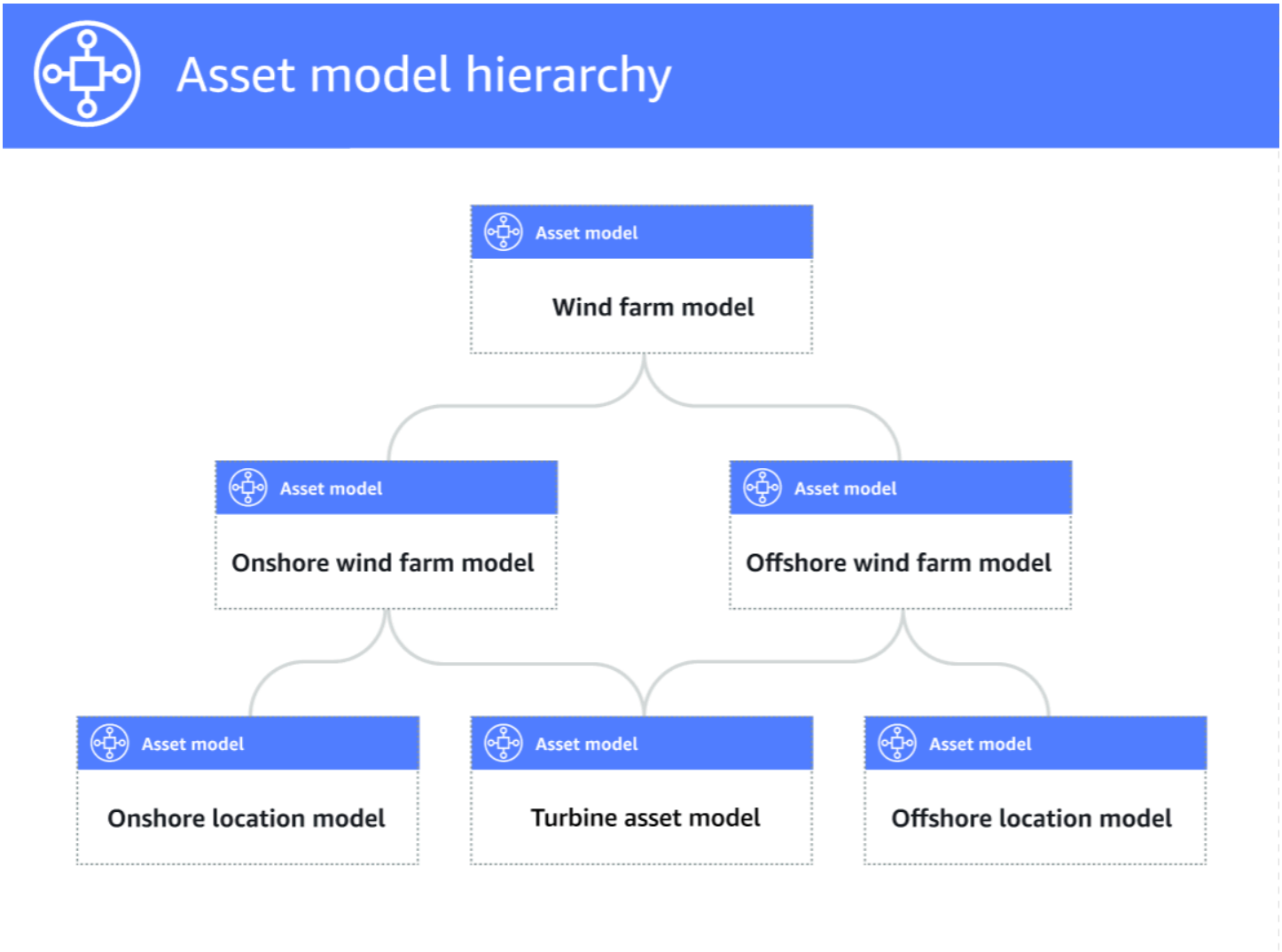
```
{
  "assetModelName": "Wind Farm Asset Model",
  "assetModelDescription": "Represents a wind farm.",
  "assetModelProperties": [
    {
      "name": "Code",
      "dataType": "INTEGER",
      "type": {
        "attribute": {
          "defaultValue": "300"
        }
      }
    },
    {
      "name": "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"
    }
  ]
}
```

Definición de jerarquías de modelos de activos

Puede definir jerarquías de modelos de activos para crear asociaciones lógicas entre los modelos de activos de su operación industrial. Por ejemplo, puede definir un parque eólico compuesto por parques eólicos terrestres y marinos. Un parque eólico terrestre contiene una turbina y una ubicación terrestre. Un parque eólico marino contiene una turbina y una ubicación en alta mar.



Cuando asocia un modelo de activo secundario con un activo principal mediante una jerarquía, las métricas del modelo de activo principal pueden agregar datos de las métricas del modelo de activo secundario. Puede utilizar jerarquías y métricas de modelos de activos para calcular estadísticas que proporcionan información sobre la operación o un subconjunto de la operación. Para obtener más información, consulte Agregación de datos de propiedades y otros activos (métricas).

Cada jerarquía define una relación entre un modelo de activo principal y un modelo de activo secundario. En un modelo de activo principal, puede definir varias jerarquías para el mismo modelo de entidad secundaria. Por ejemplo, si tiene dos tipos diferentes de aerogeneradores en sus parques eólicos, donde todos los aerogeneradores están representados por el mismo modelo de activo, puede definir una jerarquía para cada tipo. A continuación, puede definir métricas en el modelo de parque eólico para calcular estadísticas independientes y combinadas para cada tipo de aerogenerador.

Un modelo de activo principal se puede asociar a varios modelos de entidades secundarias. Por ejemplo, si tiene un parque eólico terrestre y un parque eólico marino representados por dos modelos de activos diferentes, puede asociar estos modelos de activos al mismo modelo de activo del parque eólico principal.

También se puede asociar un modelo de entidades secundarias a varios modelos de activos principales. Por ejemplo, si tiene dos tipos diferentes de parques eólicos, en los que todos los aerogeneradores están representados por el mismo modelo de activos, puede asociar el modelo de activos de los aerogeneradores a distintos modelos de activos de parques eólicos.

> **Note**
>
> Al definir una jerarquía de modelos de activos, el modelo de activos secundario debe estar `ACTIVE` o tener una versión `ACTIVE` anterior. Para obtener más información, consulte Estados de activos y modelos.

Después de definir modelos de activos jerárquicos y crear activos, puede asociar los activos para completar la relación principal-secundario. Para obtener más información, consulte Creación de activos y Asociación y disociación de activos.

Temas

- Definición de jerarquías de modelos de activos (consola)
- Definición de jerarquías de activos ()AWS CLI

Definición de jerarquías de modelos de activos (consola)

Al definir una jerarquía para un modelo de activos en la AWS IoT SiteWise consola, se especifican los siguientes parámetros:

- Nombre de la jerarquía: el nombre de la jerarquía, por ejemplo **`Wind Turbines`**.
- Modelo de la jerarquía: el modelo de entidad secundaria.
- ID externo de jerarquía (opcional): se trata de un ID definido por el usuario. Para obtener más información, consulte Hacer referencia a objetos con identificadores externos en la Guía del usuario de AWS IoT SiteWise .

Para obtener más información, consulte Creación de un modelo de activos (consola).

Definición de jerarquías de activos ()AWS CLI

Al definir una jerarquía para un modelo de activos con la AWS IoT SiteWise API, se especifican los siguientes parámetros:

- `name`: el nombre de la jerarquía, por ejemplo **`Wind Turbines`**.
- `childAssetModelId`— El ID o el ID externo del modelo de activos secundario de la jerarquía. Puede utilizar la ListAssetModelsoperación para buscar el ID de un modelo de activos existente.

Example Definición de jerarquía de ejemplo

En el ejemplo siguiente, se muestra una jerarquía de modelos de activos que representa la relación de un parque eólico con las turbinas eólicas. Este objeto es un ejemplo de AssetModelHierarchy. Para obtener más información, consulte Crear un modelo de activos (AWS CLI).

```
{
  ...
  "assetModelHierarchies": [
    {
      "name": "Wind Turbines",
      "childAssetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE"
    },
  ]
}
```

Creación de modelos de componentes

Utilice los modelos de AWS IoT SiteWise componentes para definir subconjuntos a los que pueda hacer referencia desde modelos de activos u otros modelos de componentes. De esta forma, puede reutilizar la definición del componente en varios modelos diferentes o varias veces dentro del mismo modelo.

El proceso de definición de un modelo de componentes es muy similar a la definición de un modelo de activos. Al igual que un modelo de activos, un modelo de componentes tiene un nombre, una descripción y propiedades de activos. Sin embargo, los modelos de componentes no pueden incluir definiciones de jerarquías de activos, ya que los modelos de componentes en sí mismos no se pueden utilizar para crear activos directamente. Los modelos de componentes tampoco pueden definir las alarmas.

Por ejemplo, puede definir un componente para un servomotor con las propiedades de temperatura del motor, temperatura del codificador y resistencia de aislamiento. A continuación, puede definir un modelo de activos para los equipos que contienen servomotores, como una máquina CNC.

> **Note**
>
> - Le recomendamos que modele su operación comenzando con los nodos de nivel más bajo. Por ejemplo, cree el componente del servomotor antes de crear el modelo de activos de la máquina CNC. Los modelos de activos contienen referencias a modelos de componentes existentes.
> - No puede crear un activo directamente a partir de un modelo de componentes. Para crear un activo que utilice su componente, debe crear un modelo de activo para su activo. A continuación, debe crear un modelo compuesto personalizado para él que haga referencia a su componente. Para obtener más información sobre la creación de modelos de activos, consulte Creación de modelos de activos Para obtener más información sobre la creación de modelos compuestos personalizados, consulteCreación de modelos compuestos personalizados (componentes).

En las siguientes secciones se describe cómo utilizar la AWS IoT SiteWise API para crear modelos de componentes.

Temas

Crear un modelo de componentes (AWS CLI)

Puede utilizar AWS Command Line Interface (AWS CLI) para crear un modelo de componentes.

Utilice la CreateAssetModeloperación para crear un modelo de componentes con propiedades. Esta operación espera una carga útil con la siguiente estructura:

```
{
  "assetModelType": "COMPONENT_MODEL",
  "assetModelName": "String",
  "assetModelDescription": "String",
  "assetModelProperties": Array of AssetModelProperty,
```

```
}
```

Para crear un modelo de componentes ()AWS CLI

1. Cree un archivo llamado `component-model-payload.json` y, a continuación, copie el siguiente objeto JSON en el archivo:

   ```
   {
     "assetModelType": "COMPONENT_MODEL",
     "assetModelName": "",
     "assetModelDescription": "",
     "assetModelProperties": [

     ]
   }
   ```

2. Use su editor de texto JSON preferido para editar el archivo `component-model-payload.json` para lo que se muestra a continuación:

   a. Introduzca un nombre (`assetModelName`) para el modelo del componente, como **`Servo Motor`** o**`Servo Motor Model`**. Este nombre debe ser único en todos los modelos de activos y modelos de componentes de su cuenta en esta Región de AWS.

   b. (Opcional) Introduzca un identificador externo (`assetModelExternalId`) para el modelo del componente. Se trata de un ID definido por el usuario. Para obtener más información, consulte Hacer referencia a objetos con identificadores externos en la Guía del usuario de AWS IoT SiteWise .

   c. (Opcional) Escriba una descripción (`assetModelDescription`) para el modelo de activos o elimine el par de clave-valor `assetModelDescription`.

   d. (Opcional) Defina las propiedades de los activos (`assetModelProperties`) para el modelo de componentes. Para obtener más información, consulte Definición de las propiedades de datos.

   e. (Opcional) Agregue etiquetas (`tags`) para el modelo de activos. Para obtener más información, consulte Etiquetar sus recursos AWS IoT SiteWise.

3. Ejecute el siguiente comando para crear un modelo de componentes a partir de la definición del archivo JSON.

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

La operación devuelve una respuesta que contiene la respuesta a la `assetModelId` que hace referencia al añadir una referencia a su modelo de componentes en un modelo de activos o en otro modelo de componentes. La respuesta también contiene el estado del modelo (`assetModelStatus.state`), que es inicialmente `CREATING`. El estado del modelo de componentes es `CREATING` hasta que se propaguen los cambios.

> **Note**
>
> El proceso de creación del modelo de componentes puede tardar unos minutos en el caso de modelos complejos. Para comprobar el estado actual del modelo de componentes, utilice la DescribeAssetModeloperación especificando el`assetModelId`. Una vez que el estado del modelo de componentes sea`ACTIVE`, puede añadir referencias a su modelo de componentes en modelos de activos u otros modelos de componentes. Para obtener más información, consulte Estados de activos y modelos.

4. (Opcional) Cree modelos compuestos personalizados para su modelo de componente. Con los modelos compuestos personalizados, puede agrupar propiedades dentro del modelo o incluir un subensamblaje haciendo referencia a otro modelo de componente. Para obtener más información, consulte Creación de modelos compuestos personalizados (componentes).

Ejemplo de modelo de componentes

Esta sección contiene un ejemplo de definición de modelo de componentes que puede utilizar para crear un modelo de componentes con los AWS IoT SiteWise SDK AWS CLI y. Este modelo de componentes representa un servomotor que se puede utilizar en otro equipo, como una máquina CNC.

Temas

- Modelo de componentes de servomotor

Modelo de componentes de servomotor

El siguiente modelo de componentes representa un servomotor que se puede utilizar en equipos como máquinas CNC. El servomotor proporciona diversas medidas, como la temperatura y la resistencia eléctrica. Estas medidas están disponibles como propiedades en los activos creados a partir de modelos de activos que hacen referencia al modelo de componentes del servomotor.

```
{
    "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"
        }
    ]
}
```

Definición de las propiedades de datos

Las propiedades de activo son las estructuras dentro de cada activo que contienen datos del activo. Las propiedades de un activo pueden ser cualquiera de los siguientes tipos:

- Atributos: las propiedades generalmente estáticas de un activo, como el fabricante del dispositivo o la región geográfica. Para obtener más información, consulte Definición de datos estáticos (atributos).
- Mediciones: flujos de datos sin procesar de un activo procedentes del sensor de un dispositivo, como los valores de velocidad de rotación con marca temporal o los valores de temperatura en grados Celsius con marca temporal. Una medida se define mediante un alias de flujo de datos. Para obtener más información, consulte Definición de flujos de datos procedentes del equipo (mediciones).
- Transformaciones: valores de serie temporal de un activo transformados, como los valores de temperatura en grados Fahrenheit con marca temporal. Una transformación se define por una expresión y las variables que se consumen con esa expresión. Para obtener más información, consulte Transformación de datos (transformaciones).

- Métricas: los datos de un activo agregados durante un intervalo de tiempo específico, como la temperatura media por hora. Una métrica se define mediante un intervalo de tiempo, una expresión y las variables que se consumen con esa expresión. Las expresiones métricas pueden introducir las propiedades métricas de los activos asociados, para que pueda calcular las métricas que representan su operación o un subconjunto de la misma. Para obtener más información, consulte Agregación de datos de propiedades y otros activos (métricas).

Para obtener más información, consulte Creación de modelos de activos.

Para obtener un ejemplo de cómo utilizar mediciones, transformaciones y métricas para calcular la efectividad global del equipo (OEE), consulte Calcular el OEE en AWS IoT SiteWise.

Temas

- Definición de datos estáticos (atributos)
- Definición de flujos de datos procedentes del equipo (mediciones)
- Transformación de datos (transformaciones)
- Agregación de datos de propiedades y otros activos (métricas)
- Uso de expresiones de fórmula

Definición de datos estáticos (atributos)

Los atributos de activos representan información que generalmente es estática, como el fabricante del dispositivo o la ubicación geográfica. Cada activo creado a partir de un modelo de activos contiene los atributos de dicho modelo.

Temas

- Definición de atributos (consola)
- Definición de atributos ()AWS CLI

Definición de atributos (consola)

Al definir un atributo para un modelo de activos en la AWS IoT SiteWise consola, se especifican los siguientes parámetros:

- Nombre: el nombre de la propiedad.

- Valor predeterminado – (Opcional) El valor predeterminado de este atributo. Los activos creados a partir del modelo tienen este valor para el atributo. Para obtener más información acerca de cómo reemplazar el valor por defecto en un activo creado a partir de un modelo, consulte Actualización de valores de atributos.
- Tipo de datos: el tipo de datos de la propiedad, que es uno de los siguientes:
  - Cadena – Una cadena con hasta 1024 bytes.
  - Entero – Un entero de 32 bits con signo con rango [-2.147.483.648, 2.147.483.647].
  - Doble – Un número de punto flotante con rango [-10^100, 10^100] e IEEE 754 doble precisión.
  - Booleano: `true` o `false`.
- ID externo: (opcional) Este es un ID definido por el usuario. Para obtener más información, consulte Hacer referencia a objetos con identificadores externos en la Guía del usuario de AWS IoT SiteWise .

Para obtener más información, consulte Creación de un modelo de activos (consola).

Definición de atributos ()AWS CLI

Al definir un atributo para un modelo de activos con la AWS IoT SiteWise API, se especifican los siguientes parámetros:

- `name`: el nombre de la propiedad.
- `defaultValue` – (Opcional) El valor predeterminado de este atributo. Los activos creados a partir del modelo tienen este valor para el atributo. Para obtener más información acerca de cómo reemplazar el valor por defecto en un activo creado a partir de un modelo, consulte Actualización de valores de atributos.
- `dataType`: el tipo de datos de la propiedad, que es uno de los siguientes:
  - `STRING` – Una cadena con hasta 1024 bytes.
  - `INTEGER`: un entero de 32 bits con signo con rango [-2.147.483.648, 2.147.483.647].
  - `DOUBLE`: un número de punto flotante con rango [-10^100, 10^100] e IEEE 754 doble precisión.
  - `BOOLEAN` – `true` o `false`.
- `externalId`— (Opcional) Se trata de un ID definido por el usuario. Para obtener más información, consulte Hacer referencia a objetos con identificadores externos en la Guía del usuario de AWS IoT SiteWise .

Example Definición de atributo de ejemplo

En el ejemplo siguiente se muestra un atributo que representa el número de modelo de un activo con un valor predeterminado. Este objeto es un ejemplo de un objeto AssetModelPropertyque contiene un atributo. Puede especificar este objeto como parte de la carga útil de la CreateAssetModelsolicitud para crear una propiedad de atributo. Para obtener más información, consulte Crear un modelo de activos (AWS CLI).

```
{
...
"assetModelProperties": [
{
  "name": "Model number",
  "dataType": "STRING",
  "type": {
    "attribute": {
      "defaultValue": "BLT123"
    }
  }
}
],
...
}
```

Definición de flujos de datos procedentes del equipo (mediciones)

Una medición representa el flujo de datos sin formato del sensor de un dispositivo, como los valores de temperatura con marca de tiempo o los valores de revoluciones por minuto (RPM) con marca de tiempo.

Temas

- Definición de medidas (consola)
- Definición de medidas ()AWS CLI

Definición de medidas (consola)

Al definir una medida para un modelo de activos en la AWS IoT SiteWise consola, se especifican los siguientes parámetros:

- Nombre: el nombre de la propiedad.

- Unidad: (opcional) la unidad científica de la propiedad, como mm o Celsius.
- Tipo de datos: el tipo de datos de la propiedad, que es uno de los siguientes:
  - Cadena – Una cadena con hasta 1024 bytes.
  - Entero – Un entero de 32 bits con signo con rango [-2.147.483.648, 2.147.483.647].
  - Doble – Un número de punto flotante con rango [-10^100, 10^100] e IEEE 754 doble precisión.
  - Booleano: `true` o `false`.
- ID externo: (opcional) Este es un ID definido por el usuario. Para obtener más información, consulte Hacer referencia a objetos con identificadores externos en la Guía del usuario de AWS IoT SiteWise .

Para obtener más información, consulte Creación de un modelo de activos (consola).

Definición de medidas ()AWS CLI

Al definir una medición para un modelo de activos con la AWS IoT SiteWise API, se especifican los siguientes parámetros:

- `name`: el nombre de la propiedad.
- `dataType`: el tipo de datos de la propiedad, que es uno de los siguientes:
  - `STRING` – Una cadena con hasta 1024 bytes.
  - `INTEGER`: un entero de 32 bits con signo con rango [-2.147.483.648, 2.147.483.647].
  - `DOUBLE`: un número de punto flotante con rango [-10^100, 10^100] e IEEE 754 doble precisión.
  - `BOOLEAN` – `true` o `false`.
- `unit`: (opcional) la unidad científica de la propiedad, como mm o Celsius.
- `externalId`— (Opcional) Se trata de un ID definido por el usuario. Para obtener más información, consulte Hacer referencia a objetos con identificadores externos en la Guía del usuario de AWS IoT SiteWise .

Example Definición de medida de ejemplo

En el ejemplo siguiente se muestra una medición que representa las lecturas del sensor de temperatura de un activo. Este objeto es un ejemplo de un objeto AssetModelPropertyque contiene una medición. Puede especificar este objeto como parte de la carga útil de la CreateAssetModelsolicitud para crear una propiedad de medición. Para obtener más información, consulte Crear un modelo de activos (AWS CLI).

La estructura Medida es una estructura vacía cuando define un modelo de activos, ya que más adelante configurará cada activo para que utilice flujos de datos de dispositivos únicos. Para obtener más información acerca de cómo conectar la propiedad de medición de un activo al flujo de datos del sensor de un dispositivo, consulte Asignación de flujos de datos industriales a propiedades de activos.

```
{
      ...
      "assetModelProperties": [
      {
          "name": "Temperature C",
          "dataType": "DOUBLE",
          "type": {
              "measurement": {}
          },
          "unit": "Celsius"
      }
  ],
      ...
}
```

Transformación de datos (transformaciones)

Las transformaciones son expresiones matemáticas que asignan puntos de datos de la propiedad de un activo de un formulario a otro. Una expresión de transformación consta de variables de propiedad de activos, literales, operadores y funciones comunes. Los puntos de datos transformados mantienen una one-to-one relación con los puntos de datos de entrada. AWS IoT SiteWise calcula un nuevo punto de datos transformado cada vez que alguna de las propiedades de entrada recibe un nuevo punto de datos.

Por ejemplo, si su activo tiene un flujo de medición de temperatura denominado `Temperature_C` con unidades en Celsius, puede convertir cada punto de datos a Fahrenheit con la fórmula `Temperature_F = 9/5 * Temperature_C + 32`. Cada vez que AWS IoT SiteWise recibe un punto de datos en el flujo de `Temperature_C` medición, el `Temperature_F` valor correspondiente se calcula en unos segundos y está disponible como `Temperature_F` propiedad.

Si la transformación contiene más de una variable, el punto de datos que llegue antes inicia el cálculo inmediatamente. Considere un ejemplo en el que un fabricante de piezas utiliza una transformación para monitorear la calidad del producto. Aplicando estándares diferentes según el tipo de pieza, el fabricante utiliza las siguientes mediciones para representar el proceso:

- `Part_Number`: una cadena que identifica el tipo de pieza.
- `Good_Count`: un número entero que aumenta en uno si la pieza cumple el estándar.
- `Bad_Count`: un número entero que aumenta en uno si la pieza no cumple el estándar.

El fabricante crea además una transformación `Quality_Monitor`, que equivale a `if(eq(Part_Number, "BLT123") and (Bad_Count / (Good_Count + Bad_Count) > 0.1), "Caution", "Normal")`.

Esta transformación monitorea el porcentaje de piezas defectuosas producidas para un tipo de pieza específico. Si el número de pieza es BLT123 y el porcentaje de piezas defectuosas supera el 10 por ciento (0,1), la transformación devuelve el mensaje `"Caution"`. De lo contrario, la transformación devuelve el mensaje `"Normal"`.

> **Note**
>
> - Si `Part_Number` recibe un nuevo punto de datos antes que otras mediciones, la transformación de `Quality_Monitor` utiliza el nuevo valor de `Part_Number` y los valores de `Good_Count` y `Bad_Count` más recientes. Para evitar errores, reinicie `Good_Count` y `Bad_Count` antes de la siguiente ronda de fabricación.
> - Utilice las métricas si quiere evaluar las expresiones solo después de que todas las variables hayan recibido nuevos puntos de datos.

Temas

- Definición de transformaciones (consola)
- Definir transformaciones (AWS CLI)

Definición de transformaciones (consola)

Al definir una transformación para un modelo de activos en la AWS IoT SiteWise consola, se especifican los siguientes parámetros:

- Nombre: el nombre de la propiedad.
- Unidad: (opcional) la unidad científica de la propiedad, como mm o Celsius.
- Tipo de datos: el tipo de datos de la transformación, que puede ser Doble o Cadena.

- ID externo: (opcional) Este es un ID definido por el usuario. Para obtener más información, consulte Hacer referencia a objetos con identificadores externos en la Guía del usuario de AWS IoT SiteWise .
- Fórmula: la expresión de transformación. Las expresiones de transformación no pueden usar funciones de agregación ni funciones temporales. Para abrir la función de autocompletar, comienza a escribir o presiona la tecla de flecha hacia abajo. Para obtener más información, consulte Uso de expresiones de fórmula.

> **Important**
>
> Las transformaciones pueden agregar propiedades de tipo entero, doble, booleano o cadena. Los valores booleanos se convierten en `0` (falso) y `1` (verdadero).
> Las transformaciones deben especificar una o más propiedades que no sean atributos y cualquier número de propiedades de atributo. AWS IoT SiteWise calcula un nuevo punto de datos transformado cada vez que la propiedad de entrada de no atributo recibe un nuevo punto de datos. Los nuevos valores de atributo no lanzan actualizaciones de transformación. La misma tasa de solicitudes para las operaciones de la API de datos de propiedades de activos se aplica a los resultados del cálculo de transformaciones.
> Las expresiones de fórmula solo pueden generar valores dobles o de cadena. Las expresiones anidadas pueden generar otros tipos de datos, como cadenas, pero la fórmula en su conjunto debe evaluarse como un número o una cadena. Puede usar la función jp para convertir una cadena en un número. El valor booleano debe ser 1 (verdadero) o 0 (falso). Para obtener más información, consulte Valores indefinidos, infinitos y de desbordamiento.

Para obtener más información, consulte Creación de un modelo de activos (consola).

Definir transformaciones (AWS CLI)

Al definir una transformación para un modelo de activos con la AWS IoT SiteWise API, se especifican los siguientes parámetros:

- `name`: el nombre de la propiedad.
- `unit`: (opcional) la unidad científica de la propiedad, como mm o Celsius.
- `dataType`: el tipo de datos de la transformación, que debe ser `DOUBLE` o `STRING`.

- `externalId`— (Opcional) Se trata de un ID definido por el usuario. Para obtener más información, consulte Hacer referencia a objetos con identificadores externos en la Guía del usuario de AWS IoT SiteWise .
- `expression` – Una expresión de transformación. Las expresiones de transformación no pueden usar funciones de agregación ni funciones temporales. Para obtener más información, consulte Uso de expresiones de fórmula.
- `variables` – Una lista de variables que define las otras propiedades del activo que se van a utilizar en la expresión. Cada estructura de variable contiene un nombre sencillo para utilizar en la expresión y una estructura de `value` que identifica qué propiedad vincular a esa variable. La estructura `value` contiene la siguiente información:
  - `propertyId`: el ID de la propiedad desde la que se van a introducir los valores. Puede usar el nombre de la propiedad en lugar de su ID.

> **Important**
>
> Las transformaciones pueden agregar propiedades de tipo entero, doble, booleano o cadena. Los valores booleanos se convierten en `0` (falso) y `1` (verdadero).
> Las transformaciones deben especificar una o más propiedades que no sean atributos y cualquier número de propiedades de atributo. AWS IoT SiteWise calcula un nuevo punto de datos transformado cada vez que la propiedad de entrada de no atributo recibe un nuevo punto de datos. Los nuevos valores de atributo no lanzan actualizaciones de transformación. La misma tasa de solicitudes para las operaciones de la API de datos de propiedades de activos se aplica a los resultados del cálculo de transformaciones.
> Las expresiones de fórmula solo pueden generar valores dobles o de cadena. Las expresiones anidadas pueden generar otros tipos de datos, como cadenas, pero la fórmula en su conjunto debe evaluarse como un número o una cadena. Puede usar la función jp para convertir una cadena en un número. El valor booleano debe ser 1 (verdadero) o 0 (falso). Para obtener más información, consulte Valores indefinidos, infinitos y de desbordamiento.

Example definición de transformación

El siguiente ejemplo muestra una propiedad de transformación que convierte los datos de medición de temperatura de un activo de Celsius a Fahrenheit. Este objeto es un ejemplo de un objeto AssetModelPropertyque contiene una transformación. Puedes especificar este objeto como parte

de la carga útil de la CreateAssetModelsolicitud para crear una propiedad de transformación. Para obtener más información, consulte Crear un modelo de activos (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 definición de transformación que contiene tres variables

En el siguiente ejemplo, se muestra una propiedad de transformación que devuelve un mensaje de advertencia (`"Caution"`) si más del 10 por ciento de las piezas del BLT123 no cumplen el estándar. De lo contrario, devuelve un mensaje 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"
                }
            }
        ]
    }
}
}
...
}
```

Agregación de datos de propiedades y otros activos (métricas)

Las métricas son expresiones matemáticas que utilizan funciones agregadas para procesar todos los puntos de datos de entrada y generar un único punto de datos por intervalo de tiempo especificado. Por ejemplo, una métrica puede calcular la temperatura media por hora a partir de un flujo de datos de temperatura.

Las métricas pueden agregar datos de métricas de activos asociados, de modo que puede calcular estadísticas que proporcionan información sobre la operación o un subconjunto de la operación. Por ejemplo, una métrica puede calcular la temperatura media por hora en todas las turbinas eólicas de un parque eólico. Para obtener más información acerca de cómo definir asociaciones entre activos, consulte Definición de jerarquías de modelos de activos.

Las métricas también pueden introducir datos de otras propiedades sin agregar datos en cada intervalo de tiempo. Si se especifica un atributo en una fórmula, AWS IoT SiteWise utiliza el valor más reciente de ese atributo al calcular la fórmula. Si especifica una métrica en una fórmula, AWS IoT SiteWise utiliza el último valor del intervalo de tiempo durante el que calcula la fórmula. Esto significa que se pueden definir métricas como `OEE = Availability * Quality * Performance`, donde `Availability`, `Quality` y `Performance` son todas las demás métricas en el mismo modelo de activos.

AWS IoT SiteWise también calcula automáticamente un conjunto de métricas de agregación básicas para todas las propiedades de los activos. Para reducir los costos de cálculo, puede utilizar estos agregados en lugar de definir métricas personalizadas para cálculos básicos. Para obtener más información, consulte Consulta de agregados de propiedades de activos.

Temas

- Definición de métricas (consola)
- Definición de métricas ()AWS CLI

Definición de métricas (consola)

Al definir una métrica para un modelo de activos en la AWS IoT SiteWise consola, se especifican los siguientes parámetros:

- Nombre: el nombre de la propiedad.
- Tipo de datos: el tipo de datos de la transformación, que puede ser Doble o Cadena.
- ID externo: (opcional) Este es un ID definido por el usuario. Para obtener más información, consulte Hacer referencia a objetos con identificadores externos en la Guía del usuario de AWS IoT SiteWise .
- Fórmula: la expresión métrica. Las expresiones métricas pueden utilizar funciones de agregación para introducir datos de una propiedad para todos los activos asociados en una jerarquía. Comience a escribir o presione la tecla de flecha hacia abajo para abrir la característica de autocompletar. Para obtener más información, consulte Uso de expresiones de fórmula.

> **Important**
>
> Las métricas solo pueden agregar propiedades de tipo entero, doble, booleano o cadena. Los valores booleanos se convierten en `0` (falso) y `1` (verdadero).

Si define variables de entrada de métrica en la expresión de una métrica, esas entradas deben tener el mismo intervalo de tiempo que la métrica de salida.
Las expresiones de fórmula solo pueden generar valores dobles o de cadena. Las expresiones anidadas pueden generar otros tipos de datos, como cadenas, pero la fórmula en su conjunto debe evaluarse como un número o una cadena. Puede usar la función jp para convertir una cadena en un número. El valor booleano debe ser 1 (verdadero) o 0 (falso). Para obtener más información, consulte Valores indefinidos, infinitos y de desbordamiento.

- Intervalo de tiempo – Un intervalo de tiempo de métrica. AWS IoT SiteWise admite los siguientes intervalos de tiempo con periodos de saltos, donde cada intervalo comienza cuando termina el anterior:
  - 1 minuto: 1 minuto, calculado al final de cada minuto (00:00:00 h, 00:01:00 h, 00:02:00 h, etc.).
  - 5 minutos: 5 minutos, calculados al final de cada cinco minutos a partir de la hora en punto (00:00:00 h., 00:05:00 h., 00:10:00 h, etc.).
  - 15 minutos – 15 minutos, calculados al final de cada quince minutos a partir de la hora en punto (00:00:00 h., 00:15:00 h., 00:30:00 h, etc.).
  - 1 hora: 1 hora (60 minutos), calculados al final de cada hora en UTC (00:00:00 h, 01:00:00 h, 02:00:00 h, etc.).
  - 1 día: 1 día (24 horas), calculado al final de cada día en UTC (00:00:00 h del lunes, 00:00:00 h del martes, etc.).
  - 1 semana: 1 semana (7 días), calculada al final de cada domingo en UTC (todos los lunes a las 00:00:00 h).
  - Intervalo personalizado: puede escribir cualquier intervalo de tiempo entre un minuto y una semana.
- Desplazamiento de la fecha: (opcional) la fecha de referencia a partir de la cual se agregan los datos.
- Desplazamiento de la hora – (Opcional) la hora de referencia a partir de la cual se agregan los datos. El desplazamiento de la hora debe estar comprendido entre las 00:00:00 y las 23:59:59.
- Desplazamiento de la zona horaria: (opcional) la zona horaria de referencia. Si no se especifica, el desplazamiento predeteminado de la zona horaria es la hora universal coordinada (UTC).

Zonas horarias admitidas

- (UTC+00:00) Hora universal coordinada

- (UTC+01:00) Hora central europea
- (UTC+02:00) Europa del Este
- (UTC+03:00) Hora de África Oriental
- (UTC+04:00) Hora de Oriente Próximo
- (UTC+05:00) Hora de Lahore (Pakistán)
- (UTC+05:30) Hora estándar de India
- (UTC+06:00) Hora estándar de Bangladesh
- (UTC+07:00) Hora estándar de Vietnam
- (UTC+08:00) Hora de China Taiwán
- (UTC+09:00) Hora estándar de Japón
- (UTC+09:30) Hora central de Australia
- (UTC+10:00) Hora del Este de Australia
- (UTC+11:00) Hora estándar de Salomón
- (UTC+12:00) Hora estándar de Nueva Zelanda
- (UTC-11:00) Hora de las Islas Midway
- (UTC-10:00) Hora estándar de Hawái
- (UTC-09:00) Hora estándar de Alaska
- (UTC-08:00) Hora estándar del Pacífico
- (UTC-07:00) Hora estándar de Phoenix
- (UTC-06:00) Hora estándar central
- (UTC-05:00) Hora Estándar del Este
- (UTC-04:00) Hora de Puerto Rico y las Islas Vírgenes de los Estados Unidos
- (UTC-03:00) Hora estándar de Argentina
- (UTC-02:00) Hora de Georgia del Sur
- (UTC-01:00) Hora de África Central

Example intervalo de tiempo personalizado con un desplazamiento (consola)

El siguiente ejemplo muestra cómo definir un intervalo de tiempo de 12 horas con un desplazamiento el 20 de febrero de 2021 a las 18:30:30 h (Hora del Pacífico).

Para definir un intervalo personalizado con un desplazamiento

1. En Intervalo de tiempo, elija Intervalo personalizado.
2. Para Intervalo de tiempo, realice una de las siguientes acciones:
   - Escriba **`12`** y, a continuación, elija horas.
   - Escriba **`720`** y, a continuación, elija minutos.
   - Escriba **`43200`** y, a continuación, elija segundos.

   > **Important**
   >
   > El Intervalo de tiempo debe ser un número entero, independientemente de cuál sea la unidad.

3. En Desplazamiento de la fecha, elija 20/02/2021.
4. En Desplazamiento de la hora, escriba **`18:30:30`**.
5. Para el Desplazamiento de la zona horaria, elija (UTC-08:00), hora estándar del Pacífico.

Si crea la métrica el 1 de julio de 2021, antes o a las 18:30:30 (PST), obtendrá el primer resultado de agregación el 1 de julio de 2021 a las 18:30:30 (PST). El segundo resultado de la agregación se produce el 2 de julio de 2021 a las 06:30:30 a. m. (PST), y así sucesivamente.

Definición de métricas ()AWS CLI

Al definir una métrica para un modelo de activos con la AWS IoT SiteWise API, se especifican los siguientes parámetros:

- `name`: el nombre de la propiedad.
- `dataType`: el tipo de datos de la métrica, que puede ser `DOUBLE` o `STRING`.
- `externalId`— (Opcional) Se trata de un ID definido por el usuario. Para obtener más información, consulte Hacer referencia a objetos con identificadores externos en la Guía del usuario de AWS IoT SiteWise .
- `expression`: la expresión métrica. Las expresiones métricas pueden utilizar funciones de agregación para introducir datos de una propiedad para todos los activos asociados en una jerarquía. Para obtener más información, consulte Uso de expresiones de fórmula.

- `window`: el intervalo de tiempo y el desplazamiento de la ventana de saltos de la métrica, donde cada intervalo comienza cuando termina el anterior:
  - `interval`: el intervalo de tiempo para la ventana de caída. El intervalo de tiempo debe estar comprendido entre un minuto y una semana.
  - `offsets`: el desvío de la ventana de caída.

  Para obtener más información, consulte TumblingWindowla referencia de la AWS IoT SiteWise API.

  Example intervalo de tiempo personalizado con un desplazamiento (AWS CLI)

  El siguiente ejemplo muestra cómo definir un intervalo de tiempo de 12 horas con un desplazamiento el 20 de febrero de 2021 a las 18:30:30 h (Hora del Pacífico).

```
{
    "window": {
        "tumbling": {
            "interval": "12h",
            "offset": " 2021-07-23T18:30:30-08"
        }
    }
}
```

  Si creas la métrica el 1 de julio de 2021, antes o a las 18:30:30 (PST), obtendrás el primer resultado de agregación el 1 de julio de 2021 a las 18:30:30 (PST). El segundo resultado de la agregación se produce el 2 de julio de 2021 a las 06:30:30 a. m. (PST), y así sucesivamente.
- `variables`: una lista de variables que define las otras propiedades del activo o los activos secundarios que se van a utilizar en la expresión. Cada estructura de variable contiene un nombre sencillo para su uso en la expresión y una estructura `value` que identifica qué propiedad vincular a esa variable. La estructura `value` contiene la siguiente información:
  - `propertyId`: el ID de la propiedad desde la cual se extraen los valores. Puede utilizar el nombre de la propiedad en lugar de su identificador si la propiedad está definida en el modelo actual (en lugar de definirse en un modelo de una jerarquía).
  - `hierarchyId`: (opcional) el ID de la jerarquía desde la que se consultan las entidades secundarias de la propiedad. Puede utilizar el nombre de la definición de jerarquía en lugar de su ID. Si omite este valor, AWS IoT SiteWise busca la propiedad en el modelo actual.

> **Important**
>
> Las métricas solo pueden agregar propiedades de tipo entero, doble, booleano o cadena. Los valores booleanos se convierten en `0` (falso) y `1` (verdadero).
> Si define variables de entrada de métrica en la expresión de una métrica, esas entradas deben tener el mismo intervalo de tiempo que la métrica de salida.
> Las expresiones de fórmula solo pueden generar valores dobles o de cadena. Las expresiones anidadas pueden generar otros tipos de datos, como cadenas, pero la fórmula en su conjunto debe evaluarse como un número o una cadena. Puede usar la función jp para convertir una cadena en un número. El valor booleano debe ser 1 (verdadero) o 0 (falso). Para obtener más información, consulte Valores indefinidos, infinitos y de desbordamiento.

- `unit`: (opcional) la unidad científica de la propiedad, como mm o Celsius.

Example Definición de métrica de ejemplo

En el ejemplo siguiente se muestra una propiedad de métrica que agrega los datos de medición de temperatura de un activo para calcular la temperatura máxima por hora en Fahrenheit. Este objeto es un ejemplo de un objeto AssetModelPropertyque contiene una métrica. Puede especificar este objeto como parte de la carga útil de la CreateAssetModelsolicitud para crear una propiedad métrica. Para obtener más información, consulte Crear un modelo de activos (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 Ejemplo de definición de métrica que introduce datos procedentes de los activos asociados

El siguiente ejemplo muestra una propiedad métrica que agrega los datos de potencia media de varias turbinas eólicas para calcular la potencia media total de un parque eólico. Este objeto es un ejemplo de un objeto AssetModelPropertyque contiene una métrica. Puede especificar este objeto como parte de la carga útil de la CreateAssetModelsolicitud para crear una propiedad métrica.

```
{
      ...
      "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"
      }
    ],
    ...
}
```

Uso de expresiones de fórmula

Con las expresiones de fórmula, puede definir las funciones matemáticas para transformar y agregar los datos industriales sin procesar para obtener información sobre su operación. Las expresiones de fórmula combinan literales, operadores, funciones y variables para procesar datos. Para obtener más información acerca de cómo definir propiedades de activos que utilizan expresiones de fórmula, consulte Transformación de datos (transformaciones) y Agregación de datos de propiedades y otros activos (métricas). Las transformaciones y las métricas son propiedades de la fórmula.

Temas

- Uso de variables en las expresiones de fórmula
- Uso de literales en expresiones de fórmulas
- Uso de operadores en expresiones de fórmulas
- Uso de constantes en expresiones de fórmulas
- Uso de funciones en expresiones de fórmulas
- Tutoriales de expresiones de fórmula

Uso de variables en las expresiones de fórmula

Las variables representan las propiedades AWS IoT SiteWise de los activos en las expresiones de fórmula. Utilice variables para introducir valores de otras propiedades de activos en sus expresiones, de modo que pueda procesar datos de propiedades constantes (atributos), flujos de datos sin procesar (mediciones) y otras propiedades de la fórmula.

Las variables pueden representar propiedades de activos del mismo modelo de activo o de modelos de entidades secundarias asociadas. Solo las fórmulas métricas pueden introducir variables procedentes de modelos de entidades secundarias.

Las variables se identifican con nombres diferentes en la consola y en la API.

- AWS IoT SiteWise consola: utilice los nombres de las propiedades de los activos como variables en sus expresiones.
- AWS IoT SiteWise API (AWS CLI, AWS SDK): defina las variables con la ExpressionVariableestructura, que requiere un nombre de variable y una referencia a una propiedad de activo. El nombre puede contener letras en mayúsculas y minúsculas, números y guiones bajos. A continuación, utilice nombres de variables para hacer referencia a las propiedades de los activos en sus expresiones.

Los nombres de las variables distinguen mayúsculas de minúsculas.

Para obtener más información, consulte Definición de transformaciones y Definición de métricas.

Uso de variables para hacer referencia a propiedades

El valor de una variable define la propiedad a la que hace referencia. AWS IoT SiteWise proporciona diferentes formas de hacerlo.

- Por identificador de propiedad: puede especificar el identificador único (UUID) de la propiedad para identificarla.
- Por nombre: si la propiedad pertenece al mismo modelo de activos, puede especificar su nombre en el campo ID de la propiedad.
- Por ruta: un valor variable puede hacer referencia a una propiedad por su ruta. Para obtener más información, consulte Uso de rutas para hacer referencia a las propiedades de los modelos compuestos personalizados.

> **Note**
>
> La AWS IoT SiteWise consola no admite variables. Las utilizan la AWS IoT SiteWise API (incluidos los AWS Command Line Interface AWS CLI) y AWS los SDK.

Una variable de la que recibas una respuesta AWS IoT SiteWise incluye información completa sobre el valor, incluidos el ID y la ruta.

Sin embargo, cuando pasas una variable a AWS IoT SiteWise (por ejemplo, en una llamada de «creación» o «actualización»), solo necesitas especificar una de estas variables. Por ejemplo, si especificas la ruta, no necesitas proporcionar el ID.

Uso de literales en expresiones de fórmulas

Puede definir literales numéricos y de cadena en las expresiones de fórmula.

- Números

  Utilice números y notación científica para definir números enteros y dobles. Puede usar la notación E para expresar números con notación científica.

  Ejemplos: `1`, `2.0`, `.9`, `-23.1`, `7.89e3`, `3.4E-5`

- Strings

  Utilice los caracteres `'` (comillas) y `"` (comillas dobles) para definir las cadenas. El tipo de comilla para el inicio y el final deben coincidir. Para evitar que una comilla coincida con la que utiliza para declarar una cadena, incluya el carácter de esa comilla dos veces. Es el único carácter de escape de las AWS IoT SiteWise cadenas.

  Ejemplos: `'active'`, `"inactive"`, `'{"temp": 52}'`, `"{""temp"": ""high""}"`

Uso de operadores en expresiones de fórmulas

Puede utilizar los siguientes operadores comunes en sus expresiones de fórmulas.

Operador	Descripción
+	Si ambos operandos son números, este operador suma los operandos izquierdo y derecho. Si alguno de los operandos es una cadena, este operador concatena los operandos

Operador	Descripción
	izquierdo y derecho como cadenas. Por ejemplo, la expresión `1 + 2 + " is three"` se evalúa como `"3 is three"`. La cadena concatenada puede contener hasta 1024 caracteres. Si la cadena supera los 1024 caracteres, AWS IoT SiteWise no genera ningún punto de datos para ese cálculo.
-	Resta el operando derecho del operando izquierdo. Este operador solo se puede utilizar con operandos numéricos.
/	Divide el operando izquierdo por el operando derecho. Este operador solo se puede utilizar con operandos numéricos.
*	Multiplica los operandos izquierdo y derecho. Este operador solo se puede utilizar con operandos numéricos.
^	Eleva el operando izquierdo a la potencia del operando derecho (exponenciación). Este operador solo se puede utilizar con operandos numéricos.

Operador	Descripción
`%`	Devuelve el resto de la división del operando izquierdo por el operando derecho. El resultado tiene el mismo signo que el operando izquierdo . Este comportamiento difiere de la operación del módulo. Este operador solo se puede utilizar con operandos numéricos.
`x < y`	Devuelve `1` si `x` es menor que `y`, de lo contrario `0`.
`x > y`	Devuelve `1` si `x` es mayor que `y`, de lo contrario `0`.
`x <= y`	Devuelve `1` si `x` es menor o igual que `y`, de lo contrario `0`.
`x >= y`	Devuelve `1` si `x` es mayor o igual que `y`, de lo contrario `0`.
`x == y`	Devuelve `1` si `x` es igual a `y`, de lo contrario `0`.
`x != y`	Devuelve `1` si `x` no es igual a `y`, de lo contrario `0`.
`!x`	Devuelve `1` si `x` se evalúa como `0` (falso); en caso contrario `0`. `x` se evalúa como falso si: • `x` es un operando numérico y se evalúa como `0`. • `x` se evalúa como una cadena vacía. • `x` se evalúa como una matriz vacía. • `x` se evalúa como `None`.

Operador	Descripción
`x and y`	Devuelve `0` si `x` se evalúa como `0` (falso). De lo contrario, devuelve el resultado evaluado de `y`. `x` o `y` se evalúa como falso si: • `x` o `y` es un operando numérico y se evalúa como `0`. • `x` o `y` se evalúa como una cadena vacía. • `x` o `y` se evalúa como una matriz vacía. • `x` o `y` se evalúa como `None`.
`x or y`	Devuelve 1 si `x` se evalúa como 1 (verdadero). De lo contrario, devuelve el resultado evaluado de `y`. `x` o `y` se evalúa como falso si: • `x` o `y` es un operando numérico y se evalúa como `0`. • `x` o `y` se evalúa como una cadena vacía. • `x` o `y` se evalúa como una matriz vacía. • `x` o `y` se evalúa como `None`.
`not x`	Devuelve 1 si `x` se evalúa como `0` (falso); en caso contrario `0`. `x` se evalúa como falso si: • `x` es un operando numérico y se evalúa como `0`. • `x` se evalúa como una cadena vacía. • `x` se evalúa como una matriz vacía. • `x` se evalúa como `None`.

Operador	Descripción

`[]`
 	
`s[index]`
	Devuelve el carácter situado en un índice `index` de la cadena `s`. Esto equivale a la sintaxis de índices en Python.
	
	Example Ejemplos
	
	• `"Hello!"[1]` devuelve `e`.
	• `"Hello!"[-2]` devuelve `o`.

Operador	Descripción

`[]`
 	
`s[start:end:step]`
	Devuelve un sector de la cadena `s`. Esto equivale a la sintaxis de sectores en Python. Este operador tiene los siguientes argumentos:
	
	• `start`: (opcional) el índice inicial inclusivo del sector. El valor predeterminado es `0`.
	• `end`: (opcional) el índice final exclusivo del sector. El valor predeterminado es la longitud de la cadena.
	• `step`: (opcional) el número que se debe incrementar por cada paso del sector. Por ejemplo, puede especificar 2 para devolver un sector cada dos caracteres o especificar `-1` para invertir el sector. El valor predeterminado es 1.
	
	Puede omitir el argumento `step` para usar su valor predeterminado. Por ejemplo, `s[1:4:1]` equivale a `s[1:4]`.
	
	Los argumentos deben ser enteros o la constante none. Si lo especificanone, AWS IoT SiteWise utiliza el valor predeterminado para ese argumento.
	
	Example Ejemplos
	
	• `"Hello!"[1:4]` devuelve `"ell"`.
	• `"Hello!"[:2]` devuelve `"He"`.
	• `"Hello!"[3:]` devuelve `"lo!"`.
	• `"Hello!"[:-4]` devuelve `"He"`.
	• `"Hello!"[::2]` devuelve `"Hlo"`.
	• `"Hello!"[::-1]` devuelve `"!olleH"`.

Uso de constantes en expresiones de fórmulas

Puede utilizar las siguientes constantes matemáticas comunes en sus expresiones. Todas las constantes son incapaces de distinguir mayúsculas y minúsculas.

> **Note**
>
> Si define una variable con el mismo nombre que una constante, la variable anula a la constante.

Constant	Descripción
`pi`	El número pi (π): `3.141592653589793`
`e`	El número e: `2.718281828459045`
`true`	Equivale al número 1. En AWS IoT SiteWise, los valores booleanos se convierten en sus equivalentes numéricos.
`false`	Equivale al número 0. En AWS IoT SiteWise, los valores booleanos se convierten a sus equivalentes numéricos.
`none`	Equivale a no tener ningún valor. Puede usar esta constante para no generar nada como resultado de una expresión condicional.

Uso de funciones en expresiones de fórmulas

Puede utilizar las siguientes funciones para operar con datos de las expresiones de fórmula.

Las transformaciones y las métricas son compatibles con funciones diferentes. La siguiente tabla indica qué tipos de funciones son compatibles con cada tipo de propiedad de una fórmula.

> **Note**
>
> Se puede incluir un máximo de 10 funciones en una expresión formulaica.

Tipo de función	Transformaciones	Métricas
Uso de funciones comunes en expresiones de fórmulas	 Sí	 Sí
Uso de funciones de comparación en expresiones de fórmulas	 Sí	 Sí
Uso de funciones condicionales en expresiones de fórmulas	 Sí	 Sí
Uso de funciones de cadena en expresiones de fórmulas	 Sí	 Sí
Uso de funciones de agregación en expresiones de fórmulas	 No	 Sí
Uso de funciones temporales en expresiones de fórmulas	 Sí	 Sí

Tipo de función	Transformaciones	Métricas
Uso de funciones de fecha y hora en expresiones de fórmulas	 Sí	 Sí

Sintaxis de las funciones

Puede usar la siguiente sintaxis para crear funciones:

Sintaxis normal

Con la sintaxis normal, el nombre de la función va seguido de paréntesis con cero o más argumentos.

`function_name``(`*`argument1, argument2, argument3, ...`*`)`. Por ejemplo, las funciones con sintaxis normal podrían ser similares a `log(x)` y `contains(s, substring)`.

Sintaxis uniforme de llamada a funciones (UFCS)

La UFCS permite llamar a funciones mediante la sintaxis de las llamadas a métodos en la programación orientada a objetos. Con UFCS, el primer argumento va seguido de un punto (`.`) y del nombre de la función, seguidos del resto de los argumentos (si los hay) entre paréntesis.

`argument1``.`*`function_name`*`(`*`argument2, argument3, ...`*`)`. Por ejemplo, las funciones con UFCS podrían ser similares a `x.log()` y `s.contains(substring)`.

También puede utilizar el UFCS para encadenar funciones posteriores. AWS IoT SiteWise utiliza el resultado de la evaluación de la función actual como primer argumento de la siguiente función.

Por ejemplo, en lugar de utilizar `message.jp('$.status').lower().contains('fail')`, puede utilizar `contains(lower(jp(message, '$.status')),'fail')`.

Para obtener más información, consulte el sitio webLenguaje de programación D.

> **Note**
>
> Puede utilizar el UFCS para todas las AWS IoT SiteWise funciones.

AWS IoT SiteWise las funciones no distinguen entre mayúsculas y minúsculas. Por ejemplo, puede usar `lower(s)` y `Lower(s)` indistintamente.

Uso de funciones comunes en expresiones de fórmulas

En las transformaciones y las métricas, puede usar las siguientes funciones para calcular las funciones matemáticas comunes de las transformaciones y las métricas.

Función	Descripción
`abs(x)`	Devuelve el valor absoluto de `x`.
`acos(x)`	Devuelve el arco coseno de `x`.
`asin(x)`	Devuelve el arcoseno de `x`.
`atan(x)`	Devuelve el arco tangente de `x`.
`cbrt(x)`	Devuelve la raíz cúbica de `x`.
`ceil(x)`	Devuelve el entero más cercano mayor que `x`.
`cos(x)`	Devuelve el coseno de `x`.
`cosh(x)`	Devuelve el coseno hiperbólico de `x`.
`cot(x)`	Devuelve la tangente de `x`.
`exp(x)`	Devuelve `e` a la potencia de `x`.
`expm1(x)`	Devuelve `exp(x) - 1`. Utilice esta función para calcular con mayor precisión `exp(x) - 1` para los valores pequeños de `x`.
`floor(x)`	Devuelve el entero más cercano menor que `x`.
`log(x)`	Devuelve el $\log_e$ (base `e`) de `x`.
`log10(x)`	Devuelve el $\log_{10}$ (base `10`) de `x`.

Función	Descripción
`log1p(x)`	Devuelve `log(1 + x)`. Utilice esta función para calcular con mayor precisión `log(1 + x)` para los valores pequeños de `x`.
`log2(x)`	Devuelve el $\log_2$ (base 2) de `x`.
`pow(x, y)`	Devuelve `x` a la potencia de `y`. Esto equivale a `x ^ y`.
`signum(x)`	Devuelve el signo de `x` (`-1` para entradas negativas, `0` para entradas cero, `+1` para entradas positivas).
`sin(x)`	Devuelve el seno de `x`.
`sinh(x)`	Devuelve el seno hiperbólico de `x`.
`sqrt(x)`	Devuelve la raíz cuadrada de `x`.
`tan(x)`	Devuelve la tangente de `x`.
`tanh(x)`	Devuelve la tangente hiperbólica de `x`.

Uso de funciones de comparación en expresiones de fórmulas

En las transformaciones y las métricas, puede usar las siguientes funciones de comparación para comparar dos valores y obtener resultados 1 (verdadero) o `0` (falso). AWS IoT SiteWise compara las cadenas por orden lexicográfico.

Función	Descripción
`gt(x, y)`	Devuelve 1 si `x` es mayor que `y`, de lo contrario `0` (`x > y`). Esta función no devuelve un valor si `x` y `y` son tipos incompatibles, como un número y una cadena.

Función	Descripción
`gte(x, y)`	Devuelve 1 si `x` es mayor o igual que `y`, de lo contrario `0` (`x ≥ y`). AWS IoT SiteWise considera que los argumentos son iguales si están dentro de una tolerancia relativa de. `1E-9` Esto se comporta de forma similar a la función isclose de Python. Esta función no devuelve un valor si `x` y `y` son tipos incompatibles, como un número y una cadena.
`eq(x, y)`	Devuelve 1 si `x` es igual a `y`, de lo contrario `0` (`x == y`). AWS IoT SiteWise considera que los argumentos son iguales si están dentro de una tolerancia relativa de`1E-9`. Esto se comporta de forma similar a la función isclose de Python. Esta función no devuelve un valor si `x` y `y` son tipos incompatibles, como un número y una cadena.
`lt(x, y)`	Devuelve 1 si `x` es menor que `y`, de lo contrario `0` (`x < y`). Esta función no devuelve un valor si `x` y `y` son tipos incompatibles, como un número y una cadena.

Función	Descripción
`lte(x, y)`	Devuelve `1` si `x` es menor o igual que `y`, de lo contrario `0` (`x ≤ y`). AWS IoT SiteWise considera que los argumentos son iguales si están dentro de una tolerancia relativa de`1E-9`. Esto se comporta de forma similar a la función isclose de Python. Esta función no devuelve un valor si `x` y `y` son tipos incompatibles, como un número y una cadena.
`isnan(x)`	Devuelve `1` si `x` es igual a `NaN`, de lo contrario `0`. Esta función no devuelve un valor si `x` es una cadena.

Uso de funciones condicionales en expresiones de fórmulas

En las transformaciones y las métricas, puede usar la siguiente función para comprobar una condición y obtener resultados diferentes, independientemente de si la condición se evalúa como verdadera o falsa.

Función	Descripción
`if(condition, result_if_true, result_if_false)`	Evalúa la `condition` y devuelve `result_if_true` si la condición se evalúa como verdadera o `result_if_false` si la condición se evalúa como `false`. `condition` debe ser un número. Esta función considera `0` una cadena vacía como `false` y todo lo demás (incluido `NaN`) como `true`. Los valores booleanos se convierten en `0` (falso) y `1` (verdadero).

Función	Descripción
	Se puede devolver la constante none de esta función para descartar el resultado de una condición concreta. Esto significa que puede filtrar los puntos de datos que no cumplan una condición. Para obtener más información, consulte Filtrado de puntos de datos. Example Ejemplos • `if(0, x, y)` devuelve la variable `y`. • `if(5, x, y)` devuelve la variable `x`. • `if(gt(temp, 300), x, y)` devuelve la variable `x` si la variable `temp` es mayor que `300`. • `if(gt(temp, 300), temp, none)` devuelve la variable `temp` si es mayor o igual que `300`, o `none` (sin valor) si `temp` es menor que `300`. Se recomienda utilizar UFCS para las funciones condicionales anidadas en las que uno o más argumentos son funciones condicionales. Se puede utilizar `if(condition, result_if_true)` para evaluar una condición y `elif(condition, result_if_true, result_if_false)` para evaluar condiciones adicionales. Por ejemplo, en lugar de utilizar `if(condition1, result1_if_true).elif(condition2, result2_if_true, result2_if_false)`, puede utilizar `if(condition1, result1_if_true, if(condition2, result2_if_true, result2_if_false))`.

Función	Descripción
	También puede encadenar funciones condicionales intermedias adicionales. Por ejemplo, puede utilizar `if(condition1, result1_if_true).elif(condition2, result2_if_true).elif(condition3, result3_if_true, result3_if_false)` en lugar de anidar varias instrucciones `if`, como `if(condition1, result1_if_true, if(condition2, result2_if_true, if(condition3, result3_if_true result3_if_false)))` . **Important** Es necesario usar `elif(condition, result_if_true, result_if_false)` con UFCS.

Uso de funciones de cadena en expresiones de fórmulas

En las transformaciones y las métricas, puede utilizar las siguientes funciones para operar con cadenas. Para obtener más información, consulte Uso de cadenas en las fórmulas.

Important

Las expresiones de fórmula solo pueden generar valores dobles o de cadena. Las expresiones anidadas pueden generar otros tipos de datos, como cadenas, pero la fórmula en su conjunto debe evaluarse como un número o una cadena. Puede usar la función jp para convertir una cadena en un número. El valor booleano debe ser 1 (verdadero) o 0 (falso). Para obtener más información, consulte Valores indefinidos, infinitos y de desbordamiento.

Función	Descripción
`len(s)`	Devuelve la longitud de la cadena `s`.
`find(s, substring)`	Devuelve el índice de la cadena `substring` en la cadena `s`.
`contains(s, substring)`	Devuelve 1 si la cadena `s` contiene la cadena `substring` , en caso contrario `0`.
`upper(s)`	Devuelve la cadena `s` en mayúsculas.
`lower(s)`	Devuelve la cadena `s` en minúsculas.
`jp(s, json_path)`	Evalúa la cadena `s` con la JsonPathexpresión `json_path` y devuelve el resultado. Utilice esta función para hacer lo siguiente: • Extraer un valor, una matriz o un objeto de una estructura JSON serializada. • Convertir una cadena en un número. Por ejemplo, la fórmula `jp('111', '$')` devuelve `111` como un número. Para extraer un valor de cadena de una estructura JSON y devolverlo como un número, debe utilizar varias funciones anidadas `jp`. La función externa `jp` extrae la cadena de la estructura JSON y la función interna `jp` convierte la cadena en un número. La cadena `json_path` debe contener un literal de cadena. Esto significa que `json_path` no puede ser una expresión que se evalúe como cadena.

Función	Descripción
	Example Ejemplos • `jp('{"status":"active","value":15}', '$.value')` devuelve 15. • `jp('{"measurement":{"reading":25,"confidence":0.95}}', '$.measurement.reading')` devuelve 25. • `jp('[2,8,23]', '$[2]')` devuelve 23. • `jp('{"values":[3,6,7]}', '$.values[1]')` devuelve 6. • `jp('111', '$')` devuelve 111. • `jp(jp('{"measurement":{"reading":25,"confidence":"0.95"}}', '$.measurement.confidence'), '$')` devuelve `0.95`.
`join(s0, s1, s2, s3, ...)`	Devuelve una cadena concatenada con un delimitador. Esta función usa la primera cadena de entrada como delimitador y une las cadenas de entrada restantes. Esto se comporta de forma similar a la función join (CharSequence delimiter, CharSequence... elements) de Java. Example Ejemplos • `join("-", "aa", "bb", "cc")` devuelve `aa-bb-cc`

Función	Descripción
`format(expression: "format")` o `format("format", expression)`	Devuelve una cadena en el formato especific ado. Esta función evalúa `expression` como un valor y, a continuación, devuelve el valor en el formato especificado. Esto se comporta de forma similar a la función format(String format, Object... args) de Java. Para obtener más información sobre los formatos compatibles, consulte el apartado Conversions en la sección Class Formatter de la plataforma Java, edición estándar 7, especificación de API. Example Ejemplos • `format(100+1: "d")` devuelve una cadena, `101`. • `format("The result is %d", 100+1)` devuelve una cadena, `The result is 101`.

Función	Descripción
`f'expression'`	Devuelve una cadena concatenada. Con esta función formateada, puede utilizar una expresión sencilla para concatenar y formatear cadenas. Estas funciones pueden contener expresiones anidadas. Puede utilizar `{}` (corchetes) para interpolar expresiones. Esto se comporta de forma similar a los literales de cadena formateados de Python. Example Ejemplos • `f'abc{1+2: "f"}d'` devuelve `abc3.000000d` . Para evaluar esta expresión de ejemplo, haga lo siguiente: 1. `format(1+2: "f")` devuelve un número de punto flotante, `3.000000`. 2. `join('', "abc", 1+2, 'd')` devuelve una cadena, `abc3.000000d` . También puede escribir la expresión de la siguiente manera: `join('', "abc", format(1+2: "f"), 'd')` .

Uso de funciones de agregación en expresiones de fórmulas

Solo en las métricas, puede utilizar las siguientes funciones que agregan valores de entrada en cada intervalo de tiempo y calculan un único valor de salida. Las funciones de agregación pueden agregar datos de activos asociados.

Los argumentos de las funciones de agregación pueden ser variables, literales numéricos, funciones temporales, expresiones anidadas o funciones de agregación. La fórmula `max(latest(x), latest(y), latest(z))` utiliza una función de agregación como argumento y devuelve el valor actual más grande de las propiedades `x`, `y` y `z`.

Puede utilizar expresiones anidadas en las funciones de agregación. Cuando se utilizan expresiones anidadas, se aplican las reglas siguientes:

- Cada argumento solo puede tener una variable.

  Example

  Por ejemplo, `avg(x*(x-1))` y `sum(x/2 )/avg(y^2 )` son compatibles.

  Por ejemplo, `min(x/y)` no es compatible.
- Cada argumento puede tener expresiones anidadas de varios niveles.

  Example

  Por ejemplo, `sum(avg(x^2 )/2)` no se admite.
- Cada argumento puede tener variables diferentes.

  Example

  Por ejemplo, `sum(x/2, y*2)` no se admite.

> **Note**
>
> - Si las expresiones contienen medidas, AWS IoT SiteWise utiliza los últimos valores del intervalo de tiempo actual para que las mediciones calculen los agregados.
> - Si las expresiones contienen atributos, AWS IoT SiteWise utiliza los valores más recientes de los atributos para calcular los agregados.

Función	Descripción
`avg(`x_0`, ..., `x_n`)`	Devuelve la media de los valores de las variables dadas durante el intervalo de tiempo actual. Esta función genera un punto de datos solo si las variables dadas tienen al menos un punto de datos durante el intervalo de tiempo actual.

Función	Descripción
$sum(x_0, ..., x_n)$	Devuelve la suma de los valores de las variables dadas durante el intervalo de tiempo actual. Esta función genera un punto de datos solo si las variables dadas tienen al menos un punto de datos durante el intervalo de tiempo actual.
$min(x_0, ..., x_n)$	Devuelve el mínimo de los valores de las variables dadas durante el intervalo de tiempo actual. Esta función genera un punto de datos solo si las variables dadas tienen al menos un punto de datos durante el intervalo de tiempo actual.
$max(x_0, ..., x_n)$	Devuelve el máximo de los valores de las variables dadas durante el intervalo de tiempo actual. Esta función genera un punto de datos solo si las variables dadas tienen al menos un punto de datos durante el intervalo de tiempo actual.
$count(x_0, ..., x_n)$	Devuelve el número total de puntos de datos para las variables dadas durante el intervalo de tiempo actual. Para obtener más informaci ón acerca de cómo contar el número de puntos de datos que cumplen una condición, consulte Recuento de los puntos de datos que coinciden con una condición. Esta función calcula un punto de datos para cada intervalo de tiempo.

Función	Descripción
`stdev(x0, ..., xn)`	Devuelve la desviación estándar de los valores de las variables dadas durante el intervalo de tiempo actual. Esta función genera un punto de datos solo si las variables dadas tienen al menos un punto de datos durante el intervalo de tiempo actual.

Uso de funciones temporales en expresiones de fórmulas

Utilice funciones temporales para devolver valores basados en las marcas de tiempo de los puntos de datos.

Uso de funciones temporales en las métricas

Solo en las métricas, puede utilizar las siguientes funciones que devuelven valores basados en marcas temporales de puntos de datos.

Los argumentos de las funciones temporales deben ser propiedades del modelo de activo local o expresiones anidadas. Esto significa que no se pueden usar propiedades de modelos de entidades secundarias en las funciones temporales.

Puede usar expresiones anidadas en las funciones temporales. Cuando se utilizan expresiones anidadas, se aplican las reglas siguientes:

- Cada argumento solo puede tener una variable.

  Por ejemplo, `latest( t*9/5 + 32 )` no se admite.
- Los argumentos no pueden ser funciones de agregación.

  Por ejemplo, `first( sum(x) )` no es compatible.

Función	Descripción
`first(x)`	Devuelve el valor de la variable dada con la marca temporal más temprana durante el intervalo de tiempo especificado.
`last(x)`	Devuelve el valor de la variable dada con la última marca temporal durante el intervalo de tiempo especificado.
`earliest(x)`	Devuelve el último valor de la variable dada antes del inicio del intervalo de tiempo actual. Esta función calcula un punto de datos para cada intervalo de tiempo, si la propiedad de entrada tiene al menos un punto de datos en su historial. Para obtener más información, consulte time-range-defintion.
`latest(x)`	Devuelve el último valor de la variable dada con la última marca de tiempo antes del final del intervalo de tiempo actual. Esta función calcula un punto de datos para cada intervalo de tiempo, si la propiedad de entrada tiene al menos un punto de datos en su historial. Para obtener más información, consulte time-range-defintion.
`statetime(x)`	Devuelve la cantidad de tiempo en segundos que las variables dadas son positivas durante el intervalo de tiempo especificado. Puede usar lasfunciones de comparación para crear una propiedad de transformación para que la función `statetime` la consuma. Por ejemplo, si tiene una propiedad `Idle` que es `0` o `1`, puede calcular el tiempo de inactivid

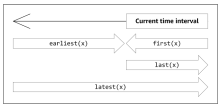
Función	Descripción
	ad por intervalo de tiempo con esta expresión : `IdleTime = statetime(Idle)` . Para obtener más información, consulte el escenario de statetime de ejemplo. La función no admite propiedades de métricas como variables de entrada. Esta función calcula un punto de datos para cada intervalo de tiempo, si la propiedad de entrada tiene al menos un punto de datos en su historial.

Función	Descripción
`TimeWeightedAvg(x, [interpolation])`	Devuelve el promedio de los datos de entrada ponderados con los intervalos de tiempo entre puntos. Consulte los Parámetros de las funciones ponderadas por tiempo para obtener detalles sobre el cálculo y los intervalos. El argumento opcional `interpolaton` debe ser una constante de cadena: • `locf` – Esta es la opción predeterminada. El cálculo utiliza el algoritmo de cálculo de última observación realizada para los intervalos entre puntos de datos. En este enfoque, el punto de datos se calcula como el último valor observado hasta la siguiente entrada de punto de datos con marca temporal. El valor que sigue a un punto de datos válido se extrapola como su valor hasta la siguiente marca temporal de puntos de datos. • `linear`: el cálculo utiliza el algoritmo de cálculo de interpolación lineal para los intervalos entre puntos de datos. El valor entre dos puntos de datos válidos se extrapola como una interpolación lineal entre los valores de esos puntos de datos. El valor entre puntos de datos válidos o nulos o el valor posterior al último punto de datos válido se extrapolará como un punto de datos válido.

Función	Descripción
`TimeWeightedStDev(x, [algo])`	Devuelve la desviación estándar de los datos de entrada ponderada con los intervalos de tiempo entre puntos. Consulte los Parámetros de las funciones ponderadas por tiempo para obtener detalles sobre el cálculo y los intervalos. El cálculo utiliza el algoritmo de cálculo de última observación realizada para los intervalos entre puntos de datos. En este enfoque, el punto de datos se calcula como el último valor observado hasta la siguiente entrada de punto de datos con marca temporal. El peso se calcula como el intervalo de tiempo en segundos entre los puntos de datos o los límites de las ventanas. El argumento opcional `algo` debe ser una constante de cadena: • `f` – Esta es la opción predeterminada. Devuelve una varianza muestral ponderada imparcial con ponderaciones de frecuencia, donde TimeWeight se calcula en segundos. Por lo general, este algoritmo se asume dentro de la desviación estándar y se conoce como corrección de Bessel de desviación estándar para muestras ponderadas. • `p`: devuelve la varianza de las muestras ponderadas sesgada, también conocida como varianza de la población. Para el cálculo se utilizan las siguientes fórmulas, donde:

Función	Descripción
	• S_p = Desviación estándar de la población • S_f = desviación estándar de la frecuencia • X_i = Datos de entrada • ω_i = ponderación que equivale al intervalo de tiempo en segundos • μ* = media ponderada de los datos entrantes Ecuación para la desviación estándar de la población: $$S_p^2 = \frac{\sum_{i=1}^{N} \omega_i (x_i - \mu^*)^2}{\sum_{i=1}^{N} \omega_i}$$ Ecuación para la desviación estándar de la frecuencia: $$S_f^2 = \frac{\sum_{i=1}^{N} \omega_i (x_i - \mu^*)^2}{\sum_{i=1}^{N} \omega_i - 1}$$

El siguiente diagrama muestra cómo se AWS IoT SiteWise calculan las funciones temporales`first`,, y `last` `earliest``latest`, en relación con el intervalo de tiempo actual.



Note

- El intervalo de tiempo para`first(x)`, `last(x)` es (inicio de la ventana actual, final de la ventana actual].
- El intervalo de tiempo `latest(x)` es (inicio del tiempo, fin de la ventana actual].

- El intervalo de tiempo `earliest(x)` es (principio del tiempo, fin de la ventana anterior].

Parámetros de funciones con ponderación de tiempo

Las funciones con ponderación temporal calculadas para la ventana de agregación tienen en cuenta lo siguiente:

- Puntos de datos dentro de la ventana
- Intervalos de tiempo entre puntos de datos
- Último punto de datos antes de la ventana
- Primer punto de datos después de la ventana (para algunos algoritmos)

Términos:

- Punto de datos nulo: cualquier punto de datos con una calidad no buena o un valor que no sea numérico. Estos no se tienen en cuenta para el cálculo de los resultados de una ventana.
- Intervalo nulo: el intervalo que sigue a un punto de datos nulo. El intervalo anterior al primer punto de datos conocido también se considera un intervalo nulo.
- Punto de datos válido: cualquier punto de datos con buena calidad y valor numérico.

> **Note**
>
> - AWS IoT SiteWise solo consume datos `GOOD` de calidad cuando calcula las transformaciones y las métricas. Ignora los puntos de datos `UNCERTAIN` y `BAD`.
> - El intervalo anterior al primer punto de datos conocido se considera un intervalo nulo. Para obtener más información, consulte the section called “Tutoriales de expresiones de fórmula”.

El intervalo posterior al último punto de datos conocido continúa indefinidamente y afecta a todas las ventanas siguientes. Cuando llega un nuevo punto de datos, la función vuelve a calcular el intervalo.

Siguiendo las reglas anteriores, se calcula el resultado agregado de la ventana y se limita a los límites de la ventana. De forma predeterminada, la función solo envía el resultado de la ventana si toda la ventana es un intervalo válido.

Si el intervalo válido de la ventana es inferior a la longitud de la ventana, la función no envía la ventana.

Cuando cambian los puntos de datos que afectan al resultado de la ventana, la función vuelve a calcular la ventana, incluso si los puntos de datos están fuera de la ventana.

Si la propiedad de entrada tiene al menos un punto de datos en su historial y se ha iniciado un cálculo, la función calcula las funciones agregadas con ponderación temporal para cada intervalo de tiempo.

Example Escenario de statetime de ejemplo

Considere un ejemplo en el que tiene un activo con las siguientes propiedades:

- `Idle`: una medición que es `0` o `1`. Cuando el valor es `1`, la máquina está inactiva.
- `Idle Time`: una métrica que utiliza la fórmula `statetime(Idle)` para calcular la cantidad de tiempo en segundos en que la máquina está inactiva, por cada intervalo de 1 minuto.

La propiedad `Idle` tiene los siguientes puntos de datos.

Timestamp	14:00:00 h	14:00:30 h	14:01:15 h	14:02:45 h	14:04:00 h
Idle	0	1	1	0	0

AWS IoT SiteWise calcula la `Idle Time` propiedad cada minuto a partir de los valores de`Idle`. Una vez realizado este cálculo, la propiedad `Idle Time` tiene los siguientes puntos de datos.

Timestamp	14:00:00 h	14:01:00 h	14:02:00 h	14:03:00 h	14:04:00 h
Idle Time	N/A	30	60	45	0

AWS IoT SiteWise realiza los siguientes cálculos `Idle Time` al final de cada minuto.

- A las 14:00 h (de las 13:59 h a las 14:00 h)
  - No hay datos para `Idle` antes de las 14:00 h, por lo que no se calcula ningún punto de datos.
- A las 14:01 h (de las 14:00 h a las 14:01 h)
  - A las 14:00:00 h, la máquina está activa (`Idle` es `0`).

  - A las 14:00:30 h, la máquina está inactiva (`Idle` es 1).
  - `Idle` no vuelve a cambiar antes del final del intervalo de las 14:01:00 h, por lo que el valor de `Idle Time` es de 30 segundos.
- A las 14:02 h (de las 14:01 h a las 14:02 h)
  - A las 14:01:00 h, el equipo está inactivo (según el último punto de datos de las 14:00:30 h).
  - A las 14:01:15 h, la máquina sigue inactiva.
  - `Idle` no vuelve a cambiar antes del final del intervalo de las 14:02:00 h, por lo que el valor de `Idle Time` es de 60 segundos.
- A las 14:03 h (de las 14:02 h a las 14:03 h)
  - A las 14:02:00 h, el equipo está inactivo (según el último punto de datos de las 14:01:15 h).
  - A las 14:02:45 h, la máquina está activa.
  - `Idle` no vuelve a cambiar antes del final del intervalo de las 14:03:00 h, por lo que el valor de `Idle Time` es de 45 segundos.
- A las 14:04 h (de las 14:03 h a las 14:04 h)
  - A las 14:03:00 h, el equipo está activo (según el último punto de datos de las 14:02:45 h).
  - `Idle` no vuelve a cambiar antes del final del intervalo de las 14:04:00 h, por lo que el valor de `Idle Time` es de 0 segundos.

Example Ejemplo TimeWeightedAvg y TimeWeightedStDev escenario

Las siguientes tablas proporcionan ejemplos de entradas y salidas para estas métricas de ventana de un minuto: `Avg(x)`, `TimeWeightedAvg(x)`, `TimeWeightedAvg(x, "linear")`, `stDev(x)`, `timeWeightedStDev(x)`, `timeWeightedStDev(x, 'p')`.

Ejemplo de entrada para una ventana agregada de un minuto:

> **Note**
>
> Todos estos puntos de datos son `GOOD` de calidad.

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

Salida de resultados agregados:

> **Note**
>
> Ninguno: no se produjo un resultado para esta ventana.

Tiempo	`Avg(x)`	`TimeWeighted Avg(x)`	`TimeWeighted Avg(X, "linear")`	`stDev(X)`	`timeWeighted StDev(x)`	`timeWeighted StDev(x, 'p')`
3:00:00	4	Ninguna	Ninguna	0	Ninguna	Ninguna
3:01:00	2	4	3	0	0	0
3:02:00	14	9	13	6	5,430610041581775	5,385164807134504
3:03:00	11	13	12,875	8,5400374531753	7,724054437220943	7,659416862050705
3:04:00	0	10	2,5	0	10,084389681792215	10

Tiempo	`Avg(x)`	`TimeWeighted Avg(x)`	`TimeWeighted Avg(X, "linear")`	`stDev(X)`	`timeWeighted StDev(x)`	`timeWeighted StDev(x, 'p')`
3:05:00	Ninguna	0	0	Ninguna	0	0

Uso de funciones temporales en las transformaciones

Solo en las transformaciones, puede utilizar la función `pretrigger()` para recuperar el valor de calidad `GOOD` de una variable antes de actualizar la propiedad que inició el cálculo de la transformación actual.

Considere un ejemplo en el que un fabricante utiliza AWS IoT SiteWise para monitorizar el estado de una máquina. El fabricante utiliza las siguientes medidas y transformaciones para representar el proceso:

- Una medición, `current_state`, que puede ser 0 o 1.
  - Si la máquina está en estado de limpieza, `current_state` equivale a 1.
  - Si la máquina está en estado de fabricación, `current_state` equivale a 0.
- Una transformación, `cleaning_state_duration`, que equivale a `if(pretrigger(current_state) == 1, timestamp(current_state) - timestamp(pretrigger(current_state)), none)`. Esta transformación devuelve el tiempo que la máquina ha estado en estado de limpieza en segundos, en formato de tiempo Unix. Para obtener más información, consulte Uso de funciones condicionales en expresiones de fórmulas y la función marca temporal().

Si la máquina permanece en estado de limpieza más tiempo del esperado, el fabricante podría investigar la máquina.

También puede utilizar la función `pretrigger()` en transformaciones multivariantes. Por ejemplo, dispone de dos mediciones denominadas `x` y `y`, y una transformación `z`, que equivale a `x + y + pretrigger(y)`. En la siguiente tabla se muestran los valores de `x`, y `y` y `z` desde las 9:00 h hasta las 9:15 h.

Note

- En este ejemplo se presupone que los valores de las mediciones llegan en orden cronológico. Por ejemplo, el valor de `x` para las 09:00 h llega antes que el valor de `x` para las 09:05 h.
- Si los puntos de datos de las 9:05 h llegan antes que los puntos de datos de las 9:00 h, no se calcula `z` a las 9:05 h.
- Si el valor de `x` para las 9:05 h llega antes que el valor de `x` para las 09:00 h y los valores de `y` llegan en orden cronológico, `z` equivale a `22 = 20 + 1 + 1` a las las 9:05 h.

	09:00 h	09:05 h	09:10 h	09:15 h
x	10	20		30
y	1	2	3	
`z = x + y + pretrigger(y)`	y no recibe ningún punto de datos antes de las 09:00 h. Por lo tanto, `z` no se calcula a las 09:00 h.	23 = 20 + 2 + 1 `pretrigger(y)` equivale a 1.	25 = 20 + 3 + 2 `x` no recibe un nuevo punto de datos. `pretrigger(y)` equivale a 2.	36 = 30 + 3 + 3 y no recibe un nuevo punto de datos. Por lo tanto, `pretrigger(y)` equivale a 3 a las 09:15 h.

Uso de funciones de fecha y hora en expresiones de fórmulas

En las transformaciones y las métricas, puede utilizar las funciones de fecha y hora de las siguientes maneras:

- Para recuperar la marca temporal actual de un punto de datos en UTC o en la zona horaria local.
- Para construir marcas temporales con argumentos, como `year`, `month` y `day_of_month`.
- Para extraer un período de tiempo, como un año o un mes, con el argumento `unix_time`.

Función	Descripción
`now()`	Devuelve la fecha y hora actuales, en segundos, en formato de tiempo Unix.
`timestamp()`	• En las transformaciones, la función devuelve la marca temporal, en segundos, del mensaje de entrada en formato de tiempo Unix. Solo en las transformaciones, puede realizar una de las siguientes acciones: • Proporcionar una variable como argumento a la función. La función `timestamp( variable-name )` devuelve la marca temporal, en segundos, del valor más reciente de calidad `GOOD` de la variable, en formato de tiempo Unix. Por ejemplo, si su activo tiene un nombre de propiedad de transformación `Temperature_F` que usa la fórmula `9/5 * Temperature_C` para convertir cada punto de datos de temperatura de grados Celsius a Fahrenheit, puede usar la función `timestamp(Temperature_F)` para obtener la marca temporal valor de calidad `GOOD` más reciente para la propiedad `Temperature_F` . • Utilizar la función `pretrigger()` como argumento de la función. La función `timestamp(pretrigger( variable-name ))` devuelve la marca temporal, en segundos, del valor más reciente de calidad `GOOD` de la variable especificada antes de actualizar la propiedad que inició el cálculo de la transformación actual, en

Función	Descripción
	formato de tiempo Unix. Para obtener más información, consulte Uso de funciones temporales en las transformaciones. • En las métricas, la función devuelve la marca de tiempo recuperada al final de la ventana actual, en segundos, en formato de tiempo Unix.

Función	Descripción
`mktime(time_zone, year, month, day_of_month, hour, minute, second)`	Devuelve el tiempo de entrada, en segundos, en formato de tiempo Unix. Los siguientes requisitos se aplican al uso de esta función: • El argumento de zona horaria debe ser una cadena entre comillas (`'UTC'`). Si no se especifica, la zona horaria predeterminada es UTC. El argumento de zona horaria puede ser el primero o el último argumento. • Los argumentos año, mes, día del mes, hora, minuto y segundo deben estar en orden. • Los argumentos de año, mes y fecha son obligatorios. Los siguientes límites se aplican al uso de esta función: • `year`: los valores válidos se encuentran entre 1970 y 2250. • `month`: los valores válidos se encuentran entre 1 y 12. • `day-of-month` : los valores válidos se encuentran entre 1 y 31. • `hour`: los valores válidos se encuentran entre 0 y 23. • `minute`: los valores válidos se encuentran entre 0 y 59. • `second`: los valores válidos se encuentran entre 0 y 60. Puede ser un número de punto flotante.

Función	Descripción
	Ejemplos: • `mktime(2020, 2, 29)` • `mktime('UTC+3', 2021, 12, 31, 22)` • `mktime(2022, 10, 13, 2, 55, 13.68, 'PST')`

Función	Descripción
`localtime(unix_time, time_zone)`	Devuelve el año, el día del mes, el día de la semana, el día del año, la hora, el minuto o el segundo de la zona horaria especificada a partir del tiempo Unix. Los siguientes requisitos se aplican al uso de esta función: • El argumento de zona horaria debe ser una cadena entre comillas (`'UTC'`). Si no se especifica, la zona horaria predeterminada es UTC. • El argumento tiempo Unix es el tiempo en segundos, en formato de tiempo Unix. El rango válido es de 1 a 31556889864403199. Puede ser un número de punto flotante. Respuesta de ejemplo: `2007-12-03T10:15:30+01:00[Europe/Paris]` `localtime(unix_time, time_zone)` no es una función independiente. Las funciones `year()`, `mon()`, `mday`, `wday()`, `yday()`, `hour()`, `minute()` y `sec()` toman `localtime(unix_time, time_zone)` como argumento. Ejemplos: • `year(localtime('GMT', 1605898608.8113723))` • `now().localtime().year()` • `timestamp().localtime('PST').year()`

Función	Descripción
	• `localtime(1605289736, 'Europe/London').year()`
`year(localtime(unix_time, time_zone)`	Devuelve el año desde `localtime (unix_time, time_zone)` .
`mon(localtime(unix_time, time_zone))`	Devuelve el mes desde `localtime (unix_time, time_zone)` .
`mday(localtime(unix_time, time_zone))`	Devuelve el día del mes desde `localtime (unix_time, time_zone)` .
`wday(localtime(unix_time, time_zone))`	Devuelve el día de la semana desde `localtime(unix_time, time_zone)` .
`yday(localtime(unix_time, time_zone))`	Devuelve el día del año desde `localtime (unix_time, time_zone)` .
`hour(localtime(unix_time, time_zone))`	Devuelve la hora desde `localtime (unix_time, time_zone)` .
`minute(localtime(unix_time, time_zone))`	Devuelve el minuto desde `localtime (unix_time, time_zone)` .
`sec(localtime(unix_time, time_zone))`	Devuelve el segundo desde `localtime (unix_time, time_zone)` .

Formatos de zona horaria admitidos

Puede especificar el argumento de zona horaria de las siguientes maneras:

- Desplazamiento de la zona horaria: especifique `'Z'` si es UTC o un desplazamiento (`'+2'` o `'-5'`).
- Identificadores de desplazamiento: combina una abreviatura de la zona horaria y un desplazamiento. Por ejemplo, `'GMT+2'` y `'UTC-01:00'`. La abreviatura de la zona horaria debe contener solo tres letras.
- Identificadores basados en regiones: por ejemplo, `'Etc/GMT+12'` y `'Pacific/Pago_Pago'`.

Abreviaturas de zona horaria compatibles

Las funciones de fecha y hora admiten las siguientes abreviaturas de zona horaria de tres letras:

- WEST: -05:00
- HOST: -10:00
- HST: -07:00
- ACT: Australia/Darwin
- AET: Australia/Sídney
- AGT: América/Argentina/Buenos_Aires
- ARTE: África/El Cairo
- AST: América/Anchorage
- BET: América/Sao_Paulo
- BST: Asia/Daca
- CAT: África/Harare
- CET: Europa/París
- CNT: América/St_Johns
- CST: América/Chicago
- CTT: Asia/Shanghái
- EAT: África/Adís_Abeba
- IET: América/Indiana/Indianápolis
- IST: Asia/Calcuta
- JST: Asia/Tokio
- MIT: Pacífico/Apia
- NET: Asia/Ereván
- NST: Pacífico/Auckland
- PLT: Asia/Karachi
- PRT: América/Puerto_Rico
- PST: America/Los_Ángeles
- SST: Pacífico/Guadalcanal

- VST: Asia/Ho_Chi_Minh

Identificadores basados en regiones compatibles

Las funciones de fecha y hora admiten los siguientes ID basados en regiones, organizados según su relación con UTC+ 00:00:

- Etc/GMT+12 (UTC-12:00)
- Pacífico/Pago_Pago (UTC-11:00)
- Pacífico/Samoa (UTC-11:00)
- Pacífico/Niue (UTC-11:00)
- EE. UU./Samoa (UTC-11:00)
- Etc/GMT+11 (UTC-11:00)
- Pacífico/Midway (UTC-11:00)
- Pacífico/Honolulú (UTC-10:00)
- Pacífico/Rarotonga (UTC-10:00)
- Pacífico/Tahití (UTC-10:00)
- Pacífico/Johnston (UTC-10:00)
- EE. UU./Hawái (UTC-10:00)
- SystemV/HST10 (UTC-10:00)
- Etc/GMT+10 (UTC-10:00)
- Pacífico/Marquesas (UTC-09:30)
- Etc/GMT+9 (UTC-09:00)
- Pacífico/Gambier (UTC-09:00)
- América/Atka (UTC-09:00)
- SystemV/YST9 (UTC-09:00)
- América/Adak (UTC-09:00)
- EE. UU./Aleutianas (UTC-09:00)
- Etc/GMT+8 (UTC-08:00)
- EE. UU./Alaska (UTC-08:00)

- América/Juneau (UTC-08:00)
- América/Metlakatla (UTC-08:00)
- América/Yakutat (UTC-08:00)
- Pacífico/Pitcairn (UTC-08:00)
- América/Sitka (UTC-08:00)
- América/Anchorage (UTC-08:00)
- SystemV/PST8 (UTC-08:00)
- América/Nome (UTC-08:00)
- SystemV/YST9YDT (UTC-08:00)
- Canadá/Yukon (UTC-07:00)
- EE. UU./Pacífico-Nuevo (UTC-07:00)
- Etc/GMT+7 (UTC-07:00)
- EE. UU./Arizona (UTC-07:00)
- América/Dawson_Creek (UTC-07:00)
- Canadá/Pacífico (UTC-07:00)
- PST8PDT (UTC-07:00)
- SystemV/MST7 (UTC-07:00)
- América/Dawson (UTC-07:00)
- México/ BajaNorte (UTC- 07:00)
- América/Tijuana (UTC-07:00)
- América/Creston (UTC-07:00)
- América/Hermosillo (UTC-07:00)
- América/Santa_Isabel (UTC-07:00)
- América/Vancouver (UTC-07:00)
- América/Ensenada (UTC-07:00)
- América/Phoenix (UTC-07:00)
- América/Whitehorse (UTC-07:00)
- América/Fort_Nelson (UTC-07:00)

- SystemV/PST8PDT (UTC-07:00)
- América/Los_Ángeles (UTC-07:00)
- EE. UU./Pacífico (UTC-07:00)
- América/El_Salvador (UTC-06:00)
- América/Guatemala (UTC-06:00)
- América/Belice (UTC-06:00)
- América/Managua (UTC-06:00)
- América/Tegucigalpa (UTC-06:00)
- Etc/GMT+6 (UTC-06:00)
- Pacífico/Pascua (UTC-06:00)
- México/ BajaSur (UTC- 06:00)
- América/Regina (UTC-06:00)
- América/Denver (UTC-06:00)
- Pacífico/Galápagos (UTC-06:00)
- América/Yellowknife (UTC-06:00)
- América/Swift_Current (UTC-06:00)
- América/Inuvik (UTC-06:00)
- América/Mazatlán (UTC-06:00)
- América/Boise (UTC-06:00)
- América/Costa_Rica (UTC-06:00)
- MST7MDT (UTC-06:00)
- SystemV/CST6 (UTC-06:00)
- América/Chihuahua (UTC-06:00)
- América/Ojinaga (UTC-06:00)
- Chile/ EasterIsland (UTC- 06:00)
- EE. UU./Montaña (UTC-06:00)
- América/Edmonton (UTC-06:00)
- Canadá/Montaña (UTC-06:00)
- América/Cambridge_Bay (UTC-06:00)

- Navajo (UTC-06:00)
- SystemV/MST7MDT (UTC-06:00)
- Canadá/Saskatchewan (UTC-06:00)
- América/Shiprock (UTC-06:00)
- América/Panamá (UTC-05:00)
- América/Chicago (UTC-05:00)
- América/Eirunepe (UTC-05:00)
- Etc/GMT+5 (UTC-05:00)
- México/General (UTC-05:00)
- América/Porto_Acre (UTC-05:00)
- América/Guayaquil (UTC-05:00)
- América/Rankin_Inlet (UTC-05:00)
- EE. UU./Central (UTC-05:00)
- América/Rainy_River (UTC-05:00)
- América/Indiana/Knox (UTC-05:00)
- América/North_Dakota/Beulah (UTC-05:00)
- América/Monterrey (UTC-05:00)
- América/Jamaica (UTC-05:00)
- América/Atikokan (UTC-05:00)
- América/Coral_Harbour (UTC-05:00)
- América/Dakota_del_Norte/Centro (UTC-05:00)
- América/Caimán (UTC-05:00)
- América/Indiana/Tell_City (UTC-05:00)
- América/Ciudad_de_México (UTC-05:00)
- América/Matamoros (UTC-05:00)
- CST6CDT (UTC-05:00)
- América/Knox_IN (UTC-05:00)
- América/Bogotá (UTC-05:00)
- América/Menominee (UTC-05:00)

- América/Resolute (UTC-05:00)
- SystemV/EST5 (UTC-05:00)
- Canadá/Central (UTC-05:00)
- Brasil/Acre (UTC-05:00)
- América/Cancún (UTC-05:00)
- América/Lima (UTC-05:00)
- América/Bahía_Banderas (UTC-05:00)
- EE. UU./Indiana-Starke (UTC-05:00)
- América/Rio_Branco (UTC-05:00)
- SystemV/CST6CDT (UTC-05:00)
- Jamaica (UTC-05:00)
- América/Mérida (UTC-05:00)
- América/Dakota_del_Norte/New_Salem (UTC-05:00)
- América/Winnipeg (UTC-05:00)
- América/Cuiabá (UTC-04:00)
- América/Marigot (UTC-04:00)
- América/Indiana/Petersburg (UTC-04:00)
- Chile/Continental (UTC-04:00)
- América/Grand_Turk (UTC-04:00)
- Cuba (UTC-04:00)
- Etc/GMT+4 (UTC-04:00)
- América/Manaos (UTC-04:00)
- América/Fort_Wayne (UTC-04:00)
- América/St_Thomas (UTC-04:00)
- América/Anguila (UTC-04:00)
- América/Habana (UTC-04:00)
- EE. UU./Michigan (UTC-04:00)
- América/Barbados (UTC-04:00)
- América/Louisville (UTC-04:00)

- América/Curazao (UTC-04:00)
- América/Guyana (UTC-04:00)
- América/Martinica (UTC-04:00)
- América/Puerto_Rico (UTC-04:00)
- América/Puerto_España (UTC-04:00)
- SystemV/AST4 (UTC-04:00)
- América/Indiana/Vevay (UTC-04:00)
- América/Indiana/Vincennes (UTC-04:00)
- América/Kralendijk (UTC-04:00)
- América/Antigua (UTC-04:00)
- América/Indianápolis (UTC-04:00)
- América/Iqaluit (UTC-04:00)
- América/St_Vincent (UTC-04:00)
- América/Kentucky/Louisville (UTC-04:00)
- América/Dominica (UTC-04:00)
- América/Asunción (UTC-04:00)
- EST5EDT (UTC-04:00)
- América/Nassau (UTC-04:00)
- América/Kentucky/Monticello (UTC-04:00)
- Brasil/Oeste (UTC-04:00)
- América/Aruba (UTC-04:00)
- América/Indiana/Indianápolis (UTC-04:00)
- América/Santiago (UTC-04:00)
- América/La_Paz (UTC-04:00)
- América/Thunder_Bay (UTC-04:00)
- América/Indiana/Marengo (UTC-04:00)
- América/Blanc-Sablon (UTC-04:00)
- América/Santo_Domingo (UTC-04:00)
- EE. UU./Este (UTC-04:00)

- Canadá/Este (UTC-04:00)
- América/Puerto_Príncipe (UTC-04:00)
- América/San_Bartolomé (UTC-04:00)
- América/Nipigon (UTC-04:00)
- EE. UU./Indiana del Este (UTC-04:00)
- América/Santa_Lucía (UTC-04:00)
- América/Montserrat (UTC-04:00)
- América/Lower_Princes (UTC-04:00)
- América/Detroit (UTC-04:00)
- América/Tórtola (UTC-04:00)
- América/Porto_Velho (UTC-04:00)
- América/Campo_Grande (UTC-04:00)
- América/Virgin (UTC-04:00)
- América/Pangnirtung (UTC-04:00)
- América/Montreal (UTC-04:00)
- América/Indiana/Winamac (UTC-04:00)
- América/Boa_Vista (UTC-04:00)
- América/Granada (UTC-04:00)
- América/Nueva_York (UTC-04:00)
- América/St_Kitts (UTC-04:00)
- América/Caracas (UTC-04:00)
- América/Guadalupe (UTC-04:00)
- América/Toronto (UTC-04:00)
- SystemV/EST5EDT (UTC-04:00)
- América/Argentina/Catamarca (UTC-03:00)
- Canadá/Atlántico (UTC-03:00)
- América/Argentina/Córdoba (UTC-03:00)
- América/Araguaina (UTC-03:00)
- América/Argentina/Salta (UTC-03:00)

- Etc/GMT+3 (UTC-03:00)
- América/Montevideo (UTC-03:00)
- Brasil/Este (UTC-03:00)
- América/Argentina/Mendoza (UTC-03:00)
- América/Argentina/Río_Gallegos (UTC-03:00)
- América/Catamarca (UTC-03:00)
- América/Córdoba (UTC-03:00)
- América/Sao_Paulo (UTC-03:00)
- América/Argentina/Jujuy (UTC-03:00)
- América/Cayenne (UTC-03:00)
- América/Recife (UTC-03:00)
- América/Buenos_Aires (UTC-03:00)
- América/Paramaribo (UTC-03:00)
- América/Moncton (UTC-03:00)
- América/Mendoza (UTC-03:00)
- América/Santarén (UTC-03:00)
- Atlántico/Bermudas (UTC-03:00)
- América/Maceió (UTC-03:00)
- Atlántico/Stanley (UTC-03:00)
- América/Halifax (UTC-03:00)
- Antártica/Rothera (UTC-03:00)
- América/Argentina/San_Luis (UTC-03:00)
- América/Argentina/Ushuaia (UTC-03:00)
- Antártica/Palmer (UTC-03:00)
- América/Punta_Arenas (UTC-03:00)
- América/Glace_Bay (UTC-03:00)
- América/Fortaleza (UTC-03:00)
- América/Thule (UTC-03:00)
- América/Argentina/La_Rioja (UTC-03:00)

- América/Belén (UTC-03:00)
- América/Jujuy (UTC-03:00)
- América/Bahía (UTC-03:00)
- América/Goose_Bay (UTC-03:00)
- América/Argentina/San_Juan (UTC-03:00)
- América/Argentina/ (UTC- 03:00) ComodRivadavia
- América/Argentina/Tucumán (UTC-03:00)
- América/Rosario (UTC-03:00)
- SystemV/AST4ADT (UTC-03:00)
- América/Argentina/Buenos_Aires (UTC-03:00)
- América/St_Johns (UTC-02:30)
- Canadá/Terranova (UTC-02:30)
- América/Miquelón (UTC-02:00)
- Etc/GMT+2 (UTC-02:00)
- América/Godthab (UTC-02:00)
- América/Noronha (UTC-02:00)
- Brasil/ DeNoronha (UTC- 02:00)
- Atlántico/Georgia_del_Sur (UTC-02:00)
- Etc/GMT+1 (UTC-01:00)
- Atlántico/Cabo_Verde (UTC-01:00)
- Pacífico/Kiritimati (UTC+14:00)
- Etc/GMT-14 (UTC+14:00)
- Pacífico/Fakaofo (UTC+13:00)
- Pacífico/Enderbury (UTC+13:00)
- Pacífico/Apia (UTC+13:00)
- Pacífico/Tongatapu (UTC+13:00)
- Etc/GMT-13 (UTC+13:00)
- NZ-CHAT (UTC+12:45)
- Pacífico/Chatham (UTC+12:45)

- Pacífico/Kwajalein (UTC+12:00)
- Antártica/ McMurdo (UTC+ 12:00)
- Pacífico/Wallis (UTC+12:00)
- Pacífico/Fiyi (UTC+12:00)
- Pacífico/Funafuti (UTC+12:00)
- Pacífico/Nauru (UTC+12:00)
- Kwajalein (UTC+12:00)
- NZ (UTC+12:00)
- Pacífico/Wake (UTC+12:00)
- Antártica/Polo_Sur (UTC+12:00)
- Pacífico/Tarawa (UTC+12:00)
- Pacífico/Auckland (UTC+12:00)
- Asia/Kamchatka (UTC+12:00)
- Etc/GMT-12 (UTC+12:00)
- Asia/Anádyr (UTC+12:00)
- Pacífico/Majuro (UTC+12:00)
- Pacífico/Ponapé (UTC+11:00)
- Pacífico/Bougainville (UTC+11:00)
- Antártica/Macquarie (UTC+11:00)
- Pacífico/Pohnpei (UTC+11:00)
- Pacífico/Efaté (UTC+11:00)
- Pacífico/Norfolk (UTC+11:00)
- Asia/Magadán (UTC+11:00)
- Pacífico/Kosrae (UTC+11:00)
- Asia/Sajalín (UTC+11:00)
- Pacífico/Numea (UTC+11:00)
- Etc/GMT-11 (UTC+11:00)
- Asia/Srednekolymsk (UTC+11:00)

- Pacífico/Guadalcanal (UTC+11:00)
- Australia/Lord_Howe (UTC+10:30)
- Australia/LHI (UTC+10:30)
- Australia/Hobart (UTC+10:00)
- Pacífico/Yap (UTC+10:00)
- Australia/Tasmania (UTC+10:00)
- Pacífico/Puerto_Moresby (UTC+10:00)
- Australia/ACT (UTC+10:00)
- Australia/Victoria (UTC+10:00)
- Pacífico/Chuuk (UTC+10:00)
- Australia/Queensland (UTC+10:00)
- Australia/Canberra (UTC+10:00)
- Australia/Currie (UTC+10:00)
- Pacífico/Guam (UTC+10:00)
- Pacífico/Truk (UTC+10:00)
- Australia/Nueva_Gales_del_Sur (UTC+10:00)
- Asia/Vladivostok (UTC+10:00)
- Pacífico/Saipán (UTC+10:00)
- Antártica/Dumont Durville (UTC+10:00)
- Australia/Sídney (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/Norte (UTC+09:30)
- Australia/Yancowinna (UTC+09:30)
- Australia/Adelaida (UTC+09:30)

- Australia/Broken_Hill (UTC+09:30)
- Australia/Sur (UTC+09:30)
- Australia/Darwin (UTC+09:30)
- Etc/GMT-9 (UTC+09:00)
- Pacífico/Palaos (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)
- ROK (UTC+09:00)
- Asia/Seúl (UTC+09:00)
- Asia/Khandyga (UTC+09:00)
- Japón (UTC+09:00)
- Asia/Tokio (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/Choybalsan (UTC+08:00)
- Asia/Shanghái (UTC+08:00)
- Antártica/Casey (UTC+08:00)
- Asia/Ulán_Bator (UTC+08:00)
- Asia/Chongqing (UTC+08:00)
- Asia/Ulaanbaatar (UTC+08:00)
- Asia/Taipéi (UTC+08:00)

- Asia/Manila (UTC+08:00)
- RPC (UTC+08:00)
- Asia/Ujung_Pandang (UTC+08:00)
- Asia/Harbin (UTC+08:00)
- Singapur (UTC+08:00)
- Asia/Brunéi (UTC+08:00)
- Australia/Oeste (UTC+08:00)
- Asia/Hong_Kong (UTC+08:00)
- Asia/Macasar (UTC+08:00)
- HongKong (UTC+08:00)
- Asia/Kuala_Lumpur (UTC+08:00)
- Asia/Irkutsk (UTC+08:00)
- Asia/Singapur (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)
- Antártica/Davis (UTC+07:00)
- Asia/Tomsk (UTC+07:00)
- Asia/Yakarta (UTC+07:00)
- Asia/Barnaul (UTC+07:00)
- India/Navidad (UTC+07:00)
- Asia/Ho_Chi_Minh (UTC+07:00)
- Asia/Hovd (UTC+07:00)
- Asia/Bangkok (UTC+07:00)
- Asia/Vientián (UTC+07:00)
- Asia/Novokuznetsk (UTC+07:00)
- Asia/Krasnoyarsk (UTC+07:00)
- Asia/Saigón (UTC+07:00)

- Asia/Yangon (UTC+06:30)
- Asia/Rangún (UTC+06:30)
- India/Cocos (UTC+06:30)
- Asia/Kasgar (UTC+06:00)
- Etc/GMT-6 (UTC+06:00)
- Asia/Almatý (UTC+06:00)
- Asia/Dacca (UTC+06:00)
- Asia/Omsk (UTC+06:00)
- Asia/Dhaka (UTC+06:00)
- India/Chagos (UTC+06:00)
- Asia/Kyzylorda (UTC+06:00)
- Asia/Bishkek (UTC+06:00)
- Antártica/Vostok (UTC+06:00)
- Asia/Urumqi (UTC+06:00)
- Asia/Timbu (UTC+06:00)
- Asia/Thimphu (UTC+06:00)
- Asia/Katmandú (UTC+05:45)
- Asia/Katmandu (UTC+05:45)
- Asia/Calcuta (UTC+05:30)
- Asia/Colombo (UTC+05:30)
- Asia/Calcutta (UTC+05:30)
- Asia/Aktau (UTC+05:00)
- Etc/GMT-5 (UTC+05:00)
- Asia/Samarcanda (UTC+05:00)
- Asia/Karachi (UTC+05:00)
- Asia/Ekaterimburgo (UTC+05:00)
- Asia/Dusambé (UTC+05:00)
- India/Maldivas (UTC+05:00)
- Asia/Oral (UTC+05:00)

- Asia/Taskent (UTC+05:00)
- Antártica/Mawson (UTC+05:00)
- Asia/Aktobé (UTC+05:00)
- Asia/Asjabad (UTC+05:00)
- Asia/Ashgabat (UTC+05:00)
- Asia/Atirau (UTC+05:00)
- India/Kerguelen (UTC+05:00)
- Irán (UTC+04:30)
- Asia/Teherán (UTC+04:30)
- Asia/Kabul (UTC+04:30)
- Asia/Ereván (UTC+04:00)
- Etc/GMT-4 (UTC+04:00)
- Etc/GMT-4 (UTC+04:00)
- Asia/Dubái (UTC+04:00)
- India/Reunión (UTC+04:00)
- Europa/Sarátov (UTC+04:00)
- Europa/Samara (UTC+04:00)
- India/Mahé (UTC+04:00)
- Asia/Bakú (UTC+04:00)
- Asia/Mascate (UTC+04:00)
- Europa/Volgogrado (UTC+04:00)
- Europa/Astracán (UTC+04:00)
- Asia/Tiflis (UTC+04:00)
- Europa/Uliánovsk (UTC+04:00)
- Asia/Adén (UTC+03:00)
- África/Nairobi (UTC+03:00)
- Europa/Estambul (UTC+03:00)
- Etc/GMT-3 (UTC+03:00)
- Europa/Zaporiyia (UTC+03:00)

- Israel (UTC+03:00)
- India/Comoro (UTC+03:00)
- Antártica/Syowa (UTC+03:00)
- África/Mogadiscio (UTC+03:00)
- Europa/Bucarest (UTC+03:00)
- África/Asmera (UTC+03:00)
- Europa/Mariehamn (UTC+03:00)
- Asia/Estambul (UTC+03:00)
- Europa/Tiráspol (UTC+03:00)
- Europa/Moscú (UTC+03:00)
- Europa/Chisináu (UTC+03:00)
- Europa/Helsinki (UTC+03:00)
- Asia/Beirut (UTC+03:00)
- Asia/Tel_Aviv (UTC+03:00)
- África/Yibuti (UTC+03:00)
- Europa/Simferópol (UTC+03:00)
- Europa/Sofía (UTC+03:00)
- Asia/Gaza (UTC+03:00)
- África/Asmara (UTC+03:00)
- Europa/Riga (UTC+03:00)
- Asia/Bagdad (UTC+03:00)
- Asia/Damasco (UTC+03:00)
- África/Dar_es_Salaam (UTC+03:00)
- África/Addis_Ababa (UTC+03:00)
- Europa/Úzhgorod (UTC+03:00)
- Asia/Jerusalén (UTC+03:00)
- Asia/Riad (UTC+03:00)
- Asia/Kuwait (UTC+03:00)
- Europa/Kirov (UTC+03:00)

- África/Kampala (UTC+03:00)
- Europa/Minsk (UTC+03:00)
- Asia/Catar (UTC+03:00)
- Europa/Kiev (UTC+03:00)
- Asia/Bahréin (UTC+03:00)
- Europa/Vilna (UTC+03:00)
- India/Antananarivo (UTC+03:00)
- India/Mayotte (UTC+03:00)
- Europa/Tallin (UTC+03:00)
- Turquía (UTC+03:00)
- África/Juba (UTC+03:00)
- Asia/Nicosia (UTC+03:00)
- Asia/Famagusta (UTC+03:00)
- W-SU (UTC+03:00)
- EET (UTC+03:00)
- Asia/Hebrón (UTC+03:00)
- Asia/Ammán (UTC+03:00)
- Europa/Nicosia (UTC+03:00)
- Europa/Atenas (UTC+03:00)
- África/El_Cairo (UTC+02:00)
- África/Babane (UTC+02:00)
- Europa/Bruselas (UTC+02:00)
- Europa/Varsovia (UTC+02:00)
- CET (UTC+02:00)
- Europa/Luxemburgo (UTC+02:00)
- Etc/GMT-2 (UTC+02:00)
- Libia (UTC+02:00)
- África/Kigali (UTC+02:00)
- África/Trípoli (UTC+02:00)

- Europa/Kaliningrado (UTC+02:00)
- África/Windhoek (UTC+02:00)
- Europa/Malta (UTC+02:00)
- Europa/Bosingen (UTC+02:00)
-
- Europa/Skopie (UTC+02:00)
- Europa/Sarajevo (UTC+02:00)
- Europa/Roma (UTC+02:00)
- Europa/Zúrich (UTC+02:00)
- Europa/Gibraltar (UTC+02:00)
- África/Lubumbashi (UTC+02:00)
- Europa/Vaduz (UTC+02:00)
- Europa/Liubliana (UTC+02:00)
- Europa/Berlín (UTC+02:00)
- Europa/Estocolmo (UTC+02:00)
- Europa/Budapest (UTC+02:00)
- Europa/Zagreb (UTC+02:00)
- Europa/París (UTC+02:00)
- África/Ceuta (UTC+02:00)
- Europa/Praga (UTC+02:00)
- Antártica/Troll (UTC+02:00)
- África/Gaborone (UTC+02:00)
- Europa/Copenhague (UTC+02:00)
- Europa/Viena (UTC+02:00)
- Europa/Tirana (UTC+02:00)
- MET (UTC+02:00)
- Europa/Ámsterdam (UTC+02:00)
- África/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)
- África/Buyumbura (UTC+02:00)
- Atlántico/Jan_Mayen (UTC+02:00)
- África/Maseru (UTC+02:00)
- Europa/Madrid (UTC+02:00)
- África/Blantire (UTC+02:00)
- África/Lusaka (UTC+02:00)
- África/Harare (UTC+02:00)
- África/Jartum (UTC+02:00)
- África/Johannesburgo (UTC+02:00)
- Europa/Belgrado (UTC+02:00)
- Europa/Bratislava (UTC+02:00)
- Ártico/Longyearbyen (UTC+02:00)
- Egipto (UTC+02:00)
- Europa/Vaticano (UTC+02:00)
- Europa/Mónaco (UTC+02:00)
- Europa/Londres (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)
- África/Túnez (UTC+01:00)
- África/Malabo (UTC+01:00)
- GB-Eire (UTC+01:00)
- África/Lagos (UTC+01:00)
- África/Argel (UTC+01:00)

- GB (UTC+01:00)
- Portugal (UTC+01:00)
- África/Sao_Tome (UTC+01:00)
- África/Yamena (UTC+01:00)
- Atlántico/Islas Faeroe (UTC+01:00)
- Eire (UTC+01:00)
- Atlántico/Islas Feroe (UTC+01:00)
- Europa/Dublín (UTC+01:00)
- África/Libreville (UTC+01:00)
- África/El_Aaiún (UTC+01:00)
- África/El_Aaiún (UTC+01:00)
- África/Duala (UTC+01:00)
- África/Brazzaville (UTC+01:00)
- África/Porto-Novo (UTC+01:00)
- Atlántico/Madeira (UTC+01:00)
- Europa/Lisboa (UTC+01:00)
- Atlántico/Canarias (UTC+01:00)
- África/Casablanca (UTC+01:00)
- Europa/Belfast (UTC+01:00)
- África/Luanda (UTC+01:00)
- África/Kinsasa (UTC+01:00)
- África/Bangui (UTC+01:00)
- WET (UTC+01:00)
- África/Niamey (UTC+01:00)
- GMT (UTC+00:00)
- Etc/GMT-0 (UTC+00:00)
- Atlántico/St_Helena (UTC+00:00)
- Etc/GMT+0 (UTC+00:00)
- África/Banjul (UTC+00:00)

- Etc/GMT (UTC+00:00)
- África/Freetown (UTC+00:00)
- África/Bamako (UTC+00:00)
- África/Conakri (UTC+00:00)
- Universal (UTC+00:00)
- África/Nuakchot (UTC+00:00)
- UTC (UTC+00:00)
- Etc/Universal (UTC+00:00)
- Atlántico/Azores (UTC+00:00)
- África/Abiyán (UTC+00:00)
- África/Acra (UTC+00:00)
- Etc/UCT (UTC+00:00)
- GMT0 (UTC+00:00)
- Zulú (UTC+00:00) Zulú (UTC+00:00)
- África/Uagadugú (UTC+00:00)
- Atlántico/Reikiavik (UTC+00:00)
- Etc/Zulú (UTC+00:00)
- Islandia (UTC+00:00)
- África/Lomé (UTC+00:00)
- Greenwich (UTC+00:00)
- Etc/GMT0 (UTC+00:00)
- América/Danmarkshavn (UTC+00:00)
- África/Dakar (UTC+00:00)
- África/Bisáu (UTC+00:00)
- Etc/Greenwich (UTC+00:00)
- África/Tombuctú (UTC+00:00)
- UTC (UTC+00:00)
- África/Monrovia (UTC+00:00)
- Etc/UTC (UTC+00:00)

Tutoriales de expresiones de fórmula

Puede seguir estos tutoriales para utilizar expresiones de fórmula en AWS IoT SiteWise.

Temas

- Uso de cadenas en las fórmulas
- Filtrado de puntos de datos
- Recuento de los puntos de datos que coinciden con una condición
- Datos antiguos en las fórmulas
- Calidad de los datos en las fórmulas
- Valores indefinidos, infinitos y de desbordamiento

Uso de cadenas en las fórmulas

Puede operar con cadenas en sus expresiones de fórmula. También puede introducir cadenas a partir de variables que hacen referencia a propiedades de atributos y medidas.

> **Important**
>
> Las expresiones de fórmula solo pueden generar valores dobles o de cadena. Las expresiones anidadas pueden generar otros tipos de datos, como cadenas, pero la fórmula en su conjunto debe evaluarse como un número o una cadena. Puede usar la función jp para convertir una cadena en un número. El valor booleano debe ser 1 (verdadero) o 0 (falso). Para obtener más información, consulte Valores indefinidos, infinitos y de desbordamiento.

AWS IoT SiteWise proporciona las siguientes funciones de expresión de fórmulas que puede utilizar para operar con cadenas:

- Literales de cadena
- El operador de índice (`s[index]`)
- El operador de sector (`s[start:end:step]`)
- Funciones de comparación, que puede utilizar para comparar cadenas en orden lexicográfico
- Funciones de cadena, que incluyen la `jp` función que puede analizar objetos JSON serializados y convertir cadenas en números

Filtrado de puntos de datos

Puede utilizar la función if para filtrar los puntos de datos que no cumplan una condición. La función `if` evalúa una condición y devuelve valores diferentes para los resultados `true` y `false`. Puede utilizar la constante none como resultado para un caso de una función `if`, para descartar el punto de datos de ese caso.

Para filtrar los puntos de datos que coinciden con una condición

- Cree una transformación que utilice la función `if` para definir una condición que compruebe si se cumple una condición y que devuelva none como el valor `result_if_true` o `result_if_false`.

Example Ejemplo: filtrar los puntos de datos en los que el agua no esté hirviendo

Considere un escenario en el que usted tiene una medición, `temp_c`, que proporciona la temperatura (en Celsius) del agua de una máquina. Puede definir la siguiente transformación para filtrar los puntos de datos en los que el agua no esté hirviendo:

- Transformación `boiling_temps = if(gte(temp_c, 100), temp_c, none)`: devuelve la temperatura si es mayor o igual a 100 grados Celsius; de lo contrario, no devuelve ningún punto de datos.

Recuento de los puntos de datos que coinciden con una condición

Puede utilizar funciones de comparación y sum() para contar el número de puntos de datos para los que se cumple una condición.

Para contar los puntos de datos que coinciden con una condición

1. Cree una transformación que utilice una función de comparación para definir una condición de filtro en otra propiedad.
2. Cree una métrica que sume los puntos de datos donde se cumple esa condición.

Example Ejemplo: Contar el número de puntos de datos en los que el agua está hirviendo

Considere un escenario en el que usted tiene una medición, `temp_c`, que proporciona la temperatura (en Celsius) del agua de una máquina. Puede definir las siguientes propiedades de transformación y métrica para contar el número de puntos de datos en los que hierve el agua:

- Transformación `is_boiling = gte(temp_c, 100)`: devuelve `1` si la temperatura es mayor o igual a 100 grados Celsius; de lo contrario, devuelve `0`.
- Métrica `boiling_count = sum(is_boiling)`: devuelve el número de puntos de datos en los que el agua está hirviendo.

Datos antiguos en las fórmulas

AWS IoT SiteWise admite la ingesta tardía de datos con una antigüedad de hasta 7 días. Cuando AWS IoT SiteWise recibe datos atrasados, recalcula los valores existentes para cualquier métrica que introduzca los datos atrasados en una ventana anterior. Estos nuevos cálculos dan lugar a cargos de procesamiento de datos.

> **Note**
>
> Cuando AWS IoT SiteWise calcula las propiedades que introducen datos atrasados, utiliza la expresión de fórmula actual de cada propiedad.

Después de AWS IoT SiteWise volver a calcular la ventana anterior de una métrica, reemplaza el valor anterior de esa ventana. Si ha activado las notificaciones para esa métrica, AWS IoT SiteWise también emite una notificación del valor de la propiedad. Esto significa que puede recibir una nueva notificación de actualización de valor de propiedad para la misma propiedad y marca temporal para la que recibió previamente una notificación. Si las aplicaciones o lagos de datos consumen notificaciones de valor de propiedad, debe actualizar el valor anterior con el nuevo valor para que sus datos sean precisos.

Calidad de los datos en las fórmulas

En AWS IoT SiteWise, cada punto de datos tiene un código de calidad, que puede ser uno de los siguientes:

- `GOOD`: los datos no se ven afectados por ningún problema.
- `BAD`: los datos se ven afectados por un problema, como un fallo del sensor.
- `UNCERTAIN`: los datos se ven afectados por un problema, como la falta de precisión de un sensor.

AWS IoT SiteWise consume solo datos `GOOD` de calidad cuando calcula las transformaciones y las métricas. AWS IoT SiteWise genera solo datos `GOOD` de calidad para que los cálculos se realicen

correctamente. Si un cálculo no se realiza correctamente, AWS IoT SiteWise no genera un punto de datos para ese cálculo. Esto puede ocurrir si un cálculo da como resultado un valor indefinido, infinito o de desbordamiento.

Para obtener más información acerca de cómo consultar datos y filtrar por calidad de datos, consulte Consulta datos de AWS IoT SiteWise.

Valores indefinidos, infinitos y de desbordamiento

Algunas expresiones de fórmula (como `x / 0`sqrt(-1), olog(0)) calculan valores indefinidos en un sistema de números reales, infinitos o que están fuera del rango admitido por él. AWS IoT SiteWise Cuando la expresión de una propiedad de un activo calcula un valor indefinido, infinito o desbordante, AWS IoT SiteWise no genera ningún punto de datos para ese cálculo.

AWS IoT SiteWise tampoco genera un punto de datos si calcula un valor no numérico como resultado de una expresión de fórmula. Esto significa que si se define una fórmula que calcula una cadena, una matriz o la constante none, AWS IoT SiteWise no generará ningún punto de datos para ese cálculo.

Example Ejemplos

Cada una de las siguientes expresiones de fórmula da como resultado un valor que no AWS IoT SiteWise se puede representar como un número. AWS IoT SiteWise no genera un punto de datos cuando calcula estas expresiones de fórmula.

- `x / 0` es indefinido.
- `log(0)` es indefinido.
- `sqrt(-1)` es indefinido en un sistema numérico real.
- `"hello" + " world"` es una cadena.
- `jp('{"values":[3,6,7]}', '$.values')` es una matriz.
- `if(gte(temp, 300), temp, none)` es `none` cuando `temp` es menos de `300`.

Creación de modelos compuestos personalizados (componentes)

Los modelos compuestos personalizados, o componentes si utiliza la consola, proporcionan otro nivel de organización para sus modelos de activos y modelos de componentes. Puede utilizarlos para estructurar sus modelos agrupando propiedades o haciendo referencia a otros modelos. Para

obtener más información sobre cómo trabajar con modelos compuestos personalizados, consulte. Modelos compuestos personalizados (componentes)

Puede crear un modelo compuesto personalizado dentro de un modelo de activos o de componentes existente. Hay dos tipos de modelos compuestos personalizados. Para agrupar propiedades relacionadas dentro de un modelo, puede crear un modelo compuesto personalizado en línea. Para hacer referencia a un modelo de componentes dentro de su modelo de activos o modelo de componentes, puede crear un modelo compuesto component-model-basedpersonalizado.

En las siguientes secciones se describe cómo utilizar la AWS IoT SiteWise API para crear modelos compuestos personalizados.

Temas

- Crear un componente en línea (consola)
- Crear un modelo compuesto personalizado en línea ()AWS CLI
- Creación de un component-model-based componente (consola)
- Crear un modelo compuesto component-model-based personalizado (AWS CLI)

Crear un componente en línea (consola)

Puede usar la AWS IoT SiteWise consola para crear un componente en línea que defina sus propias propiedades.

> **Note**
>
> Como se trata de un componente en línea, estas propiedades solo se aplican al modelo de activos actual y no se comparten en ningún otro lugar.
> Si necesita crear un modelo reutilizable (por ejemplo, para compartirlo entre varios modelos de activos o para incluir varias instancias en un modelo de activos), debe crear un componente basado en un modelo de componentes. Consulte la siguiente sección para obtener más información.

Para crear un componente (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Models (Modelos).

3. Elija el modelo de activo al que desea añadir un componente.
4. En la pestaña Propiedades, elija Componentes.
5. Selecciona Crear componente.
6. En la página Crear componente, haga lo siguiente:

    a. Introduzca un nombre para el componente, como **`ServoMotor`** o**`ServoMotor Model`**. Este nombre debe ser único en todos los componentes de su cuenta en esta región.

    b. (Opcional) Agregue Definiciones de atributos para el modelo. Los atributos representan información que rara vez cambia. Para obtener más información, consulte Definición de datos estáticos (atributos).

    c. (Opcional) Agregue Definiciones de mediciones para el modelo. Las mediciones representan flujos de datos de su equipo. Para obtener más información, consulte Definición de flujos de datos procedentes del equipo (mediciones).

    d. (Opcional) Agregue Definiciones de transformación para el modelo. Las transformaciones son fórmulas que asignan datos de un formulario a otro. Para obtener más información, consulte Transformación de datos (transformaciones).

    e. (Opcional) Agregue Definiciones de métricas para el modelo. Las métricas son fórmulas que agregan datos a lo largo de intervalos de tiempo. Las métricas pueden agregar datos de entrada de activos asociados, de modo que puede calcular valores que representan la operación o un subconjunto de la operación. Para obtener más información, consulte Agregación de datos de propiedades y otros activos (métricas).

    f. Selecciona Crear componente.

Crear un modelo compuesto personalizado en línea ()AWS CLI

Puede usar el AWS Command Line Interface (AWS CLI) para crear un modelo compuesto personalizado en línea que defina sus propias propiedades.

Utilice la CreateAssetModelCompositeModeloperación para crear un modelo en línea con propiedades. Esta operación espera una carga con la siguiente estructura.

> **Note**
>
> Como se trata de un modelo compuesto en línea, estas propiedades solo se aplican al modelo de activos actual y no se comparten en ningún otro lugar. Lo que lo convierte en «integrado» es que no proporciona un valor para el `composedAssetModelId` campo.

Si necesita crear un modelo reutilizable (por ejemplo, para compartirlo entre varios modelos de activos o para incluir varias instancias dentro de un modelo de activos), debe crear un modelo component-model-basedcompuesto en su lugar. Consulte la siguiente sección para obtener más información.

```
{
    "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"
        }
    ]
}
```

Creación de un component-model-based componente (consola)

Puede utilizar la AWS IoT SiteWise consola para crear un componente a partir de un modelo de componentes.

Para crear un component-model-based componente (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Models (Modelos).
3. Elija el modelo de activo al que desea añadir un componente.
4. En la pestaña Propiedades, elija Componentes.

5. Selecciona Crear componente.
6. En la página Crear componente, haga lo siguiente:

   a. Seleccione el modelo de componente en el que desee basar el componente.

   b. Introduzca un nombre para el componente, como **`ServoMotor`** o**`ServoMotor Model`**. Este nombre debe ser único en todos los componentes de su cuenta en esta región.

   c. Selecciona Crear componente.

Crear un modelo compuesto component-model-based personalizado (AWS CLI)

Puede usarlo AWS CLI para crear un modelo compuesto component-model-based personalizado dentro de su modelo de activos. Un modelo compuesto component-model-based personalizado es una referencia a un modelo de componentes que ya ha definido en otro lugar.

Utilice la CreateAssetModelCompositeModeloperación para crear un modelo compuesto component-model-based personalizado. Esta operación espera una carga con la siguiente estructura.

> **Note**
>
> En este ejemplo, el valor de `composedAssetModelId` es el ID del modelo de activo o el ID externo de un modelo de componente existente. Para obtener más información, consulte Hacer referencia a objetos con identificadores externos en la Guía del usuario de AWS IoT SiteWise . Para ver un ejemplo de cómo crear un modelo de componentes, consulteCrear un modelo de componentes (AWS CLI).

```
{
    "assetModelCompositeModelName": "CNCLathe_ServoMotorA",
    "assetModelCompositeModelType": "CUSTOM",
    "composedAssetModelId": component model ID
]
```

Como es solo una referencia, un modelo compuesto component-model-based personalizado no tiene propiedades propias, salvo un nombre.

Si desea añadir varias instancias del mismo componente a su modelo de activos (por ejemplo, una máquina CNC con varios servomotores), puede añadir varios modelos compuestos component-

model-based personalizados, cada uno con su propio nombre, pero que hagan referencia al mismo `composedAssetModelId` nombre.

Puede anidar componentes dentro de otros componentes. Para ello, puede añadir un modelo component-model-based compuesto, como se muestra en este ejemplo, a uno de sus modelos de componentes.

Creación de activos

Puede crear un activo a partir de un modelo de activos. Debe tener un modelo de activos para poder crear un activo. Si no ha creado un modelo de activos, consulte Creación de modelos de activos.

> **Note**
>
> Solo se pueden crear activos a partir de modelos `ACTIVE`. Si el estado del modelo no es `ACTIVE`, es posible que tenga que esperar hasta unos minutos para poder crear activos a partir de ese modelo. Para obtener más información, consulte Estados de activos y modelos.

Temas

- Creación de un activo (consola)
- Crear un activo ()AWS CLI
- Configuración de un nuevo activo

Creación de un activo (consola)

Puede utilizar la AWS IoT SiteWise consola para crear un activo.

Para crear un activo (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Activos.
3. Elija Create asset (Crear activo).
4. En la página Crear activo, haga lo siguiente:

    a. En Modelo, elija el modelo de activos desde el que desea crear un activo.

> **Note**
>
> Si el modelo no está ACTIVO, debe esperar hasta que se active o resolver los problemas si está en ERROR.

b. Escriba un Nombre para el activo.

c. (Opcional) Agregue etiquetas para su activo. Para obtener más información, consulte Etiquetar sus recursos AWS IoT SiteWise.

d. Elija Create asset (Crear activo).

Al crear un activo, la AWS IoT SiteWise consola navega hasta la página del nuevo activo. En esta página, puede consultar el Estado del activo, que inicialmente es CREANDO. Esta página se actualiza automáticamente, por lo que puede esperar a que se actualice el estado del activo.

> **Note**
>
> El proceso de creación de activos puede tardar hasta un minuto. Después de que el Estado esté ACTIVO, puede realizar operaciones de actualización en el activo. Para obtener más información, consulte Estados de activos y modelos.

Después de crear un activo, consulte Configuración de un nuevo activo.

Crear un activo ()AWS CLI

Puede usar el AWS Command Line Interface (AWS CLI) para crear un activo a partir de un modelo de activos.

Debe tener un `assetModelId` para crear un activo. Si has creado un modelo de activos, pero no lo conoces`assetModelId`, usa la ListAssetModelsAPI para ver todos tus modelos de activos.

Para crear un activo a partir de un modelo de activos, usa la CreateAssetAPI con los siguientes parámetros:

- `assetName`: el nombre del nuevo activo. Asigne un nombre a su activo que le ayude a identificarlo.

- `assetModelId`: el ID del activo. Este es el ID real en formato UUID, o `externalId:myExternalId` si lo tiene. Para obtener más información, consulte Hacer referencia a objetos con identificadores externos en la Guía del usuario de AWS IoT SiteWise .

Para crear un activo ()AWS CLI

- Ejecute el siguiente comando para crear un activo. *`Sustituya el nombre del`* activo por el nombre del activo y *`asset-model-id`*por el ID o el ID externo del modelo de activo.

```
aws iotsitewise create-asset \
  --asset-name asset-name \
  --asset-model-id asset-model-id
```

La operación devuelve una respuesta que contiene los detalles y el estado del nuevo activo en el siguiente formato.

```
{
  "assetId": "String",
  "assetArn": "String",
  "assetStatus": {
    "state": "String",
    "error": {
      "code": "String",
      "message": "String"
    }
  }
}
```

El `state` del activo es `CREATING` hasta que el activo crea.

> **Note**
>
> El proceso de creación de activos puede tardar hasta un minuto. Para comprobar el estado del activo, utilice la DescribeAssetoperación con el ID del activo como parámetro. `assetId` Cuando el `state` del activo sea `ACTIVE`, puede realizar operaciones de actualización en su activo. Para obtener más información, consulte Estados de activos y modelos.

Después de crear un activo, consulte Configuración de un nuevo activo.

Configuración de un nuevo activo

Termine de configurar su activo con cualquiera de las siguientes acciones opcionales:

- Asignación de flujos de datos industriales a propiedades de activos si su activo tiene propiedades de medición.
- Actualización de valores de atributos si su activo tiene valores de atributo únicos.
- Asociación y disociación de activos si su activo es un activo principal.

Búsqueda de activos

Utilice la función Consola de AWS IoT SiteWise de búsqueda para encontrar activos en función de los metadatos y los filtros del valor de las propiedades en tiempo real.

Requisitos previos

AWS IoT SiteWise requiere permisos para integrarse a fin de AWS IoT TwinMaker organizar y modelar mejor los datos industriales. Si ha concedido permisos para ello AWS IoT SiteWise, utilice la ExecuteQueryAPI. Si no ha concedido permisos y necesita ayuda para AWS IoT SiteWise empezar, consulteIntegración de AWS IoT SiteWise y AWS IoT TwinMaker.

Búsqueda avanzada en Consola de AWS IoT SiteWise

Búsqueda de metadatos

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, seleccione Búsqueda avanzada en Activos.
3. En Búsqueda avanzada, elija la opción de búsqueda de metadatos.
4. Rellene los parámetros. Rellene tantos campos como sea posible para una búsqueda eficiente.

    a. Nombre del activo: introduzca un nombre completo del activo o un nombre parcial para realizar una búsqueda más amplia.

    b. Nombre de la propiedad: introduzca el nombre completo de la propiedad o un nombre parcial para realizar una búsqueda más amplia.

    c. Operador: elija un operador entre:

- =
- <
- >
- <=
- >=

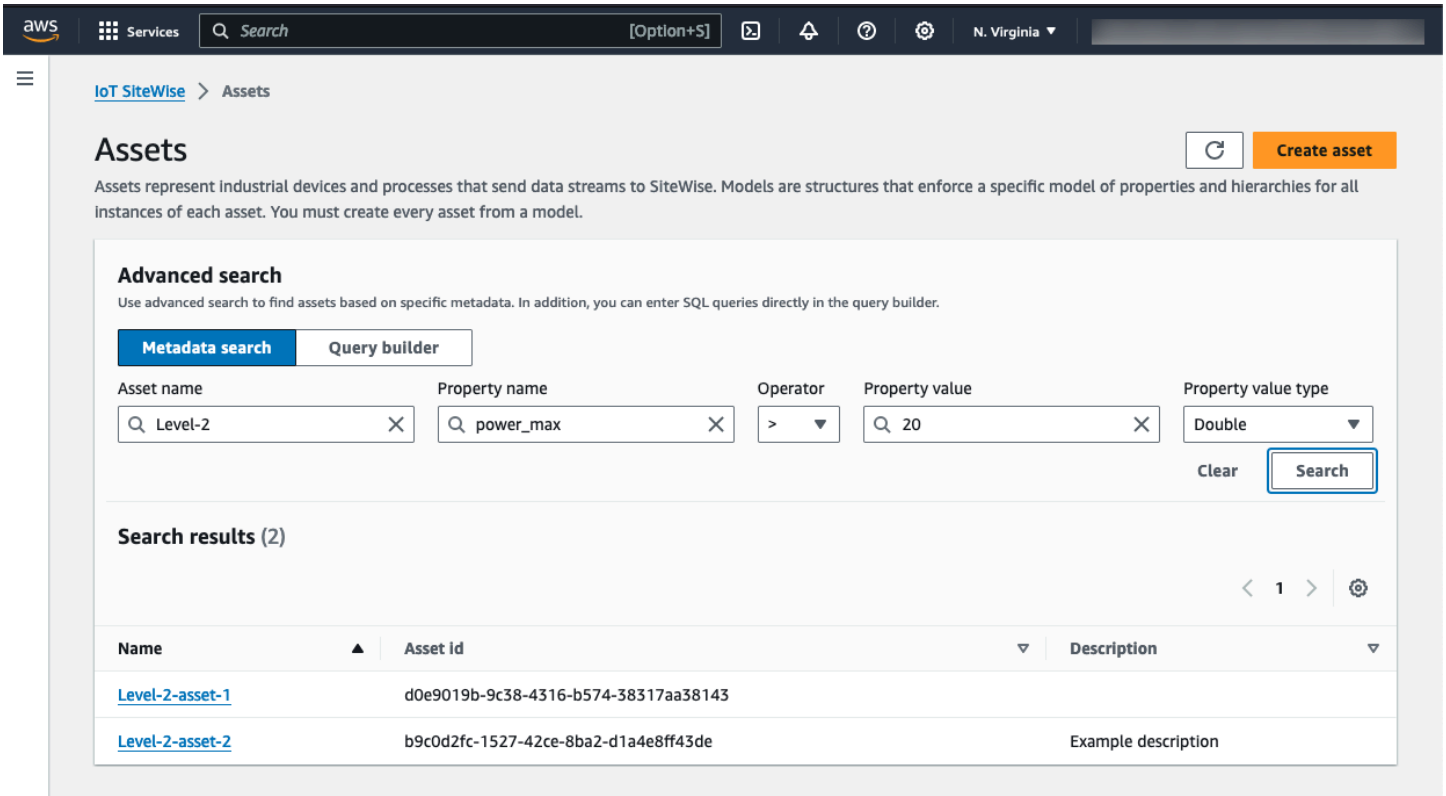
d. Valor de la propiedad: este valor se compara con el último valor de la propiedad.

e. Tipo de valor de propiedad: el tipo de datos de la propiedad. Elija una de las siguientes opciones:

- Doble
- Entero
- Cadena
- Booleano

5. Elija Buscar.

6. En la tabla de resultados de la búsqueda, elija el activo en la columna Nombre. Esto le llevará a la página detallada del activo en cuestión.



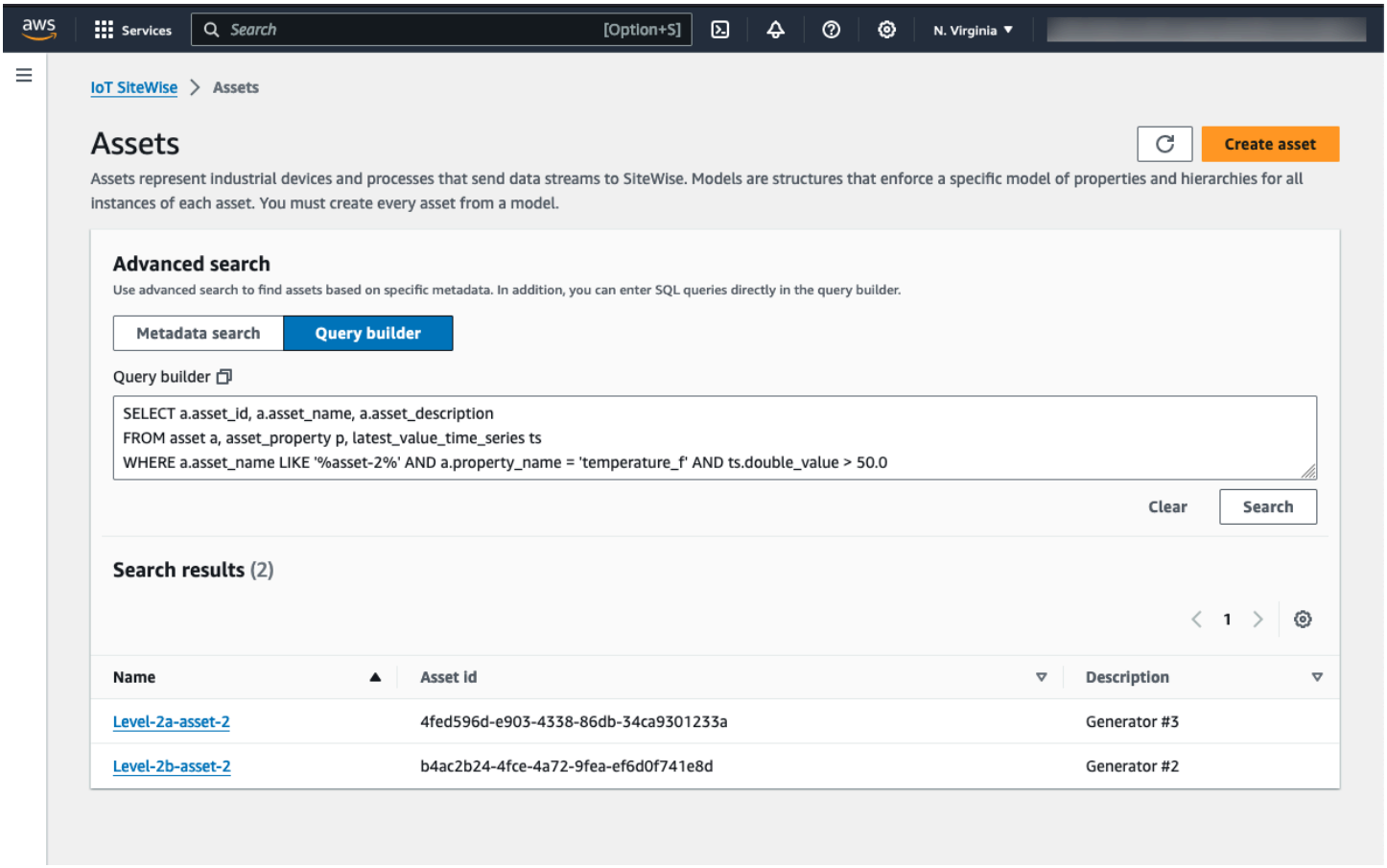
Búsqueda parcial

No es necesario proporcionar todos los parámetros para una búsqueda de activos. Estos son algunos ejemplos de búsquedas parciales que utilizan la opción de búsqueda de metadatos:

- Busque los activos por su nombre:
  - Introduzca un valor solo en el campo Nombre del activo.
  - Los campos Nombre de la propiedad y Valor de la propiedad están vacíos.
- Busque activos que contengan propiedades con un nombre específico:
  - Introduzca un valor solo en el campo Nombre de la propiedad.
  - Los campos Nombre del activo y Valor de la propiedad están vacíos.
- Busque activos en función de los valores más recientes de sus propiedades:
  - Introduzca los valores en los campos Nombre de la propiedad y Valor de la propiedad.
  - Seleccione un operador y un tipo de valor de propiedad.

Búsqueda en el generador de consultas

1. Vaya a Consola de AWS IoT SiteWise.
2. En el panel de navegación, seleccione Búsqueda avanzada en Activos.
3. En Búsqueda avanzada, elija la opción Generador de consultas.
4. En el panel Generador de consultas, escriba su consulta SQL para recuperar un`asset_name`, `asset_id` y`asset_description`.
5. Elija Buscar.
6. En la tabla de resultados de la búsqueda, elija el activo de la columna Nombre. Esto le llevará a la página detallada del activo en cuestión.



> **Note**
>
> - La `SELECT` cláusula de la consulta SQL debe incluir los `asset_id` campos `asset_name` y para garantizar que un activo sea válido en la tabla de resultados de la búsqueda.
> - El generador de consultas solo muestra el nombre, el identificador del activo y la descripción en la tabla de resultados. Añadir más campos a la `SELECT` cláusula no añade más columnas a la tabla de resultados

Asignación de flujos de datos industriales a propiedades de activos

Puede definir un alias de propiedad en la propiedad de un activo. Esto le ayuda a identificar la propiedad de un activo cuando ingiere o recupera los datos del activo. Si el activo tiene propiedades de medición, debe definir los alias de propiedad para mapear los flujos de datos a esas propiedades de medición.

Este proceso requiere que conozca el alias de su propiedad.

- Si ingiere datos de servidores OPC-UA mediante una fuente de datos OPC-UA en una puerta de enlace SiteWise Edge, el alias de su propiedad será la ruta a una variable situada en el nodo Objects, empezando por. `/`

  Example

  Si la ruta a su variable es`company/windfarm/3/turbine/7/temperature`, entonces el alias de su propiedad es. `/company/windfarm/3/turbine/7/temperature`

  Para obtener más información sobre la arquitectura de información del OPC-UA, consulte el modelo de información y el mapeo del espaciado de direcciones en la referencia en línea del OPC UA.

  > Notas
  >
  > - Si configura un prefijo de flujo de datos para el origen OPC-UA, debe incluir ese prefijo en el alias de propiedad para todas las secuencias de datos de ese origen.
  >
  >   Example
  >
  >   Si `/RentonWA` es un prefijo, entonces el alias anterior es. `/RentonWA/company/windfarm/3/turbine/7/temperature`
  > - Los alias de propiedades pueden contener hasta 1000 bits. Las rutas de variables OPC-UA pueden contener hasta 4096 bytes. Actualmente, AWS IoT SiteWise no admite la ingesta de datos de variables OPC-UA con rutas largas.

- Si ingiere datos de servidores Modbus mediante una fuente de datos Modbus TCP en una puerta de enlace SiteWise Edge, el alias de su propiedad es:

  Modbus `register set tag name`

  Utilice este valor para enviar datos de este conjunto de registros a una propiedad de activo.

- Si ingiere datos de otras fuentes, como mediante AWS IoT reglas o la API, debe definir los alias de sus propiedades. Puede definir un sistema de nombres de alias de propiedad que sea aplicable a la configuración de su dispositivo. Por ejemplo, si ingiere datos de elementos de AWS IoT , puede incluir el nombre del elemento en alias de propiedad para identificar de forma exclusiva las secuencias de datos. Para obtener más información sobre este ejemplo, consulta el tutorial sobre cómo ingerir datos de AWS IoT cosas.

Los alias de propiedad deben ser únicos dentro de una región y AWS una cuenta. AWS IoT SiteWise devuelve un error si se establece un alias de propiedad como uno que ya existe en otra propiedad del activo.

Si tiene varias fuentes OPC-UA con rutas de flujo de datos idénticas, añada un prefijo a las rutas de cada fuente para formar alias únicos. Para obtener más información, consulte Configuración de orígenes de datos.

> **Note**
>
> En esta sección se describe cómo establecer alias para las propiedades de medición. Para obtener más información sobre cómo configurar alias para las propiedades de los estados de las alarmas externas, consulte Asignación de flujos de estados de las alarmas externas.

Temas

Configuración de un alias de propiedad (consola)

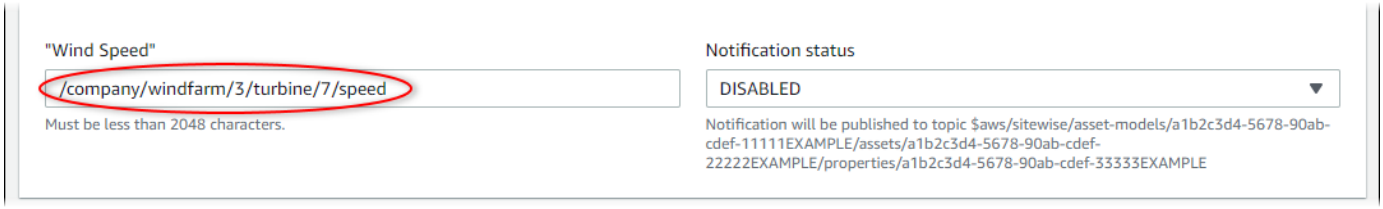
Puede utilizar la AWS IoT SiteWise consola para establecer un alias para la propiedad de un activo.

Para configurar un alias de propiedad (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Activos.
3. Elija el activo para el que desea configurar un alias de propiedad.

   > **Tip**
   >
   > Puede elegir el icono de flecha para expandir una jerarquía de activos y encontrar su activo.

4. Seleccione Editar.
5. Encuentre la propiedad para la que desea configurar un alias y, a continuación, escriba el alias de propiedad.



6. Seleccione Guardar.

Establecer un alias de propiedad (AWS CLI)

Utilice el AWS Command Line Interface (AWS CLI) para establecer un alias para la propiedad de un activo.

Debe conocer los `assetId` de sus activos y los `propertyId` de las propiedades para completar este procedimiento. También puede usar el ID externo. Si has creado un activo y no lo sabes`assetId`, usa la ListAssetsAPI para enumerar todos los activos de un modelo específico. Utilice la DescribeAssetoperación para ver las propiedades de su activo, incluidos los identificadores de propiedad.

Utilice la UpdateAssetPropertyoperación para asignar un flujo de datos a la propiedad de su activo. Especifique los siguientes parámetros:

- `assetId`— El identificador del activo o el identificador externo. Para obtener más información, consulte Hacer referencia a objetos con identificadores externos en la Guía del usuario de AWS IoT SiteWise .
- `propertyId`— El identificador de la propiedad del activo o el identificador externo.
- `propertyAlias`: la ruta del flujo de datos hasta el alias de la propiedad.
- `propertyNotificationState`: el estado de notificación del valor de la propiedad, `ENABLED` o `DISABLED`. Especifique el estado de notificación existente de la propiedad cuando actualice el alias de propiedad. Puede recuperar el estado de notificación existente con la DescribeAssetPropertyoperación.

  Si omite este parámetro, el nuevo estado de notificación será `DISABLED`. Para obtener más información acerca de las notificaciones de propiedades, consulte Interacción con otros AWS servicios.

Para establecer un alias de propiedad (AWS CLI)

1. Ejecute el siguiente comando para recuperar el estado de notificación actual de la propiedad. Reemplace *asset-id* y *property-id* por los ID de la propiedad del activo.

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

   La operación devuelve una respuesta que contiene detalles de la propiedad del activo en el siguiente formato. El estado de notificación de propiedades se encuentra en `assetProperty.notification.state` en el objeto 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. Ejecute el siguiente comando para configurar el alias de la propiedad del activo. Reemplace *property-alias* por el alias de propiedad y *notification-state* por el estado de notificación u omita `--property-notification-state` para desactivar las notificaciones. Si lo desea, puede actualizar la unidad del activo con una nueva *unit* y `--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. Para comprobar que se ha establecido el alias, ejecute el siguiente comando para recuperar los detalles de la propiedad. Reemplace *asset-id* y *property-id* por los ID de la propiedad del activo.

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

La operación devuelve una respuesta que contiene detalles de la propiedad del activo en el siguiente formato. El alias de la propiedad es `assetProperty.alias` en el objeto JSON y está configurada como `myAlias` en este ejemplo.

```
{
  "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": {}
    }
  }
}
```

Actualización de valores de atributos

Los activos heredan los atributos de su modelo de activos, incluido el valor predeterminado del atributo. En algunos casos, querrá conservar el atributo predeterminado del modelo de activos, por ejemplo para una propiedad de fabricante de activos. En otros casos, querrá actualizar el atributo heredado, como para la latitud y la longitud de un activo.

Updating an attribute value (console)

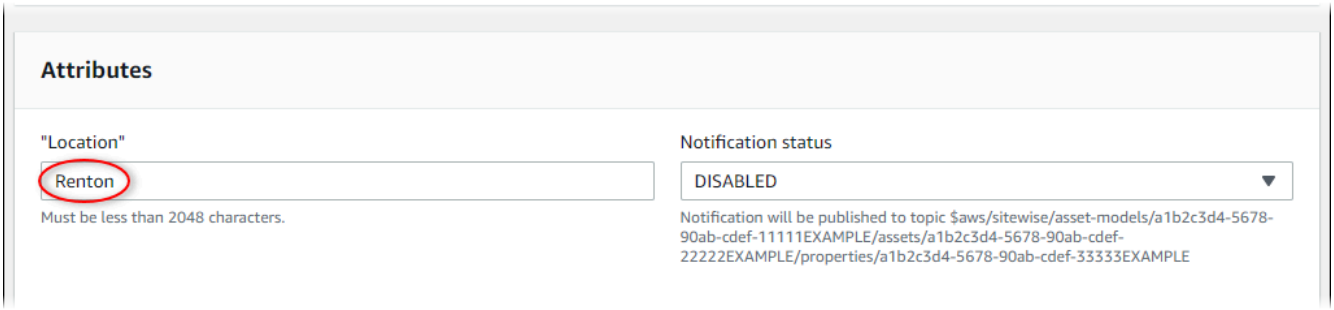
Puede utilizar la AWS IoT SiteWise consola para actualizar el valor de una propiedad de activo de atributo.

Para actualizar el valor de un atributo (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Activos.
3. Elija el activo para el que desea actualizar un atributo.

> **Tip**
>
> Puede elegir el icono de flecha para expandir una jerarquía de activos y encontrar su activo.

4. Seleccione Editar.
5. Encuentre el atributo que desea actualizar y, a continuación, escriba su nuevo valor.



6. Seleccione Guardar.

Updating an attribute value (AWS CLI)

Puedes usar AWS Command Line Interface (AWS CLI) para actualizar el valor de un atributo.

Debe conocer los `assetId` de sus activos y los `propertyId` de las propiedades para completar este procedimiento. También puedes usar el ID externo. Si has creado un activo y no lo sabes`assetId`, usa la ListAssetsAPI para enumerar todos los activos de un modelo específico. Utilice la DescribeAssetoperación para ver las propiedades de su activo, incluidos los identificadores de propiedad.

Utilice la BatchPutAssetPropertyValueoperación para asignar valores de atributos a su activo. Puede utilizar esta operación para establecer varios atributos a la vez. La carga de esta operación contiene una lista de entradas y cada una contiene el ID de activo, el ID de propiedad y el valor de atributo.

Para actualizar el valor de un atributo (AWS CLI)

1. Cree un archivo llamado `batch-put-payload.json` y copie el siguiente objeto JSON en el archivo. En esta carga de ejemplo se muestra cómo establecer la latitud y la longitud de una turbina eólica. Actualice los ID, los valores y las marcas temporales para modificar la carga para su caso de 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
          }
        }
      ]
    }
  ]
}
```

- Cada entrada de la carga contiene un `entryId` que puede definir como una única cadena. Si la entrada de la solicitud no se realiza correctamente, cada error contendrá el `entryId` de la solicitud correspondiente para que sepa qué solicitudes deben volver a intentarse.
- Para establecer un valor de atributo, puede incluir una estructura timestamp-quality-value (TQV) en la lista de propiedades `propertyValues` de cada atributo. Esta estructura debe contener el nuevo `value` y la `timestamp` actual.
  - `value`: una estructura que contiene uno de los siguientes campos, en función del tipo de propiedad que se establezca:
    - `booleanValue`
    - `doubleValue`
    - `integerValue`
    - `stringValue`
  - `timestamp`— Una estructura que contiene el tiempo de época actual de Unix en segundos,. `timeInSeconds` AWS IoT SiteWise rechaza todos los puntos de datos con marcas de tiempo que hayan existido durante más de 7 días o más de 5 minutos en el futuro.

Para obtener más información sobre cómo preparar una carga útil para BatchPutAssetPropertyValue, consulte. Ingerir datos mediante la API AWS IoT SiteWise

2. Ejecute el siguiente comando para enviar los valores de los atributos a AWS IoT SiteWise:

```
aws iotsitewise batch-put-asset-property-value -\-cli-input-json file://batch-
put-payload.json
```

Asociación y disociación de activos

Si el modelo de activos define jerarquías de modelos de activos secundarios, puede asociar activos secundarios al activo. Los activos principales pueden acceder a los datos de los activos asociados y agregarlos. Para obtener más información acerca de los modelos de activos jerárquicos, consulte Definición de jerarquías de modelos de activos.

Temas

Asociación y disociación de activos (consola)

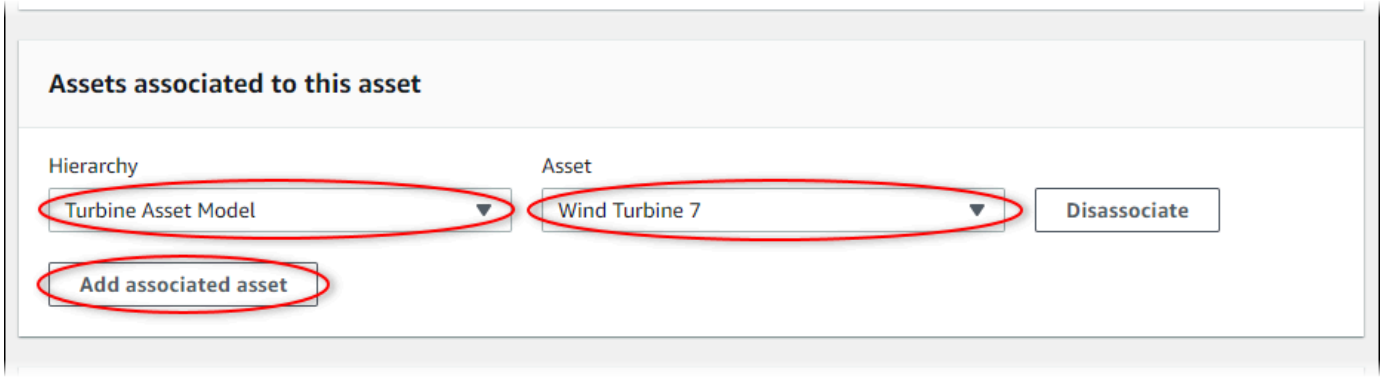
Puede utilizar la AWS IoT SiteWise consola para asociar y desasociar activos.

Para asociar un activo (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Activos.
3. Elija el activo principal con el que desea asociar un activo secundario.

> **Tip**
>
> Puede elegir el icono de flecha para expandir una jerarquía de activos y encontrar su activo.

4. Seleccione Editar.
5. En Activos asociados a este activo, elija Agregar un activo asociado.



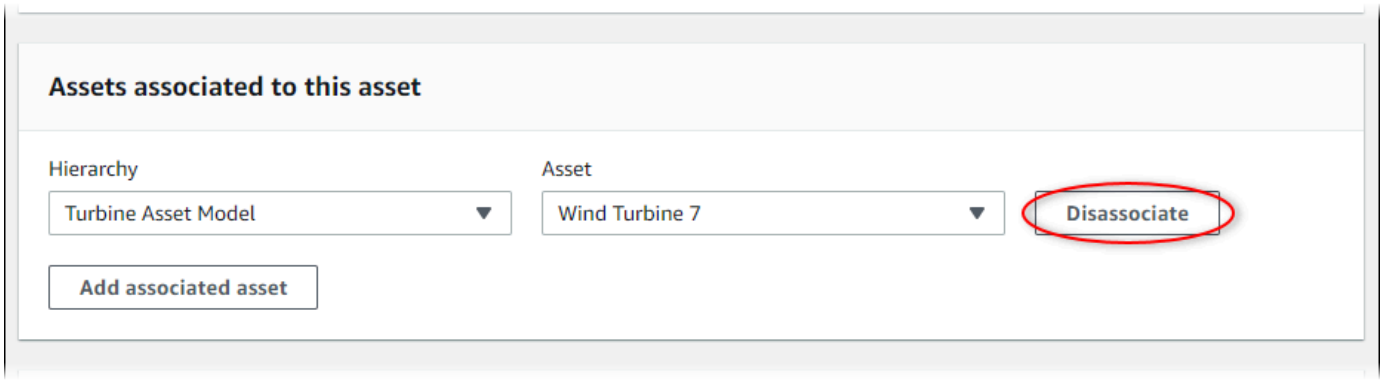
6. En Jerarquía, elija la jerarquía que defina la relación entre el activo principal y el activo secundario.
7. En Activo, elija el activo secundario que desea asociar.
8. Seleccione Guardar.

Para disociar un activo (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Activos.
3. Elija el activo principal para el que desea disociar un activo secundario.

> **Tip**
>
> Puede elegir el icono de flecha para expandir una jerarquía de activos y encontrar su activo.

4. Seleccione Editar.
5. En Activos asociados a este activo, elija Desvincular para el activo.



6. Seleccione Guardar.

Asociar y disociar activos ()AWS CLI

Puede usar AWS Command Line Interface (AWS CLI) para asociar y disociar activos.

Para este procedimiento, debe conocer el ID de la jerarquía (`hierarchyId`) en el modelo de activos principal que define la relación con el modelo de activos secundario. Utilice la DescribeAssetoperación para buscar el identificador de jerarquía en la respuesta.

Para encontrar un ID de jerarquía

- Ejecute el siguiente comando para describir el activo principal. *parent-asset-id*Sustitúyalo por el identificador del activo principal o el identificador externo.

  ```
  aws iotsitewise describe-asset --asset-id parent-asset-id
  ```

  La operación devuelve una respuesta que contiene los detalles del activo. La respuesta contiene una `assetHierarchies` lista que tiene la siguiente estructura:

  ```
  {
    ...
    "assetHierarchies": [
      {
        "id": "String",
        "name": "String"
      }
    ],
    ...
  }
  ```

  El ID de jerarquía es el valor `id` para una jerarquía en la lista de jerarquías de activos.

Después de tener el ID de jerarquía, puede asociar o disociar un activo con esa jerarquía.

Para asociar un activo secundario a un activo principal, utilice la AssociateAssetsoperación. Para desasociar un activo secundario de un activo principal, utilice la DisassociateAssetsoperación. Especifique los siguientes parámetros, que son los mismos para ambas operaciones:

- `assetId`— El identificador del activo principal o el identificador externo.
- `hierarchyId`— El ID de jerarquía o el ID externo del activo principal.
- `childAssetId`— El identificador del activo secundario o el identificador externo.

Para asociar un activo (AWS CLI)

- Ejecute el siguiente comando para asociar un activo secundario con un activo principal. Sustituya *parent-asset-id*el *identificador de jerarquía* y por *child-asset-id*los identificadores correspondientes:

```
aws iotsitewise associate-assets \
  --asset-id parent-asset-id \
  --hierarchy-id hierarchy-id \
  --child-asset-id child-asset-id
```

Para desasociar un activo ()AWS CLI

- Ejecute el siguiente comando para disociar un activo secundario de un activo principal. Sustituya *parent-asset-id*el *identificador de jerarquía* y por los *child-asset-id*identificadores correspondientes:

```
aws iotsitewise disassociate-assets \
  --asset-id parent-asset-id \
  --hierarchy-id hierarchy-id \
  --child-asset-id child-asset-id
```

Actualizar activos y modelos

Puede actualizar sus activos, modelos de activos y modelos de componentes AWS IoT SiteWise para modificar sus nombres y definiciones. Estas operaciones de actualización son asíncronas y tardan un tiempo en propagarse. AWS IoT SiteWise Compruebe el estado del activo o modelo antes de realizar cambios adicionales. Debe esperar hasta que se propaguen los cambios para poder seguir utilizando el activo o modelo actualizado.

Temas

- Actualización de activos
- Actualización de los modelos de activos y los modelos de componentes
- Actualización de modelos compuestos personalizados (componentes)

Actualización de activos

Puede usar la AWS IoT SiteWise consola o la API para actualizar el nombre de un activo.

Cuando se actualiza un activo, el estado del activo es `UPDATING` hasta que se propagan los cambios. Para obtener más información, consulte Estados de activos y modelos.

Temas

Actualización de un activo (consola)

Puede usar la AWS IoT SiteWise consola para actualizar los detalles del activo.

Para actualizar un activo (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Activos.
3. Elija el activo que desea actualizar.

   > **Tip**
   >
   > Puede elegir el icono de flecha para expandir una jerarquía de activos y encontrar su activo.

4. Seleccione Editar.
5. Actualice el Nombredel activo.
6. (Opcional) En esta página, actualice otra información para el activo. Para más información, consulte los siguientes temas:

   - Asignación de flujos de datos industriales a propiedades de activos
   - Actualización de valores de atributos
   - Interacción con otros AWS servicios
7. Seleccione Guardar.

Actualizar un activo (AWS CLI)

Puedes usar AWS Command Line Interface (AWS CLI) para actualizar el nombre de un activo.

Utilice la UpdateAssetoperación para actualizar un activo. Especifique los siguientes parámetros:

- `assetId`: el ID del activo. Este es el ID real en formato UUID, o `externalId:myExternalId` si lo tiene. Para obtener más información, consulte Hacer referencia a objetos con identificadores externos en la Guía del usuario de AWS IoT SiteWise .
- `assetName`: el nuevo nombre del activo.

Para actualizar el nombre de un activo ()AWS CLI

- Ejecute el siguiente comando para actualizar el nombre de un activo. *Sustituya el identificador* del activo por el identificador o el identificador externo del activo. Actualice el *nombre del activo por el nuevo nombre* del activo.

```
aws iotsitewise update-asset \
  --asset-id asset-id \
  --asset-name asset-name
```

Actualización de los modelos de activos y los modelos de componentes

Puede utilizar la AWS IoT SiteWise consola o la API para actualizar un modelo de activos o un modelo de componentes.

No puede cambiar el tipo o el tipo de datos de una propiedad existente ni la ventana de una métrica existente. Tampoco puede cambiar el tipo de modelo de un modelo de activos a un modelo de componentes o al revés.

> **Important**
>
> - Si elimina una propiedad de un modelo de activos o de un modelo de componentes, AWS IoT SiteWise elimina todos los datos anteriores de esa propiedad. En el caso de los modelos de componentes, esto afecta a todos los modelos de activos que utilizan ese modelo de componentes, por lo que debe tener especial cuidado de comprender hasta qué punto puede aplicarse el cambio.
> - Si elimina una definición de jerarquía de un modelo de activos, AWS IoT SiteWise disocia todos los activos de esa jerarquía.

Al actualizar un modelo de activos, todos los activos basados en ese modelo reflejan los cambios que realice en el modelo subyacente. Hasta que los cambios se propaguen, cada activo tiene el estado `UPDATING`. Debe esperar hasta que esos activos vuelvan al estado `ACTIVE` antes de interactuar con ellos. Durante este tiempo, el estado del modelo de activos actualizado será `PROPAGATING`.

Al actualizar un modelo de componentes, todos los modelos de activos que incorporan ese modelo de componentes reflejan los cambios. Hasta que los cambios en el modelo de componentes se propaguen, cada modelo de activo afectado tiene el `UPDATING` estado y, a continuación, sus activos asociados, tal y como se describe en el párrafo anterior. `PROPAGATING` Debe esperar a que esos modelos de activos vuelvan a su `ACTIVE` estado antes de interactuar con ellos. Durante este tiempo, el estado del modelo de componentes actualizado será`PROPAGATING`.

Para obtener más información, consulte Estados de activos y modelos.

Temas

- Actualización de un modelo de activo o componente (consola)
- Actualización de un modelo de activo o componente (AWS CLI)

Actualización de un modelo de activo o componente (consola)

Puede utilizar la AWS IoT SiteWise consola para actualizar un modelo de activos o un modelo de componentes.

Para actualizar un modelo de activos o un modelo de componentes (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Models (Modelos).
3. Elija el modelo de activos o el modelo de componentes que desee actualizar.
4. Elija Editar.
5. En la página Editar el modelo, realice alguna de las siguientes acciones:
    - En Detalles del modelo, cambie el Nombre del modelo.
    - Cambie cualquiera de las Definiciones de atributos. No se puede cambiar el Tipo de datos de los atributos existentes. Para obtener más información, consulte Definición de datos estáticos (atributos).

- Cambie cualquiera de las Definiciones de mediciones. No se puede cambiar el Tipo de datos de las mediciones existentes. Para obtener más información, consulte Definición de flujos de datos procedentes del equipo (mediciones).
- Cambie cualquiera de las Definiciones de transformación. Para obtener más información, consulte Transformación de datos (transformaciones).
- Cambie cualquiera de las Definiciones de métricas. No se puede cambiar el Intervalo de tiempo de las métricas existentes. Para obtener más información, consulte Agregación de datos de propiedades y otros activos (métricas).
- (Solo modelos de activos) Cambie cualquiera de las definiciones de la jerarquía. No se puede cambiar el Modelo de jerarquía de las jerarquías existentes. Para obtener más información, consulte Definición de jerarquías de modelos de activos.

6. Seleccione Save (Guardar).

Actualización de un modelo de activo o componente (AWS CLI)

Puede usar el AWS Command Line Interface (AWS CLI) para actualizar un modelo de activos o un modelo de componentes.

Utilice la UpdateAssetModelAPI para actualizar el nombre, la descripción y las propiedades de un modelo de activos o un modelo de componentes. Solo en el caso de los modelos de activos, puede actualizar las jerarquías. Especifique los siguientes parámetros:

- `assetModelId`: el ID del activo. Este es el ID real en formato UUID, o `externalId:myExternalId` si lo tiene. Para obtener más información, consulte Hacer referencia a objetos con identificadores externos en la Guía del usuario de AWS IoT SiteWise .

Especifique el modelo actualizado en la carga útil. Para obtener más información sobre el formato esperado de un modelo de activos o un modelo de componentes, consulteCreación de modelos de activos.

> **Warning**
>
> La UpdateAssetModelAPI sobrescribe el modelo existente con el modelo que usted proporciona en la carga útil. Para evitar eliminar las propiedades o jerarquías del modelo, debes incluir sus ID y definiciones en la carga útil del modelo actualizado. Para

obtener información sobre cómo consultar la estructura existente del modelo, consulte la DescribeAssetModeloperación.

> **Note**
>
> El siguiente procedimiento solo puede actualizar modelos compuestos de este tipo`AWS/ALARM`. Si desea actualizar los modelos `CUSTOM` compuestos, utilice UpdateAssetModelCompositeModelen su lugar. Para obtener más información, consulte Actualización de modelos compuestos personalizados (componentes).

Para actualizar un modelo de activos o un modelo de componentes (AWS CLI)

1. Ejecute el siguiente comando para recuperar la definición del modelo existente. *`asset-model-id`*Sustitúyalo por el ID o el ID externo del modelo de activos o del modelo de componentes que desee actualizar.

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

   La operación devuelve una respuesta que contiene los detalles del modelo. La respuesta tiene la siguiente estructura.

   ```
   {
     "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"
  }
}
```

Para obtener más información, consulte la DescribeAssetModeloperación.

2. Cree un archivo llamado `update-asset-model.json` y copie la respuesta del comando anterior en el archivo.
3. Elimine los siguientes pares de clave-valor del objeto JSON en `update-asset-model.json`:

   - `assetModelId`
   - `assetModelArn`
   - `assetModelCompositeModelSummaries`
   - `assetModelCreationDate`
   - `assetModelLastUpdateDate`
   - `assetModelStatus`
   - `assetModelType`

   La UpdateAssetModeloperación espera una carga útil con la siguiente estructura:

```
{
  "assetModelName": "String",
  "assetModelDescription": "String",
  "assetModelProperties": Array of AssetModelProperty,
  "assetModelHierarchies": Array of AssetModelHierarchyDefinition,
  "assetModelCompositeModels": Array of AssetModelCompositeModel
}
```

4. En `update-asset-model.json`, realice una de las siguientes acciones:

   - Cambie el nombre del modelo de activos (`assetModelName`).
   - Cambie, agregue o elimine la descripción del modelo de activos (`assetModelDescription`).
   - Cambie, agregue o elimine cualquiera de las propiedades del modelo de activos (`assetModelProperties`). No puede cambiar `dataType` de las propiedades existentes ni `window` de las métricas existentes. Para obtener más información, consulte Definición de las propiedades de datos.

- Cambie, agregue o elimine cualquiera de las jerarquías del modelo de activos (`assetModelHierarchies`). No puede cambiar `childAssetModelId` de las jerarquías existentes. Para obtener más información, consulte Definición de jerarquías de modelos de activos.
- Cambie, añada o elimine cualquiera de los modelos compuestos de tipo `AWS/ALARM` (`assetModelCompositeModels`) del modelo de activos. Las alarmas monitorean otras propiedades para que pueda identificar cuándo requieren atención los equipos o procesos. Cada definición de alarma es un modelo compuesto que estandariza el conjunto de propiedades que utiliza la alarma. Para obtener más información, consulte Monitoreo de datos con alarmas y Definición de alarmas en los modelos de activos.

5. Ejecute el siguiente comando para actualizar el modelo de activos con la definición almacenada en `update-asset-model.json`. *`asset-model-id`*Sustitúyalo por el ID del modelo de activos:

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

Actualización de modelos compuestos personalizados (componentes)

Puede utilizar la AWS IoT SiteWise API para actualizar un modelo compuesto personalizado o la AWS IoT SiteWise consola para actualizar los componentes.

Temas

- Actualización de un componente (consola)
- Actualización de un modelo compuesto personalizado (AWS CLI)

Actualización de un componente (consola)

Puede utilizar la AWS IoT SiteWise consola para actualizar un componente.

Para actualizar un componente (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Models (Modelos).
3. Elija el modelo de activo en el que se encuentra el componente.

4. En la pestaña Propiedades, elija Componentes.
5. Elija el componente que desee actualizar.
6. Elija Editar.
7. En la página Editar componente, realice una de las siguientes acciones:
   - En Detalles del modelo, cambie el Nombre del modelo.
   - Cambie cualquiera de las Definiciones de atributos. No se puede cambiar el Tipo de datos de los atributos existentes. Para obtener más información, consulte Definición de datos estáticos (atributos).
   - Cambie cualquiera de las Definiciones de mediciones. No se puede cambiar el Tipo de datos de las mediciones existentes. Para obtener más información, consulte Definición de flujos de datos procedentes del equipo (mediciones).
   - Cambie cualquiera de las Definiciones de transformación. Para obtener más información, consulte Transformación de datos (transformaciones).
   - Cambie cualquiera de las Definiciones de métricas. No se puede cambiar el Intervalo de tiempo de las métricas existentes. Para obtener más información, consulte Agregación de datos de propiedades y otros activos (métricas).
8. Seleccione Save (Guardar).

Actualización de un modelo compuesto personalizado (AWS CLI)

Puede utilizar el AWS Command Line Interface (AWS CLI) para actualizar un modelo compuesto personalizado.

Para actualizar el nombre o la descripción, utilice la UpdateAssetModelCompositeModeloperación. Solo en el caso de los modelos compuestos personalizados en línea, también puede actualizar las propiedades. No puede actualizar las propiedades de un modelo compuesto component-model-based personalizado, ya que el modelo de componentes al que se hace referencia proporciona las propiedades asociadas.

> **Important**
>
> Si elimina una propiedad de un modelo compuesto personalizado, AWS IoT SiteWise elimina todos los datos anteriores de esa propiedad. No puede cambiar el tipo o el tipo de datos de una propiedad existente.
> Para reemplazar una propiedad de modelo compuesto existente por una nueva con la misma propiedad`name`, haga lo siguiente:

1. Envíe una `UpdateAssetModelCompositeModel` solicitud eliminando toda la propiedad existente.
2. Envía una segunda `UpdateAssetModelCompositeModel` solicitud que incluya la nueva propiedad. El nuevo activo será el `name` mismo que el anterior y AWS IoT SiteWise generará un nuevo activo único`id`.

Para actualizar un modelo compuesto personalizado (AWS CLI)

1. Para recuperar la definición del modelo compuesto existente, ejecute el siguiente comando. *`composite-model-id`*Sustitúyalo por el ID o el ID externo del modelo compuesto personalizado que se va a actualizar y *`asset-model-id`*por el modelo de activos al que está asociado el modelo compuesto personalizado. Para obtener más información, consulte AWS IoT SiteWise en la Guía del usuario de .

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

   Para obtener más información, consulte la DescribeAssetModelCompositeModeloperación.
2. Cree un archivo denominado yu`pdate-custom-composite-model.json`, a continuación, copie la respuesta del comando anterior en el archivo.
3. Elimine todos los pares clave-valor del objeto JSONu`pdate-custom-composite-model.json`, excepto los siguientes campos:
   - `assetModelCompositeModelName`
   - `assetModelCompositeModelDescription`(si está presente)
   - `assetModelCompositeModelProperties`(si está presente)
4. En `update-custom-composite-model.json`, realice una de las siguientes acciones:
   - Cambie el valor de`assetModelCompositeModelName`.
   - Añada`assetModelCompositeModelDescription`, elimine o cambie su valor.
   - Solo para modelos compuestos personalizados en línea: cambie, añada o elimine cualquiera de las propiedades del modelo de activos en`assetModelCompositeModelProperties`.

Para obtener más información sobre el formato necesario para este archivo, consulte la sintaxis de solicitud de. UpdateAssetModelCompositeModel

5. Ejecute el siguiente comando para actualizar el modelo compuesto personalizado con la definición almacenada enupdate-custom-composite-model.json. *composite-model-id*Sustitúyalo por el ID del modelo compuesto y *asset-model-id*por el ID del modelo de activos en el que se encuentra.

```
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
```

Eliminación de activos y modelos

Puede eliminar sus activos y modelos a partir del AWS IoT SiteWise momento en que haya terminado de usarlos. Las operaciones de borrado son asíncronas y tardan un tiempo en propagarse. AWS IoT SiteWise

Temas

- Eliminación de activos
- Eliminación de modelos de activos

Eliminación de activos

Puede usar la AWS IoT SiteWise consola o la API para eliminar un activo.

Antes de poder eliminar un activo, primero debe disociar sus activos secundarios y disociarlos de su activo principal. Para obtener más información, consulte Asociación y disociación de activos. Si usas el AWS Command Line Interface (AWS CLI), puedes usar la ListAssociatedAssetsoperación para enumerar los elementos secundarios de un activo.

Cuando se elimina un activo, su estado es `DELETING` hasta que se propagan los cambios. Para obtener más información, consulte Estados de activos y modelos. Después de eliminar el activo, no puede consultar ese activo. Si lo hace, la API devuelve una respuesta HTTP 404.

> **Important**
>
> AWS IoT SiteWise elimina todos los datos de propiedad de los activos eliminados.

Temas

Eliminación de un activo (consola)

Puede utilizar la AWS IoT SiteWise consola para eliminar un activo.

Para eliminar un activo (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Activos.
3. Elija el activo que desea eliminar.

   > **Tip**
   >
   > Puede elegir el icono de flecha para expandir una jerarquía de activos y encontrar su activo.

4. Si el activo tiene Activos asociados, elimine cada activo. Puede elegir el nombre de un activo para navegar hasta su página, donde puede eliminarlo.
5. En la página del activo, elija Eliminar.
6. En el cuadro de diálogo Eliminar activo, haga lo siguiente:

   a. Escriba **`Delete`** para confirmar la eliminación.

   b. Elija Eliminar.

Eliminar un activo (AWS CLI)

Puede usar AWS Command Line Interface (AWS CLI) para eliminar un activo.

Utilice la DeleteAssetoperación para eliminar un activo. Especifique el siguiente parámetro:

- `assetId`: el ID del activo. Este es el ID real en formato UUID, o `externalId:myExternalId` si lo tiene. Para obtener más información, consulte Hacer referencia a objetos con identificadores externos en la Guía del usuario de AWS IoT SiteWise .

Para eliminar un activo ()AWS CLI

1. Ejecute el siguiente comando para mostrar las jerarquías del activo. Sustituya el *asset-id* por el ID o el ID externo del activo:

   ```
   aws iotsitewise describe-asset --asset-id asset-id
   ```

   La operación devuelve una respuesta que contiene los detalles del activo. La respuesta contiene una `assetHierarchies` lista que tiene la siguiente estructura:

   ```
   {
     ...
     "assetHierarchies": [
       {
         "id": "String",
         "name": "String"
       }
     ],
     ...
   }
   ```

   Para obtener más información, consulte la DescribeAssetoperación.

2. Para cada jerarquía, ejecute el siguiente comando para mostrar los secundarios del activo que están asociados con esa jerarquía. *Sustituya el identificador* de activo por el identificador o el identificador externo del activo y el identificador de *jerarquía por el identificador* o identificador externo de la jerarquía.

   ```
   aws iotsitewise list-associated-assets \
     --asset-id asset-id \
     --hierarchy-id hierarchy-id
   ```

   Para obtener más información, consulte la operación. ListAssociatedAssets

3. Ejecute el siguiente comando para eliminar cada activo asociado y, a continuación, para eliminar el activo. Sustituya el *asset-id* por el ID o el ID externo del activo.

```
aws iotsitewise delete-asset --asset-id asset-id
```

Eliminación de modelos de activos

Puede utilizar la AWS IoT SiteWise consola o la API para eliminar un modelo de activos.

Para poder eliminar un modelo de activos, primero debe eliminar todos los activos que se crearon a partir del modelo de activos.

Cuando se elimina un modelo de activos, su estado es `DELETING` hasta que se propagan los cambios. Para obtener más información, consulte Estados de activos y modelos. Una vez eliminado el modelo de activos, no se puede consultar ese modelo de activos. Si lo hace, la API devuelve una respuesta HTTP 404.

Temas

- Eliminación de un modelo de activos (consola)
- Eliminar un modelo de activo (AWS CLI)

Eliminación de un modelo de activos (consola)

Puede utilizar la AWS IoT SiteWise consola para eliminar un modelo de activos.

Para eliminar un modelo de activos (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Models (Modelos).
3. Elija el modelo de activos que desea eliminar.
4. Si el modelo tiene Activos, elimine cada activo. Elija el nombre de un activo para navegar hasta su página, donde puede eliminarlo. Para obtener más información, consulte Eliminación de un activo (consola).
5. En la página del modelo, elija Eliminar.
6. En el cuadro de diálogo Eliminar modelo, haga lo siguiente:
   a. Escriba **`Delete`** para confirmar la eliminación.
   b. Elija Eliminar.

Eliminar un modelo de activo (AWS CLI)

Puede usar AWS Command Line Interface (AWS CLI) para eliminar un modelo de activos.

Utilice la DeleteAssetModeloperación para eliminar un modelo de activos. Especifique el siguiente parámetro:

- `assetModelId`: el ID del activo. Este es el ID real en formato UUID, o `externalId:myExternalId` si lo tiene. Para obtener más información, consulte Hacer referencia a objetos con identificadores externos en la Guía del usuario de AWS IoT SiteWise .

Para eliminar un modelo de activos ()AWS CLI

1. Ejecute el siguiente comando para mostrar todos los activos creados a partir del modelo. *`asset-model-id`*Sustitúyalo por el ID o el ID externo del modelo de activos.

   ```
   aws iotsitewise list-assets --asset-model-id asset-model-id
   ```

   Para obtener más información, consulte la ListAssetsoperación.
2. Si el comando anterior devuelve activos del modelo, elimine cada activo. Para obtener más información, consulte Eliminar un activo (AWS CLI).
3. Ejecute el siguiente comando para eliminar el modelo de activos. *`asset-model-id`*Sustitúyalo por el ID o el ID externo del modelo de activos.

   ```
   aws iotsitewise delete-asset-model --asset-model-id asset-model-id
   ```

Operaciones masivas con activos y modelos

Para trabajar con una gran cantidad de activos o modelos de activos, utilice las operaciones masivas para importar y exportar recursos de forma masiva a una ubicación diferente. Por ejemplo, puede crear un archivo de datos que defina los activos o modelos de activos en un bucket de Amazon S3 y utilizar la importación masiva para crearlos o actualizarlos AWS IoT SiteWise. Como alternativa, si tiene una gran cantidad de activos o modelos de activos AWS IoT SiteWise, puede exportarlos a Amazon S3.

> **Note**
>
> Las operaciones masivas se realizan AWS IoT SiteWise mediante llamadas a las operaciones de la AWS IoT TwinMaker API. Puede hacerlo sin configurar AWS IoT TwinMaker ni crear un AWS IoT TwinMaker espacio de trabajo. Todo lo que necesita es un depósito de Amazon S3 en el que pueda colocar su AWS IoT SiteWise contenido.

Temas

Conceptos y terminología clave

AWS IoT SiteWise Las funciones de importación y exportación masivas se basan en los siguientes conceptos y terminología:

- Importación: acción de mover activos o modelos de activos de un archivo de un bucket de Amazon S3 a AWS IoT SiteWise.
- Exportación: acción de mover activos o modelos de activos desde AWS IoT SiteWise un bucket de Amazon S3.
- Origen: la ubicación inicial desde la que desea mover el contenido.

  Por ejemplo, un bucket de Amazon S3 es una fuente de importación y AWS IoT SiteWise una fuente de exportación.
- Destino: la ubicación deseada a la que quieres mover el contenido.

Por ejemplo, un bucket de Amazon S3 es un destino de exportación y AWS IoT SiteWise un destino de importación.

- AWS IoT SiteWise Esquema: este esquema se utiliza para importar y exportar metadatos desde AWS IoT SiteWise.
- Recurso de nivel superior: un AWS IoT SiteWise recurso que puede crear o actualizar de forma individual, como un activo o un modelo de activos.
- Subrecurso: recurso anidado dentro de un AWS IoT SiteWise recurso de nivel superior. Los ejemplos incluyen propiedades, jerarquías y modelos compuestos.
- Metadatos: información clave necesaria para importar o exportar los recursos correctamente. Algunos ejemplos de metadatos son las definiciones de activos y los modelos de activos.
- metadataTransferJob: el objeto que se crea al ejecutar`CreateMetadataTransferJob`.

Funcionalidades compatibles

En este tema se explica lo que puede hacer cuando ejecuta una operación masiva. Las operaciones masivas admiten las siguientes funciones:

- Creación de recursos de nivel superior: al importar un activo o un modelo de activo que no define un identificador o cuyo identificador no coincide con el de uno existente, se creará como un recurso nuevo.
- Reemplazo de recursos de nivel superior: cuando importas un activo o un modelo de activo cuyo ID coincide con uno que ya existe, reemplazará el recurso existente.
- Creación, reemplazo o eliminación de subrecursos: cuando la importación reemplaza un recurso de nivel superior, como un activo o un modelo de activos, la nueva definición reemplaza a todos los subrecursos, como las propiedades, las jerarquías o los modelos compuestos.

  Por ejemplo, si actualizas un modelo de activos durante una importación masiva y la versión actualizada define una propiedad que no estaba presente en la versión original, se crea una nueva propiedad. Si define una propiedad que ya existe, se actualizará la propiedad existente. Si el modelo de activos actualizado omite una propiedad que estaba presente en el original, se elimina la propiedad.
- Sin eliminación de recursos de nivel superior: las operaciones masivas no eliminan un activo o un modelo de activos. Las operaciones masivas solo las crean o actualizan.

Requisitos previos para las operaciones masivas

En esta sección se explican los requisitos previos para las operaciones masivas, incluidos los permisos AWS Identity and Access Management (de IAM) para intercambiar recursos entre la máquina local y la máquina local. Servicios de AWS Antes de iniciar una operación masiva, complete el siguiente requisito previo:

- Cree un bucket de Amazon S3 para almacenar los recursos. Para obtener más información sobre el uso de Amazon S3, consulte ¿Qué es Amazon S3?

Permisos de IAM

Para realizar operaciones masivas, debe crear una política AWS Identity and Access Management (IAM) con permisos que permitan el intercambio de AWS recursos entre Amazon S3 y su máquina local. AWS IoT SiteWise Para obtener más información acerca de la creación de políticas de IAM, consulte Crear políticas de IAM.

Para realizar operaciones masivas, necesita las siguientes políticas.

AWS IoT SiteWise política

Esta política permite el acceso a las acciones de la AWS IoT SiteWise API necesarias para las operaciones masivas:

```
{
    "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 política

Esta política permite el acceso a las operaciones de la AWS IoT TwinMaker API que se utilizan para trabajar con operaciones masivas:

```
{
    "Sid": "MetadataTransferJobApiAccess",
    "Effect": "Allow",
    "Action": [
        "iottwinmaker:CreateMetadataTransferJob",
        "iottwinmaker:CancelMetadataTransferJob",
        "iottwinmaker:GetMetadataTransferJob",
        "iottwinmaker:ListMetadataTransferJobs"
    ],
    "Resource": "*"
}
```

Política de Amazon S3

Esta política proporciona acceso a los depósitos de Amazon S3 para transferir metadatos para operaciones masivas.

For a specific Amazon S3 bucket

Si utiliza un depósito específico para trabajar con los metadatos de sus operaciones masivas, esta política le proporciona acceso a ese depósito:

```
{
    "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

Si vas a utilizar muchos depósitos diferentes para trabajar con los metadatos de tus operaciones masivas, esta política te da acceso a cualquier depósito:

```
{
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:AbortMultipartUpload",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
    ],
    "Resource": "*"
}
```

Para obtener información sobre cómo solucionar problemas en las operaciones de importación y exportación, consulteSolución de problemas de importación y exportación masivas.

Ejecutar un trabajo de importación masiva

La importación masiva es la acción de mover los metadatos a un AWS IoT SiteWise espacio de trabajo. Por ejemplo, la importación masiva puede mover los metadatos de un archivo local o de un archivo de un bucket de Amazon S3 a un AWS IoT SiteWise espacio de trabajo.

Paso 1: Prepare el archivo para importarlo

Descargue el archivo de formato AWS IoT SiteWise nativo para importar los activos y los modelos de activos. Consulte AWS IoT SiteWise esquema de trabajo de transferencia de metadatos para obtener más detalles.

Paso 2: Cargue el archivo preparado en Amazon S3

Cargue el archivo en Amazon S3. Consulte Carga de un archivo a Amazon S3 en la Guía del usuario de Amazon Simple Storage Service para obtener más información.

Importar metadatos (consola)

Puede utilizarla Consola de AWS IoT SiteWise para importar metadatos de forma masiva. Siga Paso 1: Prepare el archivo para importarlo y Paso 2: Cargue el archivo preparado en Amazon S3 prepare un archivo que esté listo para ser importado.

Importación de datos de Amazon S3 a Consola de AWS IoT SiteWise

1. Vaya a la consola de AWS IoT SiteWise.
2. Seleccione Operaciones masivas nuevas en el panel de navegación.
3. Seleccione Nueva importación para iniciar el proceso de importación.
4. En la página Importar metadatos:
   - Seleccione Browse Amazon S3 para ver el bucket y los archivos de Amazon S3.
   - Navegue hasta el depósito de Amazon S3 que contiene el archivo de importación preparado.
   - Seleccione el archivo que desee importar.
   - Revisa el archivo seleccionado y selecciona Importar.
5. La página Operaciones masivas en SiteWise metadatos del Consola de AWS IoT SiteWise muestra el trabajo de importación recién creado en la tabla de progreso de los trabajos.

Importar metadatos (AWS CLI)

Para realizar una acción de importación, utilice el siguiente procedimiento:

Importación de datos de Amazon S3 a AWS CLI

1. Cree un archivo de metadatos que especifique los recursos que desea importar, siguiendo lasAWS IoT SiteWise esquema de trabajo de transferencia de metadatos. Guarde este archivo en su bucket de Amazon S3.

   Para ver ejemplos de archivos de metadatos para importar, consulteEjemplos de metadatos de importación.

2. Ahora cree un archivo JSON con el cuerpo de la solicitud. El cuerpo de la solicitud especifica el origen y el destino del trabajo de transferencia. Este archivo es independiente del archivo del paso anterior. Asegúrese de especificar su bucket de Amazon S3 como origen y `iotsitewise` como destino.

   El siguiente ejemplo muestra el cuerpo de la solicitud:

   ```
   {
         "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. `CreateMetadataTransferJob`Para invocarlo, ejecute el siguiente AWS CLI comando. En este ejemplo, se nombra `createMetadataTransferJobExport.json` el archivo del cuerpo de la solicitud del paso anterior.

   ```
   aws iottwinmaker create-metadata-transfer-job --region us-east-1 \
     --cli-input-json file://createMetadataTransferJobImport.json
   ```

Esto creará un trabajo de transferencia de metadatos e iniciará el proceso de transferencia de los recursos seleccionados.

Ejecutar un trabajo de exportación masiva

La exportación masiva es la acción de mover los metadatos de un AWS IoT SiteWise espacio de trabajo a un bucket de Amazon S3.

Al realizar una exportación masiva de su AWS IoT SiteWise contenido a Amazon S3, puede especificar filtros para limitar los modelos de activos y activos específicos que desea exportar.

Los filtros deben especificarse en una `iotSiteWiseConfiguration` sección dentro de la sección de fuentes de su solicitud de JSON.

> **Note**
>
> Puedes incluir varios filtros en tu solicitud. La operación masiva exportará los modelos de activos y los activos que coincidan con cualquiera de los filtros.
> Si no proporciona ningún filtro, la operación masiva exporta todos sus modelos y activos de activos.

Example cuerpo de la solicitud con filtros

```
{
      "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"
         }
      }
}
```

Exportación de metadatos (consola)

El siguiente procedimiento explica la acción de exportación de la consola:

Cree un trabajo de exportación en el Consola de AWS IoT SiteWise

1. Vaya a la consola de AWS IoT SiteWise.
2. Seleccione Operaciones masivas nuevas en el panel de navegación.
3. Seleccione Nueva exportación para iniciar el proceso de exportación.
4. En la página Exportar metadatos:

   - Introduzca un nombre para el trabajo de exportación. Este es el nombre que se utiliza para el archivo exportado en su bucket de Amazon S3.
   - Elija los recursos que desea exportar, lo que establece los filtros para el trabajo:
     - Exporte todos los activos y modelos de activos. Utilice filtros en los activos y los modelos de activos.
     - Exporte activos. Filtra tus activos.
       - Seleccione el activo que desee utilizar para el filtro de exportación.

        - (Opcional) Añada el modelo de activos derivado o asociado.
      - Exporte modelos de activos. Filtre sus modelos de activos.
        - Seleccione el modelo de activos que desee utilizar para el filtro de exportación.
        - (Opcional) Añada la descendencia, el activo asociado o ambos.
      - Elija Siguiente.
    - Navegue hasta el bucket de Amazon S3:
      - Seleccione Browse Amazon S3 para ver el bucket y los archivos de Amazon S3.
      - Navegue hasta el depósito de Amazon S3 donde debe colocarse el archivo.
      - Elija Siguiente.
    - Revise el trabajo de exportación y seleccione Exportar.
5. La página Operaciones masivas en SiteWise metadatos Consola de AWS IoT SiteWise muestra el trabajo de importación recién creado en la tabla de progreso de los trabajos.

Para conocer las diferentes formas de utilizar los filtros al exportar metadatos, consulteEjemplos de metadatos de exportación.

Exportar metadatos (AWS CLI)

El siguiente procedimiento explica la acción AWS CLI de exportación:

Exportación de datos desde AWS IoT SiteWise Amazon S3

1. Cree un archivo JSON con el cuerpo de la solicitud. El cuerpo de la solicitud especifica el origen y el destino del trabajo de transferencia. En el siguiente ejemplo se muestra un ejemplo del cuerpo de la solicitud:

```
{
    "metadataTransferJobId": "your-transfer-job-Id",
    "sources": [{
        "type": "iotsitewise"
    }],
    "destination": {
        "type": "s3",
        "s3Configuration": {
            "location": "arn:aws:s3:::your-S3-bucket-location"
        }
```

```
    }
}
```

Asegúrese de especificar su bucket de Amazon S3 como destino del trabajo de transferencia de metadatos.

> **Note**
>
> En este ejemplo, se exportarán todos sus modelos y activos de activos. Para limitar la exportación a modelos o activos específicos, puede incluir filtros en el cuerpo de la solicitud. Para obtener más información sobre la aplicación de filtros de exportación, consulteEjemplos de metadatos de exportación.

2. Guarde el cuerpo de la solicitud para usarlo en el siguiente paso. En este ejemplo, el archivo se denomina `createMetadataTransferJobExport.json`.
3. `CreateMetadataTransferJob`Para invocarlo, ejecute el siguiente AWS CLI comando:

```
aws iottwinmaker create-metadata-transfer-job --region us-east-1 \
        --cli-input-json file://createMetadataTransferJobExport.json
```

Sustituya el archivo `createMetadataTransferJobExport.json` JSON de entrada por su propio nombre de archivo de transferencia.

Seguimiento del progreso de los trabajos y gestión de errores

El procesamiento de un trabajo de proceso masivo lleva tiempo. Cada trabajo se procesa en el orden en que se AWS IoT SiteWise recibió la solicitud. Se procesa one-at-a-time para cada cuenta. Cuando se completa un trabajo, el siguiente en la cola comienza a procesarse automáticamente. AWS IoT SiteWise resuelve los trabajos de forma asíncrona y actualiza el estado de cada uno a medida que avanza. Cada trabajo tiene un campo de estado que contiene el estado del recurso y un mensaje de error, si corresponde.

El estado puede ser uno de los siguientes valores:

- `VALIDATING`— Validar el trabajo, incluido el formato de archivo enviado y su contenido.
- `PENDING`— El trabajo está en cola. Puede cancelar los trabajos en este estado desde la AWS IoT SiteWise consola, pero todos los demás estados continuarán hasta el final.

- `RUNNING`— Procesando el trabajo. Consiste en crear y actualizar los recursos según lo definido en el archivo de importación, o en exportar los recursos en función de los filtros de trabajo de exportación elegidos. Si se cancela, no se eliminará ningún recurso importado por este trabajo. Para obtener más información, consulte Revise el progreso y los detalles del trabajo (consola).
- `CANCELLING`— El trabajo se está cancelando activamente.
- `ERROR`— No se pudieron procesar uno o más recursos. Consulte el informe de trabajo detallado para obtener más información. Para obtener más información, consulte Inspeccione los detalles del error (consola).
- `COMPLETED`— Job realizado sin errores.
- `CANCELLED`— El trabajo está cancelado y no está en cola. Si ha cancelado un `RUNNING` trabajo, los recursos que ya había importado este trabajo en el momento de la cancelación no se eliminarán de AWS IoT SiteWiseél.

Temas

- Seguimiento del progreso de los trabajos
- Inspeccione los errores

Seguimiento del progreso de los trabajos

Revise el progreso y los detalles del trabajo (consola)

Consulte Importar metadatos (consola) o Exportación de metadatos (consola) para iniciar un trabajo masivo.

Descripción general del progreso del trabajo en la AWS IoT SiteWise consola:

1. Vaya a la consola de AWS IoT SiteWise.
2. Seleccione Operaciones masivas nuevas en el panel de navegación.
3. La tabla de progreso de los trabajos de la AWS IoT SiteWise consola muestra la lista de trabajos de operaciones masivas.
4. La columna Tipo de trabajo describe si se trata de un trabajo de exportación o importación. Las columnas Fecha de importación muestran la fecha en que se inició el trabajo.
5. La columna Estado muestra el estado del trabajo. Puede seleccionar un trabajo para ver los detalles del trabajo.

6. El trabajo seleccionado muestra el éxito si se ha realizado correctamente o una lista de los errores si el trabajo ha fallado. También se muestra una descripción del error con cada tipo de recurso.

Descripción general de los detalles del trabajo en la AWS IoT SiteWise consola:

La tabla de progreso de los trabajos de la AWS IoT SiteWise consola muestra la lista de trabajos de operaciones masivas.

1. Elija un trabajo para ver más detalles.
2. En el caso de un trabajo de importación, `Data source ARN` representa la ubicación en Amazon S3 del archivo de importación.
3. En el caso de un trabajo de exportación, `Data destination ARN` representa la ubicación del archivo en Amazon S3 tras la exportación.
4. Las `Status` y `Status reason` proporcionan detalles adicionales sobre el trabajo actual. Consulte Seguimiento del progreso de los trabajos y gestión de errores para obtener más detalles.
5. El `Queued position` representa la posición del trabajo en la cola de procesos. Los trabajos se procesan de uno en uno. Una posición en cola igual a 1 indica que el trabajo se procesará a continuación.
6. La página de detalles de los trabajos también muestra los recuentos de progreso del trabajo.
    - Los tipos de recuento del progreso del trabajo son:
        i. `Total resources`— Indica el recuento total de activos en el proceso de transferencia.
        ii. `Succeeded`— Indica el recuento de activos transferidos correctamente durante el proceso.
        iii. `Failed`— Indica el recuento de activos que fallaron durante el proceso.
        iv. `Skipped`— Indica el recuento de activos que se omitieron durante el proceso.
7. Un estado de trabajo igual `PENDING` – o`VALIDATING`, muestra todos los recuentos de progreso de los trabajos. Esto indica que se están evaluando los recuentos de progreso de los trabajos.
8. Un estado de trabajo de `RUNNING` muestra el `Total resources` recuento, el trabajo enviado para su procesamiento. Los recuentos detallados (`Succeeded``Failed`, y`Skipped`) se aplican

a los recursos procesados. La suma de los recuentos detallados es menor que el `Total resources` recuento, hasta que el estado del trabajo sea `COMPLETED` o`ERROR`.

9. Si el estado de un trabajo es `COMPLETED` o`ERROR`, el `Total resources` recuento es igual a la suma de los recuentos detallados (`Succeeded`+`Failed`, y`Skipped`).
10. Si el estado de un trabajo es`ERROR`, consulte la tabla de fallos de trabajo para obtener detalles sobre los errores y fallos específicos. Consulte Inspeccione los detalles del error (consola) para obtener más detalles.

Revise el progreso y los detalles del trabajo (AWS CLI)

Tras iniciar una operación masiva, puedes comprobar o actualizar su estado mediante las siguientes acciones de la API:

- Para recuperar información sobre un trabajo específico, usa la acción de la GetMetadataTransferJobAPI.

  Recupera información con la **`GetMetadataTransferJob`** API:

  1. Crea y ejecuta un trabajo de transferencia. Llame a la API de `GetMetadataTransferJob`.

     Example AWS CLI comando:

     ```
     aws iottwinmaker get-metadata-transfer-job \
             --metadata-transfer-job-id your_metadata_transfer_job_id \
             --region your_region
     ```

  2. La `GetMetadataTransferJob` API devuelve un `MetadataTransferJobProgress` objeto con los siguientes parámetros:
     - SucceededCount: indica el recuento de activos transferidos correctamente en el proceso.
     - FailedCount: indica el recuento de activos que fallaron durante el proceso.
     - SkippedCount: indica el recuento de activos que se omitieron durante el proceso.
     - TotalCount: indica el recuento total de activos en el proceso de transferencia.

     Estos parámetros indican el estado del progreso del trabajo. Si el estado es`RUNNING`, ayudan a rastrear la cantidad de recursos que aún no se han procesado.

Si encuentra errores de validación del esquema o si failedCount es mayor o igual a 1, el estado de progreso del trabajo pasa a ser. ERROR Se incluye un informe de errores completo del trabajo en su bucket de Amazon S3. Consulte Inspeccione los errores para obtener más detalles.

- Para enumerar los trabajos actuales, usa la acción ListMetadataTransferJobsde la API.

  Usa un archivo JSON para filtrar los trabajos devueltos en función de su estado actual. Consulte el siguiente procedimiento:

  1. Para especificar los filtros que desea usar, cree un archivo JSON AWS CLI de entrada. Desea usar:

     ```
     {
         "sourceType": "s3",
         "destinationType": "iottwinmaker",
         "filters": [{
             "state": "COMPLETED"
         }]
     }
     ```

     Para obtener una lista de `state` valores válidos, consulta la Guía ListMetadataTransferJobsFilterde referencia de la AWS IoT TwinMaker API.

  2. Usa el archivo JSON como argumento en el siguiente comando de AWS CLI ejemplo:

     ```
     aws iottwinmaker list-metadata-transfer-job --region your_region \
             --cli-input-json file://ListMetadataTransferJobsExample.json
     ```

- Para cancelar un trabajo, usa la acción de la CancelMetadataTransferJobAPI. Esta API cancela el trabajo de transferencia de metadatos específico sin que ello afecte a los recursos ya exportados o importados:

  ```
  aws iottwinmaker cancel-metadata-transfer-job \
          --region your_region \
          --metadata-transfer-job-id job-to-cancel-id
  ```

Inspeccione los errores

Inspeccione los detalles del error (consola)

Detalles del error en la AWS IoT SiteWise consola:

1. Vaya a la consola de AWS IoT SiteWise.
2. Consulte la tabla de progreso de los trabajos Consola de AWS IoT SiteWise para ver una lista de los trabajos de operaciones masivas.
3. Seleccione un trabajo para ver los detalles del trabajo.
4. Si el estado de un trabajo es `COMPLETED` o`ERROR`, el `Total resources` recuento es igual a la suma de los recuentos detallados (`Succeeded`+`Failed`, y`Skipped`).
5. Si el estado de un trabajo es`ERROR`, consulte la tabla de fallos de trabajo para obtener detalles sobre los errores y fallos específicos.
6. La tabla de errores de trabajo muestra el contenido del informe de trabajo. El `Resource type` campo indica la ubicación del error o los fallos, como los siguientes:

   - Por ejemplo, un error de validación `Bulk operations template` en el `Resource type` campo indica que la plantilla de importación y el formato del archivo del esquema de metadatos no coinciden. Para obtener más información, consulte AWS IoT SiteWise esquema de trabajo de transferencia de metadatos.
   - Un error `Asset` en el `Resource type` campo indica que el activo no se ha creado debido a un conflicto con otro activo. Consulte Errores comunes para obtener información sobre los errores y conflictos de AWS IoT SiteWise recursos.

Inspeccione los detalles del error (AWS CLI)

Para gestionar y diagnosticar los errores producidos durante un trabajo de transferencia, consulta el siguiente procedimiento sobre el uso de la acción de la `GetMetadataTransferJob` API:

1. Tras crear y ejecutar un trabajo de transferencia, llama a GetMetadataTransferJob:

   ```
   aws iottwinmaker get-metadata-transfer-job \
           --metadata-transfer-job-id your_metadata_transfer_job_id \
           --region us-east-1
   ```

2. Una vez que veas en qué estado se encuentra el trabajo`COMPLETED`, puedes empezar a verificar los resultados del trabajo.

3. Cuando llamasGetMetadataTransferJob, devuelve un objeto llamado MetadataTransferJobProgress.

   El MetadataTransferJobProgress objeto contiene los siguientes parámetros:

   - FailedCount: indica el recuento de activos que fallaron durante el proceso de transferencia.
   - Recuento omitido: indica el recuento de activos que se omitieron durante el proceso de transferencia.
   - Recuento exitoso: indica el recuento de activos que se realizaron correctamente durante el proceso de transferencia.
   - Recuento total: indica el recuento total de activos involucrados en el proceso de transferencia.
4. Además, la llamada a la API devuelve un elemento `reportUrl` que contiene una URL prefirmada. Si tu trabajo de transferencia tiene algún problema que necesites investigar más a fondo, visita esta URL.

Ejemplos de metadatos de importación

En esta sección se muestra cómo crear archivos de metadatos para importar modelos y activos con una sola operación de importación masiva.

Ejemplo de importación masiva

Puede importar muchos modelos de activos y activos con una sola operación de importación masiva. El siguiente ejemplo muestra cómo crear un archivo de metadatos para ello.

En este escenario de ejemplo, tiene varios sitios de trabajo que contienen robots industriales en celdas de trabajo.

El ejemplo define dos modelos de activos:

- `RobotModel1`: Este modelo de activos representa un tipo concreto de robot que tiene en sus lugares de trabajo. El robot tiene una propiedad de medición,`Temperature`.
- `WorkCell`: Este modelo de activos representa un conjunto de robots dentro de uno de sus sitios de trabajo. El modelo de activos define una jerarquía para representar la relación entre una célula de trabajo y los robots. `robotHierarchyOEM1`

El ejemplo también define algunos activos:

- `WorkCell1`: una célula de trabajo dentro de su sede de Boston
- `RobotArm123456`: un robot dentro de esa celda de trabajo
- `RobotArm987654`: otro robot dentro de esa celda de trabajo

El siguiente archivo de metadatos JSON define estos modelos y activos de activos. Al realizar una importación masiva con estos metadatos, se crean los modelos de activos y los activos que contienen AWS IoT SiteWise, incluidas sus relaciones jerárquicas.

Archivo de metadatos para importar

```
{
    "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"
                }
            ]
        }
    ]
}
```

Ejemplo de incorporación inicial de modelos y activos

En este escenario de ejemplo, tiene varios sitios de trabajo que contienen robots industriales en una empresa.

El ejemplo define varios modelos de activos:

- `Sample_Enterprise`— Este modelo de activos representa a la empresa de la que forman parte los sitios. El modelo de activos define una jerarquía`Enterprise to Site`,, para representar la relación de los sitios con la empresa.

- `Sample_Site`— Este modelo de activos representa las plantas de fabricación de la empresa. El modelo de activos define una jerarquía`Site to Line`,, para representar la relación de las líneas con el sitio.
- `Sample_Welding Line`— Este modelo de activos representa una línea de ensamblaje dentro de los sitios de trabajo. El modelo de activos define una jerarquía para representar la relación de los robots con la línea. `Line to Robot`
- `Sample_Welding Robot`— Este modelo de activos representa un tipo particular de robot en sus lugares de trabajo.

El ejemplo también define los activos en función de los modelos de activos.

- `Sample_AnyCompany Motor`— Este activo se crea a partir del modelo de `Sample_Enterprise` activos.
- `Sample_Chicago`— Este activo se crea a partir del modelo de `Sample_Site` activos.
- `Sample_Welding Line 1`— Este activo se crea a partir del modelo de `Sample_Welding Line` activos.
- `Sample_Welding Robot 1`— Este activo se crea a partir del modelo de `Sample_Welding Robot` activos.
- `Sample_Welding Robot 2`— Este activo se crea a partir del modelo de `Sample_Welding Robot` activos.

El siguiente archivo de metadatos JSON define estos modelos y activos de activos. Al realizar una importación masiva con estos metadatos, se crean los modelos de activos y los activos que contienen AWS IoT SiteWise, incluidas sus relaciones jerárquicas.

Archivo JSON para incorporar activos y modelos para su importación

```
{
    "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": {
```

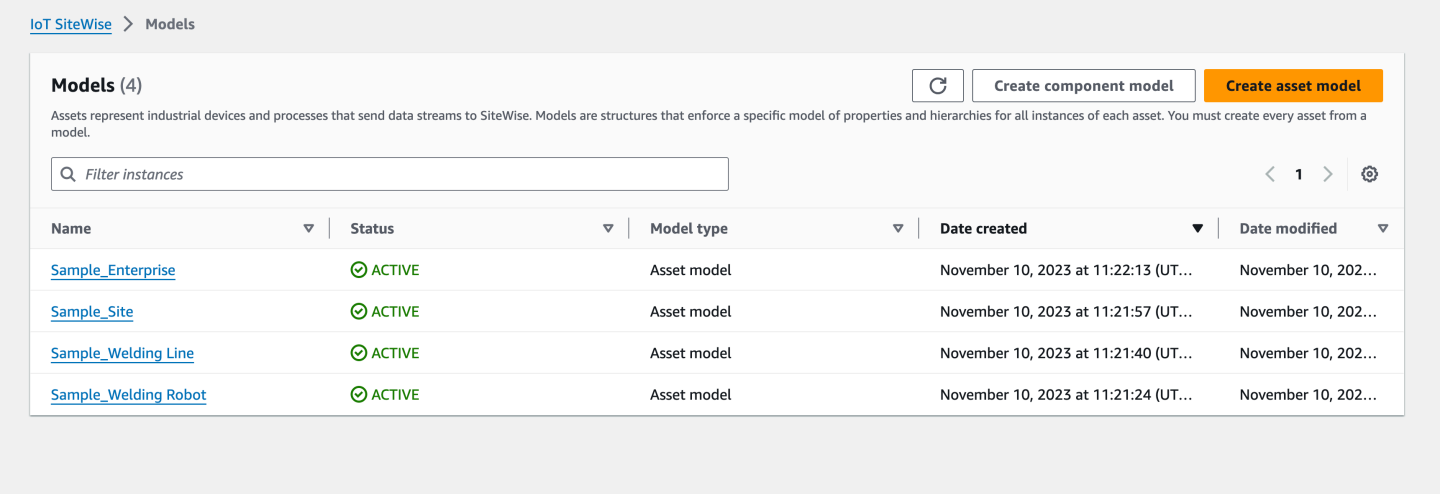
```
                                "interval": "5m"
                            }
                        }
                    }
                },
                "unit": "Amps"
            }
        ]
    },
    {
        "assetModelExternalId": "External_Id_Welding_Line",
        "assetModelName": "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",
```

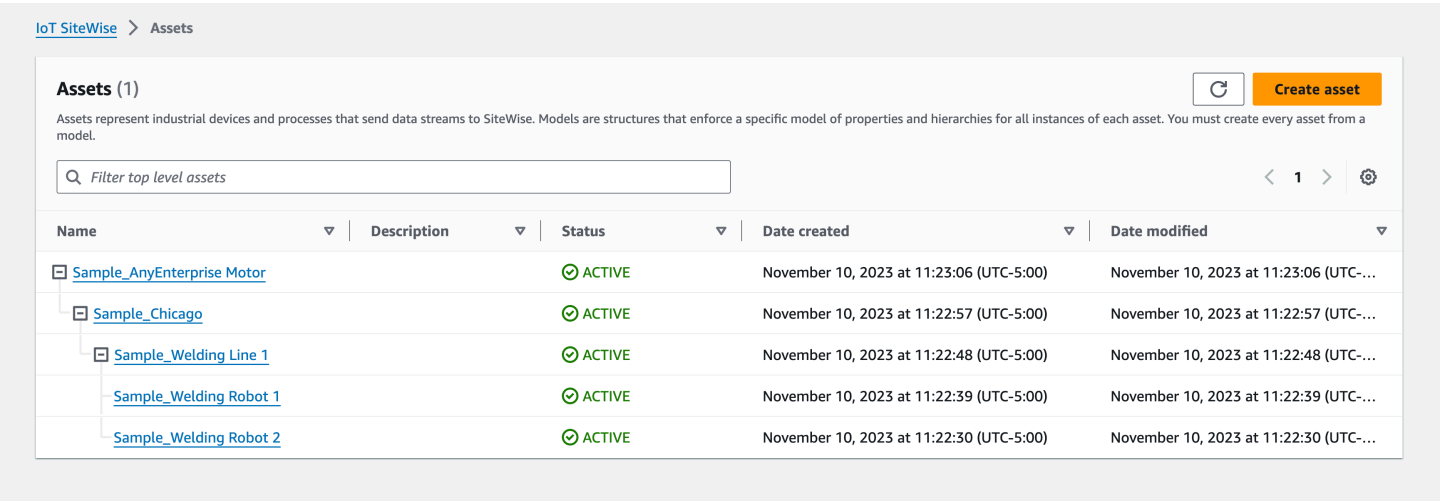
```
                    "attributeValue": "S1000"
                },
                {
                    "externalId": "External_Id_Welding_Robot_Cycle_Count",
                    "alias": "AnyCompany/Chicago/Welding Line/S1000/Count"
                },
                {
                    "externalId": "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 siguiente captura de pantalla muestra los modelos que aparecen Consola de AWS IoT SiteWise después de ejecutar el ejemplo de código anterior.



La siguiente captura de pantalla muestra los modelos, activos y jerarquías que se muestran Consola de AWS IoT SiteWise después de ejecutar el ejemplo de código anterior.



Ejemplo de incorporación de activos adicionales

En este ejemplo, se definen activos adicionales para importarlos a un modelo de activos existente en su cuenta:

- `Sample_Welding Line 2`— Este activo se crea a partir del modelo de `Sample_Welding Line` activos.
- `Sample_Welding Robot 3`— Este activo se crea a partir del modelo de `Sample_Welding Robot` activos.
- `Sample_Welding Robot 4`— Este activo se crea a partir del modelo de `Sample_Welding Robot` activos.

Para crear los activos iniciales de este ejemplo, consulte[Ejemplo de incorporación inicial de modelos y activos](#).

El siguiente archivo de metadatos JSON define estos modelos y activos de activos. Al realizar una importación masiva con estos metadatos, se crean los modelos de activos y los activos que contienen AWS IoT SiteWise, incluidas sus relaciones jerárquicas.

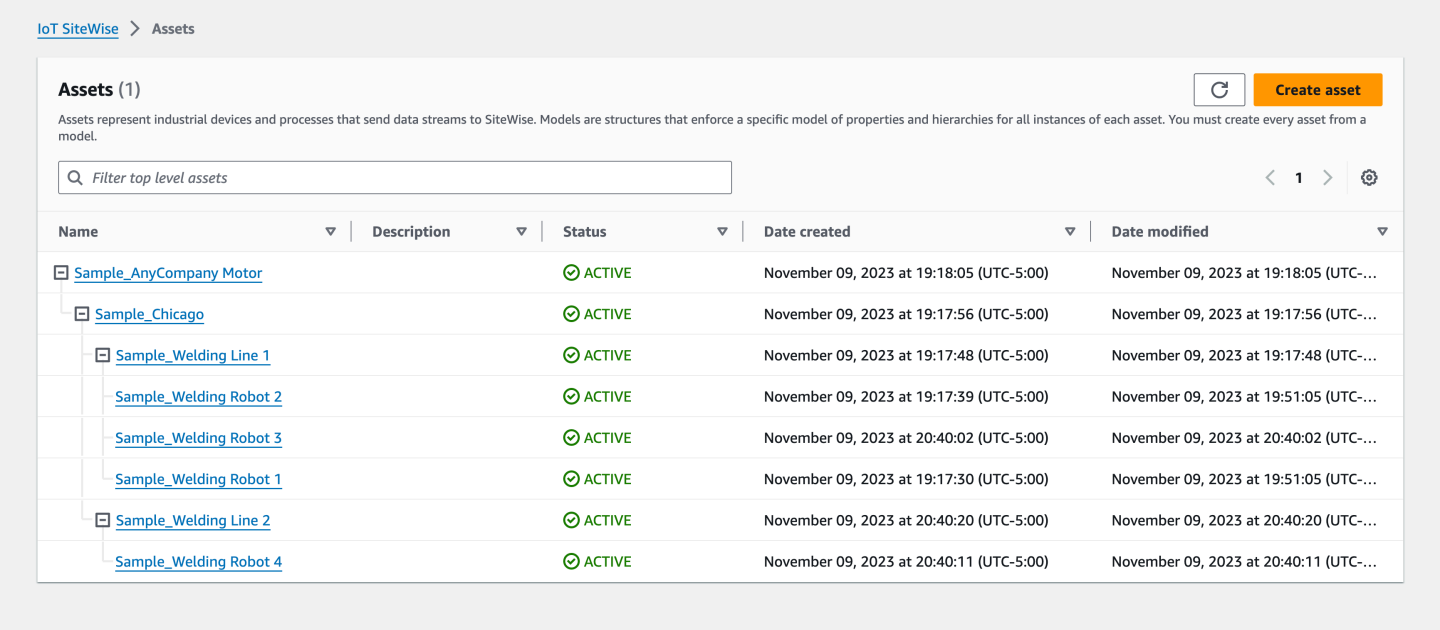
Archivo JSON para incorporar activos adicionales

```
{
    "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 siguiente captura de pantalla muestra los modelos, activos y jerarquías que se muestran Consola de AWS IoT SiteWise después de ejecutar el ejemplo de código anterior.



Ejemplo de incorporación de nuevas propiedades

En este ejemplo, se definen nuevas propiedades en los modelos de activos existentes. Consulte Ejemplo de incorporación de activos adicionales para incorporar activos y modelos adicionales.

- `Joint 1 Temperature`— Esta propiedad se añade al modelo `Sample_Welding Robot` de activos. Esta nueva propiedad también se propagará a cada activo creado a partir del modelo de `Sample_Welding Robot` activos.

Para añadir una nueva propiedad a un modelo de activos existente, consulte el siguiente ejemplo de archivo de metadatos JSON. Como se muestra en el JSON, se debe proporcionar la definición

completa del modelo de `Sample_Welding Robot` activos existente junto con la nueva propiedad. Si no se proporciona la lista completa de propiedades de la definición existente, AWS IoT SiteWise elimina las propiedades omitidas.

Archivo JSON para incorporar nuevas propiedades

En este ejemplo, se añade una nueva propiedad `Joint 1 Temperature` al modelo de activos.

```
{
    "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"
                }
            ]
        }
    ]
}
```

Ejemplos de metadatos de exportación

Al realizar una exportación masiva de su AWS IoT SiteWise contenido a Amazon S3, puede especificar filtros para limitar los modelos de activos y activos específicos que desea exportar.

Los filtros se especifican en una `iotSiteWiseConfiguration` sección dentro de la `sources` sección del cuerpo de la solicitud.

> **Note**
>
> Puede incluir varios filtros. La operación masiva exportará cualquier modelo de activo o activo que coincida con alguno de los filtros.
> Si no proporciona ningún filtro, la operación exportará todos sus modelos y activos de activos.

```
{
    "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"
        }
    }
}
```

Filtrar por modelo de activos

Puede filtrar un modelo de activo específico. También puede incluir todos los activos que utilizan ese modelo o todos los modelos de activos dentro de su jerarquía. No puede incluir tanto los activos como la jerarquía.

Para obtener más información acerca de las jerarquías, consulte Definición de jerarquías de modelos de activos.

Asset model

Este filtro incluye el modelo de activos especificado:

```
"filterByAssetModel": {
    "assetModelId": "asset model ID"
}
```

Asset model and its assets

Este filtro incluye el modelo de activos especificado, junto con todos los activos que utilizan ese modelo de activos:

```
"filterByAssetModel": {
    "assetModelId": "asset model ID",
    "includeAssets": true
}
```

Asset model and its hierarchy

Este filtro incluye el modelo de activos especificado, junto con todos los modelos de activos asociados en su jerarquía:

```
"filterByAssetModel": {
    "assetModelId": "asset model ID",
    "includeOffspring": true
}
```

Filtrado por activo

Puede filtrar un activo específico. También puede incluir su modelo de activos o todos los activos asociados dentro de su jerarquía. No puede incluir tanto el modelo de activos como la jerarquía.

Para obtener más información acerca de las jerarquías, consulte Definición de jerarquías de modelos de activos.

Asset

Este filtro incluye el activo especificado:

```
"filterByAsset": {
    "assetId": "asset ID"
}
```

Asset and its asset model

Este filtro incluye el activo especificado, junto con el modelo de activo que utiliza:

```
"filterByAsset": {
    "assetId": "asset ID",
    "includeAssetModel": true
}
```

Asset and its hierarchy

Este filtro incluye el activo especificado, junto con todos los activos asociados en su jerarquía:

```
"filterByAsset": {
    "assetId": "asset ID",
    "includeOffspring": true
}
```

AWS IoT SiteWise esquema de trabajo de transferencia de metadatos

Utilice el esquema de tareas de transferencia de AWS IoT SiteWise metadatos como referencia cuando realice sus propias operaciones de importación y exportación masivas:

```
{
  "$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"
      }
    }
  }
}
```

Monitoreo de datos con alarmas

Puede configurar alarmas para que sus datos le alerten a usted y a sus colaboradores cuando su equipo o los procesos no funcionen de manera óptima. Un rendimiento óptimo de una máquina o de un proceso significa que los valores de determinadas métricas deben estar dentro de un rango de límites altos y bajos. Cuando estas métricas están fuera de su rango de operación, se debe notificar a los operadores de los equipos para que solucionen el problema. Use alarmas para identificar rápidamente los problemas y notificar a los operadores para que maximicen el rendimiento del equipo y de los procesos.

Temas

Tipos de Alarmas

Puede definir las alarmas que se detectan en la AWS nube y las que se detectan con procesos externos. AWS IoT SiteWise admite los siguientes tipos de alarmas:

- AWS IoT Events alarmas

  AWS IoT Events las alarmas son alarmas que AWS IoT Events detectan AWS IoT SiteWise envía los valores de las propiedades de los activos a un modelo de alarma en AWS IoT Events. A continuación, AWS IoT Events envía el estado de alarma a AWS IoT SiteWise. Puede configurar opciones, como cuándo detecta algo la alarma y a quién notificar cuando cambie el estado de alarma. También puede definir las acciones de AWS IoT Events que se deben producirse cuando cambie el estado de alarma.

  Las alarmas AWS IoT Events son instancias de modelos de alarma. El modelo de alarma especifica el umbral y la gravedad de la alarma, qué hacer cuando cambie el estado de alarma

y más. Al configurar cada característica del modelo de alarma, se especifica una propiedad de atributo a partir del modelo de activo que monitorea la alarma. Todos los activos basados en el modelo de activos utilizan el valor del atributo al AWS IoT Events evaluar esa característica de la alarma. Para obtener más información, consulte Uso de alarmas en la Guía para desarrolladores de AWS IoT Events .

Puede responder a una AWS IoT Events alarma cuando cambia de estado. Por ejemplo, puede reconocer o posponer una alarma cuando se activa. También puede habilitar, deshabilitar y restablecer las alarmas.

SiteWise Los usuarios de Monitor pueden visualizar, configurar y responder a AWS IoT Events las alarmas en los portales de SiteWise Monitor. Para obtener más información, consulte Supervisión con alarmas en la Guía de la aplicación AWS IoT SiteWise Monitor .

> **Note**
>
> AWS IoT Events se aplican cargos para evaluar estas alarmas y transferir datos entre AWS IoT SiteWise y AWS IoT Events. Para más información, consulte Precios de AWS IoT Events.

- Alarmas externas

  Las alarmas externas son alarmas que se evalúan fuera de ellas AWS IoT SiteWise. Utilice alarmas externas si tiene un origen de datos que notifique estados de alarma. La alarma externa contiene una propiedad de medición a la que se ingieren los datos del estado de alarma.

  No se puede reconocer ni posponer una alarma externa cuando cambia de estado.

  SiteWise Los usuarios de Monitor pueden ver el estado de las alarmas externas en los portales de SiteWise Monitor, pero no pueden configurarlas ni responder a ellas.

  AWS IoT SiteWise no evalúa el estado de las alarmas externas.

Estados de alarma

Las alarmas industriales incluyen información sobre el estado del equipo o proceso que monitorean, e información (opcional) sobre la respuesta del operador al estado de alarma.

Al definir una AWS IoT Events alarma, se especifica si se habilita o no el flujo de confirmación. El flujo de reconocimiento está habilitado de forma predeterminada. Al habilitar esta opción, los operadores pueden reconocer la alarma y dejar una nota con detalles sobre la alarma o las acciones que han tomado para solucionarla. Si un operador no confirma una alarma activa antes de que se inactive, la alarma se queda bloqueada. El estado bloqueado indica que la alarma se ha activado pero no se ha confirmado, por lo que el operador debe comprobar el equipo o el proceso y reconocer la alarma bloqueada.

Las alarmas tienen los siguientes estados:

- Normal (`Normal`): la alarma está habilitada pero inactiva. El proceso o equipo industrial funciona según lo esperado.
- Activa (`Active`): la alarma está activa. El proceso o equipo industrial está fuera de su rango de operación y requiere atención.
- Confirmado (`Acknowledged`): un operador ha confirmado el estado de la alarma.

  Este estado solo se aplica a las alarmas en las que se habilita el flujo de reconocimiento.
- Bloqueado (`Latched`): la alarma ha vuelto a la normalidad, pero estaba activa y ningún operador la ha confirmado. El proceso o equipo industrial requiere la atención de un operador para restablecer la alarma a su estado normal.

  Este estado solo se aplica a las alarmas en las que se habilita el flujo de reconocimiento.
- Silenciado (`SnoozeDisabled`): la alarma está desactivada porque un operador la ha pospuesto. El operador define el tiempo durante el que se pospone la alarma. Transcurrido ese tiempo, la alarma vuelve al estado normal.
- Deshabilitada (`Disabled`): la alarma está deshabilitada y no es capaz de detectar nada.

Propiedades del estado de alarma

AWS IoT SiteWise almacena los datos del estado de la alarma como un objeto JSON serializado en una cadena. Este objeto contiene el estado e información adicional sobre la alarma, como las acciones de respuesta del operador y la regla que evalúa la alarma.

La propiedad del estado de alarma se identifica por su nombre y tipo de estructura, `AWS/ALARM_STATE`. Para obtener más información, consulte Definición de alarmas en los modelos de activos.

El objeto datos de estado de la alarma contiene la siguiente información:

`stateName`

El estado de la alarma. Para obtener más información, consulte Estados de alarma.

Tipo de datos: `STRING`

`customerAction`

(opcional) objeto que contiene información sobre la respuesta de un operador a la alarma. Los operadores pueden habilitar, deshabilitar, confirmar y posponer las alarmas. Cuando lo hacen, los datos del estado de alarma incluyen su respuesta y la nota que pueden dejar al responder. Este objeto contiene la siguiente información:

`actionName`

El nombre de la acción que realiza el operador para responder a la alarma. Este valor contiene uno de los siguientes strings:

- `ENABLE`
- `DISABLE`
- `SNOOZE`
- `ACKNOWLEDGE`
- `RESET`

Tipo de datos: `STRING`

`enable`

(opcional) objeto que está presente en `customerAction` cuando el operador habilita la alarma. Cuando un operador habilita la alarma, el estado de alarma cambia a `Normal`. Este objeto contiene la siguiente información:

`note`

(opcional) la nota que deja el cliente cuando habilita la alarma.

Tipo de datos: `STRING`

Longitud máxima: 128 caracteres

`disable`

(opcional) objeto que está presente en `customerAction` cuando el operador deshabilita la alarma. Cuando un operador habilita la alarma, el estado de alarma cambia a `Disabled`. Este objeto contiene la siguiente información:

`note`

(opcional) la nota que deja el cliente cuando deshabilita la alarma.

Tipo de datos: `STRING`

Longitud máxima: 128 caracteres

`acknowledge`

(opcional) objeto que está presente en `customerAction` cuando el operador confirma la alarma. Cuando un operador habilita la alarma, el estado de alarma cambia a `Acknowledged`. Este objeto contiene la siguiente información:

`note`

(opcional) la nota que deja el cliente cuando confirma la alarma.

Tipo de datos: `STRING`

Longitud máxima: 128 caracteres

`snooze`

(opcional) objeto que está presente en `customerAction` cuando el operador pospone la alarma. Cuando un operador habilita la alarma, el estado de alarma cambia a `SnoozeDisabled`. Este objeto contiene la siguiente información:

`snoozeDuration`

El tiempo en segundos durante el que el operador pospone la alarma. La alarma cambia al estado `Normal` pasado este tiempo.

Tipo de datos: `INTEGER`

`note`

(opcional) la nota que deja el cliente al posponer la alarma.

Tipo de datos: `STRING`

Longitud máxima: 128 caracteres

`ruleEvaluation`

(opcional) objeto que contiene información sobre la regla que evalúa la alarma. Este objeto contiene la siguiente información:

`simpleRule`

objeto que contiene información acerca de una regla simple, que compara el valor de la propiedad frente a un valor de umbral con un operador de comparación. Este objeto contiene la siguiente información:

`inputProperty`

El valor de la propiedad que evalúa esta alarma.

Tipo de datos: `DOUBLE`

`operator`

El operador de comparación que utiliza esta alarma para comparar la propiedad con el umbral. Este valor contiene uno de los siguientes strings:

- <: menor que
- <=: menor que o igual a
- ==: igual
- !=: distinto de
- >=: mayor que o igual a
- >: mayor que

Tipo de datos: `STRING`

`threshold`

El valor de umbral frente al que esta alarma compara el valor de la propiedad.

Tipo de datos: `DOUBLE`

Definición de alarmas en los modelos de activos

Los modelos de activos impulsan la normalización de sus datos y alarmas industriales. Puede establecer definiciones de alarmas en los modelos de activos, para estandarizar las alarmas de todos los activos basados en un modelo de activo.

Puede utilizar modelos de activos compuestos para definir alarmas en este modelo de activos. Los modelos de activos compuestos son modelos de activos que estandarizan un conjunto específico de propiedades en otro modelo de activo. Los modelos de activos compuestos garantizan la inclusión de determinadas propiedades en un modelo de activo. Las alarmas tienen propiedades de tipo, estado y origen (opcional), por lo que el modelo compuesto de alarmas exige que existan estas propiedades.

Cada modelo de activo compuesto tiene un tipo que define las propiedades que admite el modelo compuesto. Los modelos compuestos de alarmas definen las propiedades de tipo de alarma, estado de alarma y origen de alarma (opcional). Al crear un activo a partir de un modelo de activo con modelos compuestos, el activo incluye las propiedades del modelo compuesto junto con las propiedades que especifique en el modelo de activo.

Cada propiedad de un modelo compuesto debe tener el nombre que la identifique para su tipo de modelo compuesto. Las propiedades del modelo compuesto admiten propiedades con tipos de datos complejos. Estas propiedades tienen el tipo de datos `STRUCT` y una característica `dataTypeSpec` que especifica el tipo de datos complejo de la propiedad. Las propiedades de los tipos de datos complejos contienen datos JSON serializados en cadenas.

Los modelos compuestos de alarmas tienen las siguientes propiedades. Cada propiedad debe tener el nombre que la identifique para su tipo de modelo compuesto.

Tipo de alarma

El tipo de alarma. Especifique uno de los siguientes valores:

- `IOT_EVENTS`— Una AWS IoT Events alarma. AWS IoT SiteWise envía datos AWS IoT Events para evaluar el estado de esta alarma. Debe especificar la propiedad de la fuente de la alarma para definir el modelo de AWS IoT Events alarma para esta definición de alarma.
- `EXTERNAL`: una alarma externa. El estado de la alarma se ingiere en forma de medida.

Nombre de la propiedad: `AWS/ALARM_TYPE`

Tipo de propiedad: atributo

Tipo de datos: `STRING`

Estado de alarma

Los datos de serie temporal del estado de la alarma. Se trata de un objeto serializado en una cadena que contiene el estado y otra información sobre la alarma. Para obtener más información, consulte Propiedades del estado de alarma.

Nombre de la propiedad: `AWS/ALARM_STATE`

Tipo de propiedad: medida

Tipo de datos: `STRUCT`

Tipo de estructura de datos: `AWS/ALARM_STATE`

Origen de alarma

(opcional) el nombre de recurso de Amazon (ARN) del recurso que evalúa el estado de la alarma. En el AWS IoT Events caso de las alarmas, este es el ARN del modelo de alarma.

Nombre de la propiedad: `AWS/ALARM_SOURCE`

Tipo de propiedad: atributo

Tipo de datos: `STRING`

Example Ejemplo de modelo compuesto de alarma

El siguiente modelo de activos representa una caldera que tiene una alarma para controlar su temperatura. AWS IoT SiteWise envía los datos de temperatura AWS IoT Events para detectar la alarma.

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

Temas

- Definición de AWS IoT Events alarmas

- Definición de las alarmas externas

Definición de AWS IoT Events alarmas

Al crear una AWS IoT Events alarma, AWS IoT SiteWise envía los valores de las propiedades de los activos AWS IoT Events para evaluar el estado de la alarma. AWS IoT Events las definiciones de alarma dependen del modelo de alarma en el que se defina AWS IoT Events. Para definir una AWS IoT Events alarma en un modelo de activos, defina un modelo compuesto de alarmas que especifique el modelo de AWS IoT Events alarma como su propiedad de origen de alarma.

AWS IoT Events las alarmas dependen de entradas como los umbrales de alarma y la configuración de las notificaciones de alarmas. Estas entradas se definen como atributos en el modelo de activo. A continuación, puede personalizar estas entradas en cada activo basado en el modelo. La AWS IoT SiteWise consola puede crear estos atributos por usted. Si define las alarmas con la API AWS CLI o la API, debe definir estos atributos manualmente en el modelo de activos.

También puede definir otras acciones, como las acciones de notificación de alarma personalizadas, que deben producirse cuando la alarma detecte algo. Por ejemplo, puede configurar una acción que envíe una notificación push a un tema de Amazon SNS. Para obtener más información sobre las acciones que puede definir, consulte Trabajar con otros AWS servicios en la Guía para AWS IoT Events desarrolladores.

Al actualizar o eliminar un modelo de activos, AWS IoT SiteWise puede comprobar si un modelo de alarma AWS IoT Events monitorea una propiedad de activo asociada a este modelo de activos. Esto le impide eliminar una propiedad de activo que una AWS IoT Events alarma esté utilizando actualmente. Para activar esta función AWS IoT SiteWise, debe tener el `iotevents:ListInputRoutings` permiso. Este permiso permite AWS IoT SiteWise realizar llamadas a la operación de ListInputRoutingsAPI admitida por AWS IoT Events. Para obtener más información, consulte ListInputRoutings Permiso (opcional).

> **Note**
>
> La característica de notificaciones de alarma no está disponible en la región de China (Pekín).

Temas

- Requisitos para las notificaciones de alarma

- Definir una AWS IoT Events alarma (AWS IoT SiteWise consola)
- Definir una AWS IoT Events alarma (AWS IoT Events consola)
- Definir una AWS IoT Events alarma (AWS CLI)

Requisitos para las notificaciones de alarma

AWS IoT Events utiliza una AWS Lambda función de su AWS cuenta para enviar notificaciones de alarma. Debe crear esta función Lambda en la misma AWS región que sus alarmas para activar las notificaciones de alarma. Esta función de Lambda utiliza Amazon Simple Notification Service (Amazon SNS) para enviar notificaciones de texto y Amazon Simple Email Service (Amazon SES) para enviar notificaciones por correo electrónico. Al crear la AWS IoT Events alarma, se configuran los protocolos y los ajustes que utiliza la alarma para enviar las notificaciones.

AWS IoT Events proporciona una plantilla de AWS CloudFormation pila que puede utilizar para crear esta función Lambda en su cuenta. Para obtener más información, consulte Notificación de alarma de la función de Lambda en la Guía para desarrolladores de AWS IoT Events .

Definir una AWS IoT Events alarma (AWS IoT SiteWise consola)

Puede utilizar la AWS IoT SiteWise consola para definir una AWS IoT Events alarma en un modelo de activos existente. Para definir una AWS IoT Events alarma en un nuevo modelo de activos, cree el modelo de activos y, a continuación, complete estos pasos. Para obtener más información, consulte Creación de modelos de activos.

> **Important**
>
> Cada alarma requiere un atributo que especifique el valor de umbral con el que comparar la alarma. Debe definir el atributo de valor de umbral en el modelo de activo antes de poder definir una alarma.
> Considere un ejemplo en el que desee definir una alarma que detecte cuando una turbina eólica supere su índice de velocidad máxima del viento de 80 km/h. Antes de definir la alarma, debe definir un atributo (Velocidad máxima del viento) con un valor predeterminado de `50`.

Para definir una AWS IoT Events alarma en un modelo de activos

1. Vaya a la consola de AWS IoT SiteWise.

2. En el panel de navegación, elija Models (Modelos).
3. Elija el modelo de activo para el que desee definir una alarma.
4. Seleccione la pestaña Alarma.
5. Seleccione Añadir alarma.
6. En la sección Opciones de tipos de alarma, seleccione Alarma de AWS IoT Events .
7. En la sección Detalles de regla haga lo siguiente:

    a. Escriba un nombre para la alarma.

    b. (Opcional) Ingrese una descripción para su alarma.

8. En la sección Definiciones de umbral se define cuándo debe detectar algo la alarma y la gravedad de la alarma. Haga lo siguiente:

    a. Seleccione la Propiedad sobre la que debe detectar la alarma. Cada vez que esta propiedad recibe un nuevo valor, AWS IoT SiteWise envía el valor AWS IoT Events a para evaluar el estado de la alarma.

    b. Seleccione el Operador que se utilizará para comparar la propiedad con el valor de umbral. Puede elegir entre las siguientes opciones:

        - < Menor que
        - <= Menor que o igual a
        - == (igual)
        - != Distinto de
        - >= Mayor que o igual a
        - > Mayor que

    c. En Valor, seleccione la propiedad del atributo que desee utilizar como valor de umbral. AWS IoT Events compara el valor de la propiedad con el valor de este atributo.

    d. Introduzca la Gravedad de la alarma. Use un número que pueda comprender su equipo para reflejar la gravedad de esta alarma.

9. (Opcional) En la sección Configuración de notificaciones: opcional, haga lo siguiente:

    a. Elija Activar.

> **Note**
>
> Si elige Inactivo, ni usted ni su equipo recibirán ninguna notificación de alarma.

b. En Destinatario, elija el destinatario.

> **Important**
>
> Puede enviar notificaciones de alarma a AWS IAM Identity Center los usuarios. Para utilizar esta característica, debe habilitar IAM Identity Center. Solo puede activar el IAM Identity Center en una AWS región a la vez. Esto significa que solo puede definir las notificaciones de alarma en la región en la que habilite IAM Identity Center. Para obtener más información, consulte la Introducción de la Guía del usuario de AWS IAM Identity Center .

c. En Protocolo elija una de las siguientes opciones:

- Correo electrónico y texto: la alarma notifica a los usuarios del IAM Identity Center con un mensaje SMS y un mensaje de correo electrónico.
- Correo electrónico: la alarma notifica a los usuarios del IAM Identity Center con un mensaje de correo electrónico.
- Texto: la alarma notifica a los usuarios del IAM Identity Center con un mensaje SMS.

d. En Remitente, elija el remitente.

> **Important**
>
> Debe verificar la dirección de correo electrónico del remitente en Amazon Simple Email Service (Amazon SES). Para obtener más información, consulte Verificación de direcciones de correo electrónico en Amazon SES, en la Guía para desarrolladores de Amazon Simple Email Service.

10. En la sección Estado predeterminado del activo, puede establecer el estado predeterminado para las alarmas creadas a partir de este modelo de activo.

> **Note**
>
> Podrá activar o desactivar esta alarma para los activos que cree a partir de este modelo de activo en un paso posterior.

11. En la sección de configuración avanzada, puede configurar los permisos, los ajustes de notificación adicionales, las acciones del estado de alarma, el modelo de alarma en SiteWise Monitor y el flujo de confirmación.

> **Note**
>
> AWS IoT Events las alarmas requieren las siguientes funciones de servicio:
>
> - Una función que se AWS IoT Events supone que debe enviar los valores del estado de alarma a AWS IoT SiteWise.
> - Una función que AWS IoT Events asume el envío de datos a Lambda. Solo necesita esta función si su alarma envía notificaciones.

En la sección Permisos, haga lo siguiente:

a. En Rol de AWS IoT Events , utilice un rol existente o cree uno con los permisos necesarios. Este rol requiere el permiso `iotsitewise:BatchPutAssetPropertyValue` y una relación de confianza que permita a iotevents.amazonaws.com asumir ese rol.

b. Para el AWS IoT Events rol de Lambda, utilice un rol existente o cree un rol con los permisos necesarios. Este rol requiere los permisos `lambda:InvokeFunction` y `sso-directory:DescribeUser` y una relación de confianza que permita a `iotevents.amazonaws.com` asumir ese rol.

12. (Opcional) En la sección Configuración de notificación adicional, haga lo siguiente:

a. En Atributo del destinatario, defina un atributo cuyo valor especifique el destinatario de la notificación. Puede elegir a los usuarios del IAM Identity Center como destinatarios.

Puede crear un atributo o utilizar uno existente en el modelo de activo.

- Si elige Crear un nuevo atributo de destinatario, especifique el Nombre del atributo de destinatario y el Valor predeterminado del destinatario: opcional para el atributo.

- Si elige Usar un atributo de destinatario existente, elija el atributo en Nombre del atributo del destinatario. La alarma utiliza el valor predeterminado del atributo que elija.

Puede anular el valor predeterminado de cada activo que cree desde este modelo de activo.

b. En Atributo del mensaje personalizado, defina un atributo cuyo valor especifique el mensaje personalizado que se debe enviar además del mensaje de cambio de estado predeterminado. Por ejemplo, puede especificar un mensaje que ayude a su equipo a entender cómo abordar esta alarma.

Puede optar por crear un atributo o utilizar uno existente en el modelo de activo.

- Si opta por Crear un nuevo atributo de mensaje personalizado, especifique el Nombre de atributo del mensaje personalizado y el Valor predeterminado del mensaje personalizado: opcional para el atributo.
- Si opta por Usar un atributo de mensaje personalizado existente, elija el atributo en Nombre de atributo del mensaje personalizado. La alarma utiliza el valor predeterminado del atributo que elija.

Puede anular el valor predeterminado de cada activo que cree desde este modelo de activo.

c. En Gestionar su función de Lambda, realice alguna de las siguientes operaciones:

- Para AWS IoT SiteWise crear una nueva función de Lambda, elija Crear una nueva lambda a partir de una plantilla gestionada por AWS.
- Para usar una función de Lambda existente, elija Usar una Lambda existente y elija el nombre de la función.

Para obtener más información, consulte Administración de notificaciones de alarma en la Guía para desarrolladores de AWS IoT Events .

13. (Opcional) En la sección Configurar acción de estado, haga lo siguiente:

a. Elija Editar acción.

b. En Agregar acciones del estado de la alarma, añada acciones y, a continuación, seleccione Guardar.

Puede agregar hasta 10 acciones.

AWS IoT Events puede realizar acciones cuando la alarma está activa. Puede definir acciones integradas para usar un temporizador o establecer una variable, o enviar datos a otros AWS recursos. Para obtener más información, consulte Acciones admitidas en la Guía para desarrolladores de AWS IoT Events .

14. (Opcional) En Administrar el modelo de alarma en el SiteWise monitor (opcional), elija Activo o Inactivo.

    Utilice esta opción para actualizar el modelo de alarma en SiteWise Monitorss. Esta opción está habilitada de forma predeterminada.

15. En Flujo de reconocimiento, seleccione Activo o Inactivo. Para obtener más información sobre el flujo de reconocimiento, consulte Estados de alarma.

16. Seleccione Añadir alarma.

> **Note**
>
> La AWS IoT SiteWise consola realiza varias solicitudes de API para añadir la alarma al modelo de activos. Al elegir Agregar alarma, la consola abre un cuadro de diálogo que muestra el progreso de estas solicitudes de API. Permanezca en esta página hasta que cada solicitud de API se realice correctamente o hasta que falle una solicitud de API. Si se produce un error en una solicitud, cierre el cuadro de diálogo, corrija el problema y seleccione Agregar alarma para volver a intentarlo.

Definir una AWS IoT Events alarma (AWS IoT Events consola)

Puede utilizar la AWS IoT Events consola para definir una AWS IoT Events alarma en un modelo de activos existente. Para definir una AWS IoT Events alarma en un nuevo modelo de activos, cree el modelo de activos y, a continuación, complete estos pasos. Para obtener más información, consulte Creación de modelos de activos.

> **Important**
>
> Cada alarma requiere un atributo que especifique el valor de umbral con el que comparar la alarma. Debe definir el atributo de valor de umbral en el modelo de activo antes de poder definir una alarma.

Considere un ejemplo en el que desee definir una alarma que detecte cuando una turbina eólica supere su índice de velocidad máxima del viento de 80 km/h. Antes de definir la alarma, debe definir un atributo (Velocidad máxima del viento) con un valor predeterminado de `50`.

Para definir una AWS IoT Events alarma en un modelo de activos

1. Vaya a la consola de AWS IoT Events.
2. En el panel de navegación, elija Modelos de alarmas.
3. Elija Crear modelo de alarma.
4. Escriba un nombre para la alarma.
5. (Opcional) Ingrese una descripción para su alarma.
6. En la sección Destino de la alarma, haga lo siguiente:
   a. En Opciones de destino, elija la propiedad del activo de AWS IoT SiteWise .
   b. Elija el ,modelo de activo para el que desea añadir una alarma.
7. En la sección Definiciones de umbral se define cuándo debe detectar algo la alarma y la gravedad de la alarma. Haga lo siguiente:
   a. Seleccione la Propiedad sobre la que debe detectar la alarma. Cada vez que esta propiedad recibe un nuevo valor, AWS IoT SiteWise envía el valor AWS IoT Events a para evaluar el estado de la alarma.
   b. Seleccione el Operador que se utilizará para comparar la propiedad con el valor de umbral. Puede elegir entre las siguientes opciones:
      - < Menor que
      - <= Menor que o igual a
      - == (igual)
      - != Distinto de
      - >= Mayor que o igual a
      - > Mayor que
   c. En Valor, seleccione la propiedad del atributo que desee utilizar como valor de umbral. AWS IoT Events compara el valor de la propiedad con el valor de este atributo.

d. Introduzca la Gravedad de la alarma. Use un número que pueda comprender su equipo para reflejar la gravedad de esta alarma.

8. (Opcional) En la sección Configuración de notificaciones: opcional, haga lo siguiente:

   a. En Protocolo elija una de las siguientes opciones:

      - Correo electrónico y texto: la alarma notifica a los usuarios del IAM Identity Center con un mensaje SMS y un mensaje de correo electrónico.
      - Correo electrónico: la alarma notifica a los usuarios del IAM Identity Center con un mensaje de correo electrónico.
      - Texto: la alarma notifica a los usuarios del IAM Identity Center con un mensaje SMS.

   b. En Remitente, elija el remitente.

      > **Important**
      >
      > Debe verificar la dirección de correo electrónico del remitente en Amazon Simple Email Service (Amazon SES). Para obtener más información, consulte Verificación de direcciones de correo electrónico en Amazon SES, en la Guía para desarrolladores de Amazon Simple Email Service.

   c. Elija el atributo en Atributo del destinatario: (opcional). La alarma utiliza el valor predeterminado del atributo que elija.

   d. Elija el atributo en Atributo del mensaje personalizado: (opcional). La alarma utiliza el valor predeterminado del atributo que elija.

9. En la sección Instancia, especifique el Estado predeterminado de esta alarma. Podrá activar o desactivar esta alarma para todos los activos que cree a partir de este modelo de activo en un paso posterior.

10. En los ajustes avanzados, puede configurar los permisos, los ajustes de notificación adicionales, las acciones del estado de alarma, el modelo de alarma en SiteWise Monitor y el flujo de confirmación.

    > **Note**
    >
    > AWS IoT Events las alarmas requieren las siguientes funciones de servicio:
    >
    > - Una función que se AWS IoT Events supone que debe enviar los valores del estado de alarma a AWS IoT SiteWise.

- Una función que AWS IoT Events asume el envío de datos a Lambda. Solo necesita esta función si su alarma envía notificaciones.

a. En la sección Flujo de reconocimiento, elija Habilitado o Deshabilitado. Para obtener más información sobre el flujo de reconocimiento, consulte Estados de alarma.

b. En la sección Permisos, haga lo siguiente:

   i. En Rol de AWS IoT Events , utilice un rol existente o cree uno con los permisos necesarios. Este rol requiere el permiso `iotsitewise:BatchPutAssetPropertyValue` y una relación de confianza que permita a iotevents.amazonaws.com asumir ese rol.

   ii. Para el rol de Lambda, utilice un rol existente o cree un rol con los permisos necesarios. Este rol requiere los permisos `lambda:InvokeFunction` y `sso-directory:DescribeUser` y una relación de confianza que permita a `iotevents.amazonaws.com` asumir ese rol.

c. (Opcional) En el panel de Configuración de notificación adicional, haga lo siguiente:

   - En Gestionar su Función de Lambda, realice alguna de las siguientes operaciones:
     - Para AWS IoT Events crear una nueva función Lambda, elija Crear una nueva función Lambda.
     - Para usar una función de Lambda existente, elija Usar una función de Lambda existente y elija el nombre de la función.

   Para obtener más información, consulte Administración de notificaciones de alarma en la Guía para desarrolladores de AWS IoT Events .

d. (Opcional) En la sección Establecer acción de estado: opcional, haga lo siguiente:

   - En Acciones de estado de alarma, añada acciones y, a continuación, seleccione Guardar.

     Puede agregar hasta 10 acciones.

   AWS IoT Events puede realizar acciones cuando la alarma está activa. Puede definir acciones integradas para usar un temporizador o establecer una variable, o enviar datos a

otros AWS recursos. Para obtener más información, consulte Acciones admitidas en la Guía para desarrolladores de AWS IoT Events .

11. Seleccione Crear.

> **Note**
>
> La AWS IoT Events consola realiza varias solicitudes de API para añadir la alarma al modelo de activos. Al elegir Agregar alarma, la consola abre un cuadro de diálogo que muestra el progreso de estas solicitudes de API. Permanezca en esta página hasta que cada solicitud de API se realice correctamente o hasta que falle una solicitud de API. Si se produce un error en una solicitud, cierre el cuadro de diálogo, corrija el problema y seleccione Agregar alarma para volver a intentarlo.

Definir una AWS IoT Events alarma (AWS CLI)

Puede usar el AWS Command Line Interface (AWS CLI) para definir una AWS IoT Events alarma que supervise la propiedad de un activo. Puede definir una alarma en un modelo de activo nuevo o existente. Después de definir la alarma en el modelo de activos, se crea una alarma AWS IoT Events y se conecta al modelo de activos. En este proceso, hará lo siguiente:

Pasos

- Paso 1: definir una alarma en un modelo de activo
- Paso 2: Definir un modelo AWS IoT Events de alarma
- Paso 3: Habilitar el flujo de datos entre y AWS IoT SiteWiseAWS IoT Events

Paso 1: definir una alarma en un modelo de activo

Añada una definición de alarma y las propiedades asociadas a un modelo de activo nuevo o existente.

Para definir una alarma en un modelo de activo (CLI)

1. Cree un archivo denominado `asset-model-payload.json`. Siga los pasos de estas otras secciones para añadir los detalles de su modelo de activo al archivo, pero no envíe la solicitud para crear o actualizar el modelo de activo. En esta sección, debe añadir una definición de alarma a los detalles del modelo de activo del archivo `asset-model-payload.json`.

- Para obtener más información acerca de cómo crear un modelo de activos, consulte Crear un modelo de activos (AWS CLI).
- Para obtener más información acerca de cómo actualizar un modelo de activo existente, consulte Actualización de un modelo de activo o componente (AWS CLI).

> **Note**
>
> Su modelo de activo debe definir al menos una propiedad de activo, incluida la propiedad del activo que se va a monitorear con la alarma.

2. Añada un modelo compuesto de alarma (`assetModelCompositeModels`) al modelo de activo. Un modelo compuesto de AWS IoT Events alarmas especifica el `IOT_EVENTS` tipo y especifica una propiedad de la fuente de la alarma. La propiedad de la fuente de alarma se añade después de crear el modelo de alarma en AWS IoT Events.

> **Important**
>
> El modelo compuesto de alarma debe tener el mismo nombre que el modelo de AWS IoT Events alarma que cree más adelante. Los nombres de modelo de la alarma pueden contener únicamente caracteres alfanuméricos. Especifique un nombre alfanumérico único para poder usar el mismo nombre para el modelo de alarma.

```
{
  ...
  "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. Añada un atributo de umbral de alarma al modelo de activo. Especifique el valor predeterminado que se utilizará para este umbral. Puede anular este valor predeterminado de cada activo basado en este modelo.

> **Note**
>
> El atributo de umbral de alarma debe ser un `INTEGER` o un `DOUBLE`.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "Temperature Max Threshold",
      "dataType": "DOUBLE",
      "type": {
        "attribute": {
          "defaultValue": "105.0"
        }
      }
    }
  ]
}
```

4. (Opcional) Añada atributos de notificaciones de alarma al modelo de activo. Estos atributos especifican el destinatario del IAM Identity Center y otras entradas que se AWS IoT Events utilizan para enviar notificaciones cuando la alarma cambia de estado. Puede anular estos valores predeterminados en cada activo basado en este modelo.

> **Important**
>
> Puede enviar notificaciones de alarma a AWS IAM Identity Center los usuarios. Para utilizar esta característica, debe habilitar IAM Identity Center. Solo puede activar el IAM Identity Center en una AWS región a la vez. Esto significa que solo puede definir las notificaciones de alarma en la región en la que habilite IAM Identity Center. Para obtener más información, consulte la Introducción de la Guía del usuario de AWS IAM Identity Center .

Haga lo siguiente:

a. Añada un atributo que especifique el ID de su almacén de identidades de IAM Identity Center. Puede utilizar la operación de la ListInstancesAPI del IAM Identity Center para enumerar sus almacenes de identidades. Esta operación solo funciona en la región en la que se habilite IAM Identity Center.

```
aws sso-admin list-instances
```

A continuación, especifique el ID del almacén de identidades (por ejemplo, `d-123EXAMPLE`) como valor predeterminado para el atributo.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "identityStoreId",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "d-123EXAMPLE"
        }
      }
    }
  ]
}
```

b. Añada un atributo que especifique el ID del usuario de IAM Identity Center que recibe notificaciones. Para definir un destinatario de notificación predeterminado, añada un ID de usuario de IAM Identity Center como valor predeterminado. Realice una de las siguientes acciones para obtener un ID de usuario de IAM Identity Center:

   i. Puede utilizar la ListUsersAPI del IAM Identity Center para obtener el ID de un usuario cuyo nombre de usuario conozca. Reemplace *d-123Example* por el ID de su almacén de identidades y reemplace *Name* por el nombre del usuario.

```
aws identitystore list-users \
  --identity-store-id d-123EXAMPLE \
  --filters AttributePath=UserName,AttributeValue=Name
```

   ii. Utilice la consola de IAM Identity Center para explorar los usuarios y buscar un ID de usuario.

   A continuación, especifique el ID de usuario (por ejemplo, `123EXAMPLE-a1b2c3d4-5678-90ab-cdef-33333EXAMPLE`) como valor predeterminado para el atributo o defina el atributo sin un valor predeterminado.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "userId",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "123EXAMPLE-a1b2c3d4-5678-90ab-cdef-33333EXAMPLE"
        }
      }
    }
  ]
}
```

c. (Opcional) Añada un atributo que especifique el ID de remitente predeterminado para las notificaciones de mensajes SMS (de texto). El ID del remitente aparece como el remitente del mensaje en los mensajes que envía Amazon Simple Notification Service (Amazon SNS).

Para obtener más información, consulte Solicitud de ID de remitente para mensajería SMS con Amazon SNS en Guía para desarrolladores de Amazon Simple Notification Service.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "senderId",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "MyFactory"
        }
      }
    }
  ]
}
```

d. (Opcional) Añada un atributo que especifique la dirección de correo electrónico predeterminada que se debe utilizar como dirección de origen de en las notificaciones por correo electrónico.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "fromAddress",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "my.factory@example.com"
        }
      }
    }
  ]
}
```

e. (Opcional) Añada un atributo que especifique el asunto predeterminado que se debe utilizar en las notificaciones por correo electrónico.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "emailSubject",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "[ALERT] High boiler temperature"
        }
      }
    }
  ]
}
```

f. (Opcional) Añada un atributo que especifique un mensaje adicional para incluirlo en las notificaciones. De forma predeterminada, los mensajes de la notificación incluyen información sobre la alarma. También puede incluir un mensaje adicional que proporcione al usuario más información.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "additionalMessage",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "Turn off the power before you check the alarm."
        }
      }
    }
  ]
}
```

5. Cree el modelo de activo o actualice el modelo de activo existente. Realice una de las acciones siguientes:

   - Ejecute el siguiente comando para crear el modelo de activo.

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

- Ejecute el siguiente comando para actualizar el modelo de activo existente. *asset-model-id*Sustitúyala por la ID del modelo de activos.

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

Después de ejecutar el comando, anote `assetModelId` en la respuesta.

Ejemplo: modelo de activo de caldera

El siguiente modelo de activo representa una caldera que informa de los datos de temperatura. Este modelo de activo define una alarma que detecta cuando la caldera se sobrecalienta.

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

Paso 2: Definir un modelo AWS IoT Events de alarma

Cree el modelo de alarma en AWS IoT Events. En AWS IoT Events, se utilizan expresiones para especificar valores en los modelos de alarma. Puede utilizar expresiones para especificar los valores desde los AWS IoT SiteWise que evaluar y utilizarlos como entradas para la alarma. Cuando AWS

IoT SiteWise envía los valores de las propiedades del activo al modelo de alarma, AWS IoT Events evalúa la expresión para obtener el valor de la propiedad o el identificador del activo. Puede utilizar las siguientes expresiones en el modelo de alarma:

- Valores de propiedades de activos

  Para obtener el valor de la propiedad de un activo, utilice la siguiente expresión. *`assetModelId`*Reemplace por el ID del modelo de activo y reemplace *`PropertyID`* por el ID de la propiedad.

  ```
  $sitewise.assetModel.`assetModelId`.`propertyId`.propertyValue.value
  ```

- ID de activo

  Para obtener el ID del activo, utilice la siguiente expresión. *`assetModelId`*Reemplace por el ID del modelo de activo y reemplace *`PropertyID`* por el ID de la propiedad.

  ```
  $sitewise.assetModel.`assetModelId`.`propertyId`.assetId
  ```

> **Note**
>
> Al crear el modelo de alarma, puede definir literales en lugar de expresiones que se evalúan como valores. AWS IoT SiteWise Esto puede reducir el número de atributos que define en su modelo de activo. Sin embargo, si define un valor como literal, no podrá personalizar ese valor en los activos basados en el modelo de activo. AWS IoT SiteWise Monitor Los usuarios tampoco pueden personalizar la alarma, ya que solo pueden configurar los ajustes de alarma en los activos.

Para crear un modelo AWS IoT Events de alarma (CLI)

1. Al crear el modelo de alarma en AWS IoT Events, debe especificar el ID de cada propiedad que utilice la alarma, que incluye lo siguiente:

   - La propiedad del estado de alarma en el modelo de activo compuesto
   - La propiedad que monitorea la alarma
   - El atributo de umbral

- (Opcional) El atributo de ID del almacén de identidades de IAM Identity Center
- (Opcional) El atributo de ID de usuario de IAM Identity Center
- (Opcional) El atributo de ID del remitente del SMS
- (Opcional) El atributo de dirección de origen de del correo electrónico
- (Opcional) El atributo de asunto del correo electrónico
- (Opcional) El atributo de mensaje adicional

Ejecute el siguiente comando para recuperar los ID de estas propiedades en el modelo de activo. *asset-model-id*Sustitúyalo por el ID del modelo de activos del paso anterior.

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

La operación devuelve una respuesta que contiene los detalles del modelo de activo. Anote el ID de cada propiedad que utiliza la alarma. Estos identificadores se utilizan al crear el modelo de alarma de AWS IoT Events en el siguiente paso.

2. Cree el modelo de alarma en AWS IoT Events. Haga lo siguiente:

   a. Cree un archivo denominado `alarm-model-payload.json`.

   b. Copie el objeto JSON siguiente en el archivo.

   c. Escriba un nombre (`alarmModelName`), la descripción (`alarmModelDescription`) y gravedad (`severity`) de su alarma. Para la gravedad, especifique un número entero que refleje los niveles de gravedad de su empresa.

   > **Important**
   >
   > El modelo de alarma debe tener el mismo nombre que el modelo compuesto de alarma que definió anteriormente en su modelo de activo.
   > Los nombres de modelo de la alarma pueden contener únicamente caracteres alfanuméricos.

```
{
  "alarmModelName": "BoilerTemperatureHighAlarm",
  "alarmModelDescription": "Detects when the boiler temperature is high.",
  "severity": 3
```

```
}
```

d. Añada la regla de comparación (`alarmRule`) a la alarma. Esta regla define la propiedad que se debe monitorear (`inputProperty`), el valor de umbral que se va a comparar (`threshold`) y el operador de comparación que se debe usar (`comparisonOperator`).

- *`assetModelId`*Sustitúyalo por el ID del modelo de activos.
- *`alarmPropertyId`*Sustitúyalo por el ID de la propiedad que monitorea la alarma.
- *`thresholdAttributeId`*Sustitúyalo por el ID de la propiedad del atributo de umbral.
- Reemplace *`GREATER`* por el operador que se debe usar para comparar los valores de propiedades con el umbral. Puede elegir entre las siguientes opciones:
  - `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. Agregar una acción (`alarmEventActions`) para enviar el estado de alarma al AWS IoT SiteWise cuando la alarma cambie de estado.

> **Note**
>
> Para una configuración avanzada, puede definir acciones adicionales que deben realizarse cuando la alarma cambie de estado. Por ejemplo, puede llamar a una función de AWS Lambda o publicar en un tema de MQTT. Para obtener más información, consulte Trabajar con otros AWS servicios en la Guía para AWS IoT Events desarrolladores.

- *assetModelId*Sustitúyalo por el ID del modelo de activos.
- *alarmPropertyId*Sustitúyalo por el ID de la propiedad que monitorea la alarma.
- *Sustituya alarmStateProperty el identificador por el identificador de la propiedad del estado de alarma en el modelo compuesto de alarmas.*

```
{
  "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. (Opcional) Configure las opciones de notificación de alarmas. La acción de notificación de alarmas utiliza una función de Lambda en su cuenta para enviar notificaciones de alarma. Para obtener más información, consulte Requisitos para las notificaciones de alarma. En los ajustes de notificación de alarmas, puede configurar las notificaciones por SMS y correo electrónico para enviarlas a los usuarios del IAM Identity Center. Haga lo siguiente:

i. Añada la configuración de notificaciones de alarma (`alarmNotification`) a la carga en `alarm-model-payload.json`.

- Sustituya *`alarmNotificationFunctionArn`* por el ARN de la función Lambda que gestiona las notificaciones de alarma.

```
{
  "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. (Opcional) Configure las notificaciones por SMS (`smsConfigurations`) para enviarlas a un usuario de IAM Identity Center cuando la alarma cambie de estado.

- *identityStoreIdAttributeId*Sustitúyalo por el ID del atributo que contiene el ID del almacén de identidades del IAM Identity Center.
- Sustituya el *userIdAttributeID* por el ID del atributo que contiene el ID del usuario del Centro de Identidad de IAM.
- *Sustituya senderIdAttribute el ID por el ID del atributo que contiene el ID del remitente de Amazon SNS o elimínelo senderId de la carga útil.*
- *Sustituya additionalMessageAttribute el ID por el ID del atributo que contiene el mensaje adicional o elimínelo additionalMessage de la carga útil.*

```
{
  "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. (Opcional) Configure las notificaciones por correo electrónico (`emailConfigurations`) para enviarlas a un usuario de IAM Identity Center cuando la alarma cambie de estado.

- *identityStoreIdAttributeId*Sustitúyalo por el ID de la propiedad del atributo ID del almacén de identidades del IAM Identity Center.
- Sustituya el *userIdAttributeID* por el ID de la propiedad del atributo de ID de usuario del IAM Identity Center.
- Sustituya el *fromAddressAttributeID* por el ID de la propiedad del atributo de dirección «de» o elimínelo `from` de la carga útil.
- Sustituya el *emailSubjectAttributeID* por el ID de la propiedad del atributo del asunto del correo electrónico o elimínelo `subject` de la carga útil.
- Sustituya el *additionalMessageAttributeidentificador* por el identificador de la propiedad adicional del atributo del mensaje o elimínelo `additionalMessage` de la carga útil.

```
{
  "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. (Opcional) Añada las funciones de alarma (`alarmCapabilities`) a la carga en `alarm-model-payload.json`. En este objeto, puede especificar si se habilita el flujo de reconocimiento y el estado de activación predeterminado de los activos basados en el modelo de activo. Para obtener más información sobre el flujo de reconocimiento, consulte Estados de alarma.

```
{
  "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. Añada la función de servicio de IAM (`roleArn`) a la que AWS IoT Events se pueden enviar los datos. AWS IoT SiteWise Este rol requiere el permiso `iotsitewise:BatchPutAssetPropertyValue` y una relación de confianza que permita a `iotevents.amazonaws.com` asumir el rol. Para enviar notificaciones, este rol también requiere los permisos `lambda:InvokeFunction` y `sso-directory:DescribeUser`. Para obtener más información, consulte Rol de servicio de alarmas en la Guía para desarrolladores de AWS IoT Events .

- Sustituya el `roleArn` por el ARN del rol que AWS IoT Events puede asumir para realizar estas acciones.

```
{
  "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. Ejecute el siguiente comando para crear el modelo de AWS IoT Events alarma a partir de la carga útil entrante. `alarm-model-payload.json`

```
aws iotevents create-alarm-model --cli-input-json file://alarm-model-
payload.json
```

j. La operación devuelve una respuesta que incluye el ARN del modelo de alarma, `alarmModelArn`. Copie este ARN para configurar en el siguiente paso la definición de la alarma en su modelo de activo.

Paso 3: Habilitar el flujo de datos entre y AWS IoT SiteWiseAWS IoT Events

Después de crear los recursos necesarios en AWS IoT SiteWise y AWS IoT Events, puede habilitar el flujo de datos entre los recursos para activar la alarma. En esta sección, usted actualiza la

definición de alarma en el modelo de activo para usar el modelo de alarma que ha creado en el paso anterior.

Para habilitar el flujo de datos entre AWS IoT SiteWise y AWS IoT Events (CLI)

- Configure el modelo de alarma como origen de la alarma en el modelo de activo. Haga lo siguiente:

  a. Ejecute el siguiente comando para recuperar la definición del modelo de activo existente. *asset-model-id*Sustitúyalo por el ID del modelo de activos.

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

  La operación devuelve una respuesta que contiene los detalles del modelo de activo.

  b. Cree un archivo llamado `update-asset-model-payload.json` y copie la respuesta del comando anterior en el archivo.

  c. Elimine los siguientes pares de clave-valor del archivo `update-asset-model-payload.json`:

  - `assetModelId`
  - `assetModelArn`
  - `assetModelCreationDate`
  - `assetModelLastUpdateDate`
  - `assetModelStatus`

  d. Añada la propiedad de origen de alarma (`AWS/ALARM_SOURCE`) al modelo compuesto de alarmas que definió anteriormente. *alarmModelArn*Sustitúyalo por el ARN del modelo de alarma, que establece el valor de la propiedad de la fuente de alarma.

  ```
  {
    ...
    "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. Ejecute el siguiente comando para actualizar el modelo de activo con la definición almacenada en el archivo `update-asset-model-payload.json`. *asset-model-id*Sustitúyalo por el ID del modelo de activos.

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

Su modelo de activo ahora define una alarma capaz de detectar en AWS IoT Events. La alarma monitorea la propiedad de destino en todos los activos basados en este modelo de activo. Puede

configurar la alarma de cada activo para personalizar propiedades como el umbral o el destinatario de IAM Identity Center para cada activo. Para obtener más información, consulte Configuración de alarmas en los activos.

Definición de las alarmas externas

Las alarmas externas contienen el estado de las alarmas que se detectan fuera de AWS IoT SiteWise.

Definición de una alarma externa (consola)

Puede utilizar la AWS IoT SiteWise consola para definir una alarma externa en un modelo de activos existente. Para definir una alarma externa en un nuevo modelo de activo, cree el modelo de activo y, a continuación, siga estos pasos. Para obtener más información, consulte Creación de modelos de activos.

Para definir una alarma en un modelo de activo

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Models (Modelos).
3. Elija el modelo de activo para el que desee definir una alarma.
4. Seleccione la pestaña Definiciones de alarma.
5. Seleccione Añadir alarma.
6. En Opciones de tipos de alarmas, seleccione Alarma externa.
7. Escriba un nombre para la alarma.
8. (Opcional) Ingrese una descripción para su alarma.
9. Seleccione Añadir alarma.

Definición de una alarma externa (CLI)

Puede utilizarla AWS CLI para definir una alarma externa en un modelo de activos nuevo o existente.

Para añadir una alarma externa a un modelo de activo, añada un modelo compuesto de alarma al modelo de activo. Un modelo compuesto de alarmas externas especifica el tipo de `EXTERNAL`, pero no especifica la propiedad de origen de alarma. El siguiente ejemplo de alarma compuesta define una alarma externa de temperatura.

```
{
  ...
  "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": {}
          }
        }
      ]
    }
  ]
}
```

Para obtener más información sobre cómo añadir un modelo compuesto a un modelo de activo nuevo o existente, consulte lo siguiente:

- Crear un modelo de activos (AWS CLI)
- Actualización de un modelo de activo o componente (AWS CLI)

Después de definir la alarma externa, puede ingerir el estado de alarma a los activos basados en el modelo de activo. Para obtener más información, consulte Ingesta del estado de las alarmas externas.

Configuración de alarmas en los activos

Tras definir una AWS IoT Events alarma en un modelo de activo, puede configurar la alarma en cada activo en función del modelo de activo. Puede editar el valor de umbral y los ajustes de notificación de la alarma. Cada uno de estos valores es un atributo del activo, por lo que puede actualizar el valor predeterminado del atributo para configurar estos valores.

> **Note**
>
> Puede configurar estos valores para AWS IoT Events las alarmas, pero no para las alarmas externas.

Temas

Configuración de un valor de umbral (consola)

Puede utilizar la AWS IoT SiteWise consola para actualizar el valor del atributo que especifica el valor umbral de una alarma.

Para actualizar el valor del umbral de una alarma (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Activos.
3. Elija el activo para el que desea actualizar un valor del umbral de la alarma.

   > **Tip**
   >
   > Puede elegir el icono de flecha para expandir una jerarquía de activos y encontrar su activo.

4. Seleccione Editar.

5. Busque el atributo que utiliza la alarma para su valor de umbral y, a continuación, introduzca su nuevo valor.
6. Seleccione Guardar.

Configuración de un valor umbral (AWS CLI)

Puede usar AWS Command Line Interface (AWS CLI) para actualizar el valor del atributo que especifica el valor umbral de una alarma.

Debe conocer los `assetId` de sus activos y los `propertyId` de las propiedades para completar este procedimiento. También puede usar el ID externo. Si has creado un activo y no lo sabes`assetId`, usa la ListAssetsAPI para enumerar todos los activos de un modelo específico. Utilice la DescribeAssetoperación para ver las propiedades de su activo, incluidos los identificadores de propiedad.

Utilice la BatchPutAssetPropertyValueoperación para asignar valores de atributos a su activo. Puede utilizar esta operación para establecer varios atributos a la vez. La carga de esta operación contiene una lista de entradas y cada una contiene el ID de activo, el ID de propiedad y el valor de atributo.

Para actualizar el valor de un atributo (AWS CLI)

1. Cree un archivo llamado `batch-put-payload.json` y copie el siguiente objeto JSON en el archivo. En esta carga de ejemplo se muestra cómo establecer la latitud y la longitud de una turbina eólica. Actualice los ID, los valores y las marcas temporales para modificar la carga para su caso de 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
          }
        }
      ]
    }
  ]
}
```

- Cada entrada de la carga contiene un `entryId` que puede definir como una única cadena. Si la entrada de la solicitud no se realiza correctamente, cada error contendrá el `entryId` de la solicitud correspondiente para que sepa qué solicitudes deben volver a intentarse.
- Para establecer un valor de atributo, puede incluir una estructura timestamp-quality-value (TQV) en la lista de propiedades `propertyValues` de cada atributo. Esta estructura debe contener el nuevo `value` y la `timestamp` actual.
  - `value`: una estructura que contiene uno de los siguientes campos, en función del tipo de propiedad que se establezca:
    - `booleanValue`
    - `doubleValue`
    - `integerValue`
    - `stringValue`
  - `timestamp`— Una estructura que contiene el tiempo de época actual de Unix en segundos,. `timeInSeconds` AWS IoT SiteWise rechaza todos los puntos de datos con marcas de tiempo que hayan existido durante más de 7 días o más de 5 minutos en el futuro.

Para obtener más información sobre cómo preparar una carga útil para BatchPutAssetPropertyValue, consulte. Ingerir datos mediante la API AWS IoT SiteWise

2. Ejecute el siguiente comando para enviar los valores de los atributos a AWS IoT SiteWise:

```
aws iotsitewise batch-put-asset-property-value -\-cli-input-json file://batch-put-payload.json
```

Configuración de los ajustes de notificación (consola)

Puede utilizar la AWS IoT SiteWise consola para actualizar el valor de los atributos que especifican la configuración de notificación de una alarma.

Para actualizar los ajustes de notificación de una alarma (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Activos.
3. Elija el activo para el que desea actualizar la configuración de la alarma.
4. Elija Editar.
5. Busque el atributo que utiliza la alarma utiliza para el ajuste de notificación que desee cambiar y, a continuación, introduzca su nuevo valor.
6. Seleccione Guardar.

Configuración de los ajustes de notificación (CLI)

Puede usar el AWS Command Line Interface (AWS CLI) para actualizar el valor del atributo que especifica la configuración de notificación de una alarma.

Debe conocer los `assetId` de sus activos y los `propertyId` de las propiedades para completar este procedimiento. También puedes usar el ID externo. Si has creado un activo y no lo sabes`assetId`, usa la ListAssetsAPI para enumerar todos los activos de un modelo específico. Utilice la DescribeAssetoperación para ver las propiedades de su activo, incluidos los identificadores de propiedad.

Utilice la BatchPutAssetPropertyValueoperación para asignar valores de atributos a su activo. Puede utilizar esta operación para establecer varios atributos a la vez. La carga de esta operación contiene una lista de entradas y cada una contiene el ID de activo, el ID de propiedad y el valor de atributo.

Para actualizar el valor de un atributo (AWS CLI)

1. Cree un archivo llamado `batch-put-payload.json` y copie el siguiente objeto JSON en el archivo. En esta carga de ejemplo se muestra cómo establecer la latitud y la longitud de una turbina eólica. Actualice los ID, los valores y las marcas temporales para modificar la carga para su caso de 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
          }
        }
      ]
```

```
    }
  ]
}
```

- Cada entrada de la carga contiene un `entryId` que puede definir como una única cadena. Si la entrada de la solicitud no se realiza correctamente, cada error contendrá el `entryId` de la solicitud correspondiente para que sepa qué solicitudes deben volver a intentarse.
- Para establecer un valor de atributo, puede incluir una estructura timestamp-quality-value (TQV) en la lista de propiedades `propertyValues` de cada atributo. Esta estructura debe contener el nuevo `value` y la `timestamp` actual.
  - `value`: una estructura que contiene uno de los siguientes campos, en función del tipo de propiedad que se establezca:
    - `booleanValue`
    - `doubleValue`
    - `integerValue`
    - `stringValue`
  - `timestamp`— Una estructura que contiene el tiempo de época actual de Unix en segundos,. `timeInSeconds` AWS IoT SiteWise rechaza todos los puntos de datos con marcas de tiempo que hayan existido durante más de 7 días o más de 5 minutos en el futuro.

Para obtener más información sobre cómo preparar una carga útil para BatchPutAssetPropertyValue, consulte. Ingerir datos mediante la API AWS IoT SiteWise

2. Ejecute el siguiente comando para enviar los valores de los atributos a AWS IoT SiteWise:

```
aws iotsitewise batch-put-asset-property-value -\-cli-input-json file://batch-put-payload.json
```

Respuesta a las alarmas

Cuando una AWS IoT Events alarma cambia de estado, puede hacer lo siguiente para responder a la alarma:

- Confirmar la alarma para indicar que está gestionando el problema.

- Posponer la alarma para desactivarla temporalmente.
- Deshabilitar la alarma para desactivarla permanentemente hasta que la vuelva a habilitar.
- Habilitar una alarma deshabilitada para detectar el estado de alarma.
- Restablecer la alarma para borrar su estado y su último valor.

Puedes usar la AWS IoT SiteWise consola o la AWS IoT Events API para responder a una alarma.

> **Note**
>
> Puede responder a AWS IoT Events las alarmas, pero no a las externas.

Temas

Respuesta a una alarma (consola)

Puede usar la AWS IoT SiteWise consola para reconocer, posponer, deshabilitar o activar una alarma.

Temas

Confirmación de una alarma (consola)

Se puede confirmar la alarma para indicar que se está gestionando el problema.

> **Note**
>
> Es necesario habilitar el flujo de reconocimiento en la alarma para poder confirmarla. Esta opción está habilitada de forma predeterminada si define la alarma desde la consola de AWS IoT SiteWise .

Para confirmar una alarma (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Activos.
3. Elija el activo para el que desea confirmar una alarma.

   > **Tip**
   >
   > Puede elegir el icono de flecha para expandir una jerarquía de activos y encontrar su activo.

4. Seleccione la pestaña Alarmas.
5. Seleccione la alarma que desee reconocer y, a continuación, elija Acciones para abrir el menú de acciones de respuesta.
6. Seleccione Confirmar. El estado de la alarma cambia a Confirmado.

Posponer una alarma (consola)

Puede posponer una alarma para deshabilitarla temporalmente. Especifique el tiempo durante el que se debe posponer la alarma.

Para posponer una alarma (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Activos.
3. Elija el activo para el que desea posponer una alarma.

> **Tip**
>
> Puede elegir el icono de flecha para expandir una jerarquía de activos y encontrar su activo.

4. Seleccione la pestaña Alarmas.
5. Seleccione la alarma que desee posponer y, a continuación, elija Acciones para abrir el menú de acciones de respuesta.
6. Seleccione Posponer. Se abre un modelo en el que se especifica la duración de la pausa.
7. Elija la duración de la acción de posponer o introduzca una duración personalizada de la acción de posponer.
8. Seleccione Guardar. El estado de la alarma cambia a Silenciado.

Deshabilitación de una alarma (consola)

Se puede deshabilitar una alarma para que no detecte nada más. Después de deshabilitar la alarma, debe volver a habilitarla si desea que la alarma detecte algo.

Para deshabilitar una alarma (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Activos.
3. Elija el activo para el que desea deshabilitar una alarma.

> **Tip**
>
> Puede elegir el icono de flecha para expandir una jerarquía de activos y encontrar su activo.

4. Seleccione la pestaña Alarmas.
5. Seleccione la alarma que desee deshabilitar y, a continuación, elija Acciones para abrir el menú de acciones de respuesta.
6. Elija Deshabilitar. El estado de la alarma cambia a Deshabilitado.

Habilitar una alarma (consola)

Puede habilitar una alarma para que se vuelva a detectar después de deshabilitarla o posponerla.

Para habilitar una alarma (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Activos.
3. Elija el activo para el que desea habilitar una alarma.

   > **Tip**
   >
   > Puede elegir el icono de flecha para expandir una jerarquía de activos y encontrar su activo.

4. Seleccione la pestaña Alarmas.
5. Seleccione la alarma que desee habilitar y, a continuación, elija Acciones para abrir el menú de acciones de respuesta.
6. Seleccione Habilitar. El estado de la alarma cambia a Normal.

Restablecer una alarma (consola)

Puede restablecer una alarma para borrar su estado y su último valor.

Para restablecer una alarma (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Activos.
3. Elija el activo para el que desea restablecer una alarma.

   > **Tip**
   >
   > Puede elegir el icono de flecha para expandir una jerarquía de activos y encontrar su activo.

4. Seleccione la pestaña Alarmas.
5. Seleccione la alarma que desee habilitar y, a continuación, elija Acciones para abrir el menú de acciones de respuesta.

6. Elija Restablecer. El estado de la alarma cambia a Normal.

Responder a una alarma (API)

Puedes usar la AWS IoT Events API para reconocer, posponer, deshabilitar, habilitar o restablecer una alarma. Para obtener más información, consulte las siguientes operaciones en la Referencia de la API de AWS IoT Events :

- BatchAcknowledgeAlarm
- BatchSnoozeAlarm
- BatchDisableAlarm
- BatchEnableAlarm
- BatchResetAlarm

Para obtener más información, consulte Respuesta a las alarmas en la Guía para desarrolladores de AWS IoT Events .

Ingesta del estado de las alarmas externas

Las alarmas externas son alarmas que se evalúan fuera de ellas AWS IoT SiteWise. Puede utilizar alarmas externas si tiene un origen de datos que notifique el estado de alarma que desea ingerir a AWS IoT SiteWise.

Las propiedades de los estados de alarma requieren un formato específico para los valores de los datos de los estados de alarma. Cada valor de datos debe ser un objeto JSON serializado en una cadena. A continuación, ingiera la cadena serializada como valor de cadena. Para obtener más información, consulte Propiedades del estado de alarma.

Example Ejemplo de valor de los datos de estado de alarma (no serializado)

```
{
  "stateName": "Active"
}
```

Example Ejemplo de valor de los datos de estado de alarma (serializado)

```
{\"stateName\":\"Active\"}
```

> **Note**
>
> Si su origen de datos no puede generar datos en este formato o no puede convertirlos a este formato antes de ingerirlos, puede optar por no utilizar una propiedad de alarma. En su lugar, puede ingerir los datos como una propiedad de medición con el tipo de datos de cadena, por ejemplo. Para obtener más información, consulte Definición de flujos de datos procedentes del equipo (mediciones) y Ingerir datos para AWS IoT SiteWise.

Asignación de flujos de estados de las alarmas externas

Puede definir alias de propiedades para asignar sus flujos de datos a las propiedades de su estado de alarma. Esto le ayuda a identificar fácilmente una propiedad de estado de alarma cuando ingiera o recupera datos. Para obtener más información acerca de los alias de propiedad, consulte Asignación de flujos de datos industriales a propiedades de activos.

Temas

- Asignación de flujos de estados de alarmas externas (consola)
- Mapeo de flujos de estados de alarma externos (AWS CLI)

Asignación de flujos de estados de alarmas externas (consola)

Puede definir alias de propiedades para asignar sus flujos de datos a las propiedades de su estado de alarma. Esto le ayuda a identificar fácilmente una propiedad de estado de alarma cuando ingiera o recupera datos. Para obtener más información acerca de los alias de propiedad, consulte Asignación de flujos de datos industriales a propiedades de activos.

Puede usar la AWS IoT SiteWise consola para configurar un alias para una propiedad de estado de alarma.

Para configurar un alias de propiedad para una propiedad de estado de alarma (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Activos.
3. Elija el activo para el que desea configurar un alias de propiedad.

> **Tip**
>
> Puede elegir el icono de flecha para expandir una jerarquía de activos y encontrar su activo.

4. Elija Alarms (Alarmas).
5. Seleccione la alarma externa para la que desea establecer un alias de propiedad.
6. Elija View (Ver).
7. En el panel de Detalles del estado de alarma, seleccione Editar.
8. Escriba el alias de propiedad.
9. Elija Actualizar.

Mapeo de flujos de estados de alarma externos (AWS CLI)

Puede definir alias de propiedades para asignar sus flujos de datos a las propiedades de su estado de alarma. Esto le ayuda a identificar fácilmente una propiedad de estado de alarma cuando ingiera o recupera datos. Para obtener más información acerca de los alias de propiedad, consulte Asignación de flujos de datos industriales a propiedades de activos.

Puede usar el AWS Command Line Interface (AWS CLI) para establecer un alias para una propiedad de estado de alarma.

Debe conocer los `assetId` de sus activos y los `propertyId` de las propiedades para completar este procedimiento. También puedes usar el ID externo. Si has creado un activo y no lo sabes`assetId`, usa la ListAssetsAPI para enumerar todos los activos de un modelo específico. Utilice la DescribeAssetoperación para ver las propiedades de su activo, incluidos los identificadores de propiedad.

> **Note**
>
> La DescribeAssetrespuesta incluye la lista de modelos de activos compuestos para el activo. Cada alarma es un modelo compuesto. Para encontrar el `propertyId`, busque el modelo compuesto de la alarma y, a continuación, busque la propiedad de `AWS/ALARM_STATE` en ese modelo compuesto.

Para obtener información acerca de cómo establecer el alias de la propiedad, consulte Establecer un alias de propiedad (AWS CLI).

Ingesta de datos de los estados de alarma

Las propiedades del estado de alarma esperan que el estado de la alarma sea una cadena JSON serializada. Para transferir el estado de alarma a una alarma externa AWS IoT SiteWise, ingiera esta cadena serializada como un valor de cadena con una marca de tiempo. En el ejemplo siguiente se muestra un valor de datos de estado para una alarma activa.

```
{\"stateName\":\"Active\"}
```

Para identificar una propiedad del estado de alarma, puede especificar uno de los elementos siguientes:

- El `assetId` y el `propertyId` de la propiedad de alarma a la que se envían los datos.
- El `propertyAlias`, que es un alias de flujo de datos (por ejemplo, `/company/windfarm/3/turbine/7/temperature/high`). Para utilizar esta opción, primero debe establecer el alias de la propiedad de la alarma. Para obtener información sobre cómo configurar los alias de propiedad para las propiedades de los estados de alarma, consulte Asignación de flujos de estados de las alarmas externas.

En el siguiente ejemplo de carga útil de la BatchPutAssetPropertyValueAPI, se muestra cómo formatear el estado de una alarma externa. Esta alarma externa informa cuando la lectura de rotaciones por minuto (RPM) de una turbina eólica es demasiado alta.

Example Ejemplo de BatchPutAssetPropertyValue carga útil para datos de estado de alarma

```
{
    "entries": [
      {
        "entryId": "unique entry ID",
        "propertyAlias": "/company/windfarm/3/turbine/7/temperature/high",
        "propertyValues": [
          {
            "value": {
              "stringValue": "{\"stateName\":\"Active\"}"
            },
            "timestamp": {
```

```
            "timeInSeconds": 1607550262
          }
        }
      ]
    }
  ]
}
```

Para obtener más información sobre cómo usar la API `BatchPutAssetPropertyValue` para ingerir datos, consulte Ingerir datos mediante la API AWS IoT SiteWise.

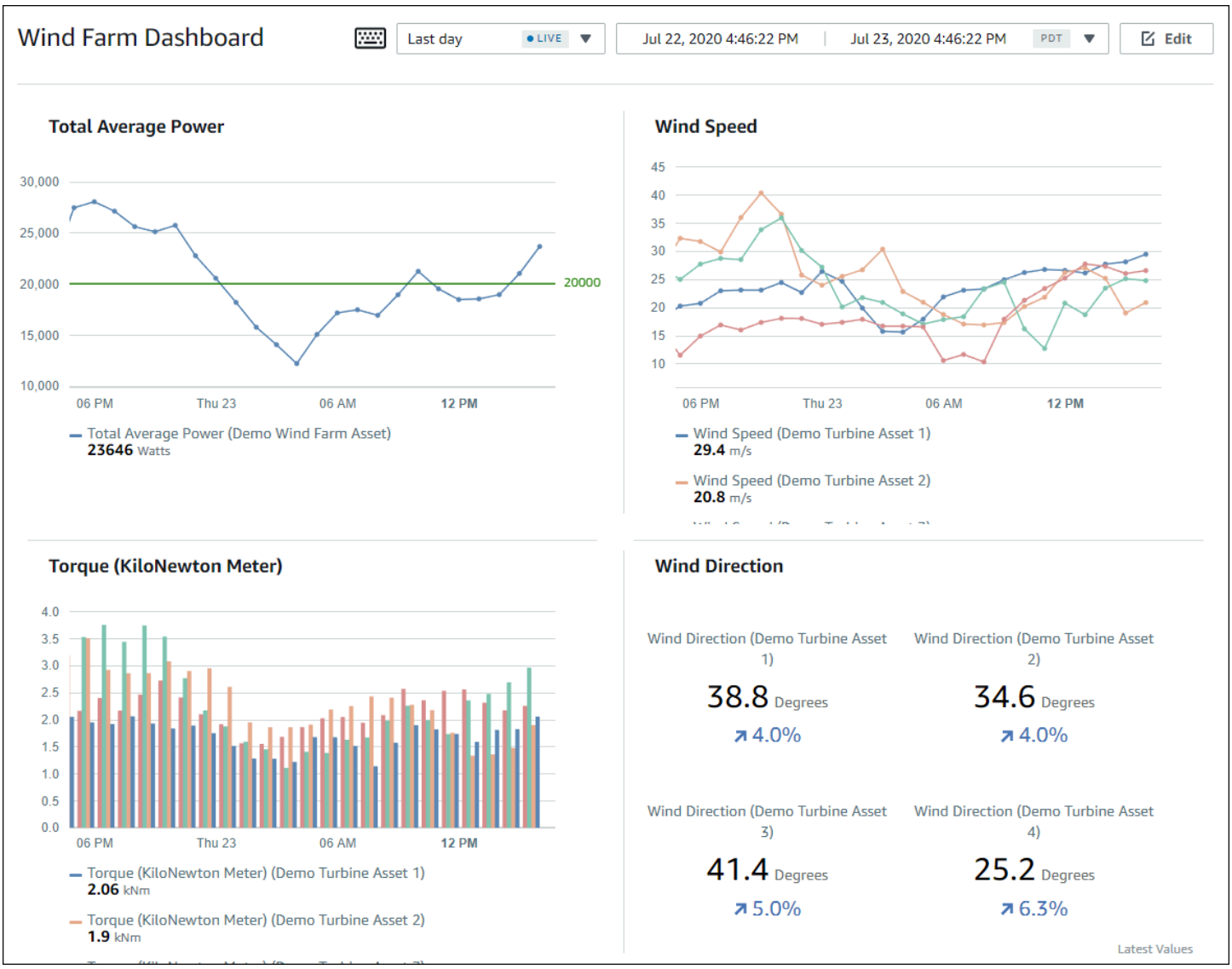
Para obtener más información acerca de otras formas de ingerir datos, consulte Ingerir datos para AWS IoT SiteWise.

Monitorización de datos con AWS IoT SiteWise Monitor

Puede utilizarlos AWS IoT SiteWise para supervisar los datos de sus procesos, dispositivos y equipos mediante la creación de portales web de SiteWise Monitor. SiteWise Monitor es una función AWS IoT SiteWise que puede utilizar para crear portales en forma de una aplicación web gestionada. A continuación, puede utilizar estos portales para ver y compartir sus datos operativos. Puede crear proyectos con paneles para visualizar datos de los procesos, dispositivos y equipos a los que están conectados AWS IoT.

Los expertos de dominio, como los ingenieros de procesos, pueden utilizar estos portales para obtener rápidamente información sobre sus datos operativos y comprender el comportamiento de los dispositivos y equipos.

A continuación se muestra un tablero de instrumentos de ejemplo que muestra los datos de un conjunto de molinos eólicos.



Como AWS IoT SiteWise captura datos a lo largo del tiempo, puede usar SiteWise Monitor para ver los datos operativos a lo largo del tiempo o los últimos valores informados en momentos específicos. Esto le permite descubrir ideas que de otro modo podrían ser difíciles de encontrar.

SiteWise Supervise las funciones

Cuatro funciones interactúan con SiteWise Monitor:

AWS administrador

El AWS administrador usa la AWS IoT SiteWise consola para crear portales. El administrador de AWS también puede asignar administradores del portal y agregar usuarios del portal.

Posteriormente, los administradores del portal asignan usuarios del portal a proyectos como propietarios o lectores. El AWS administrador trabaja exclusivamente en la AWS consola.

Administrador del portal

Cada portal de SiteWise Monitor tiene uno o más administradores de portal. Los administradores del portal utilizan el portal para crear proyectos que contengan recopilaciones de activos y paneles. A continuación, el administrador del portal asigna activos y propietarios a cada proyecto. Al controlar el acceso al proyecto, los administradores del portal especifican los activos que los propietarios y observadores de proyectos pueden ver.

Propietario del proyecto

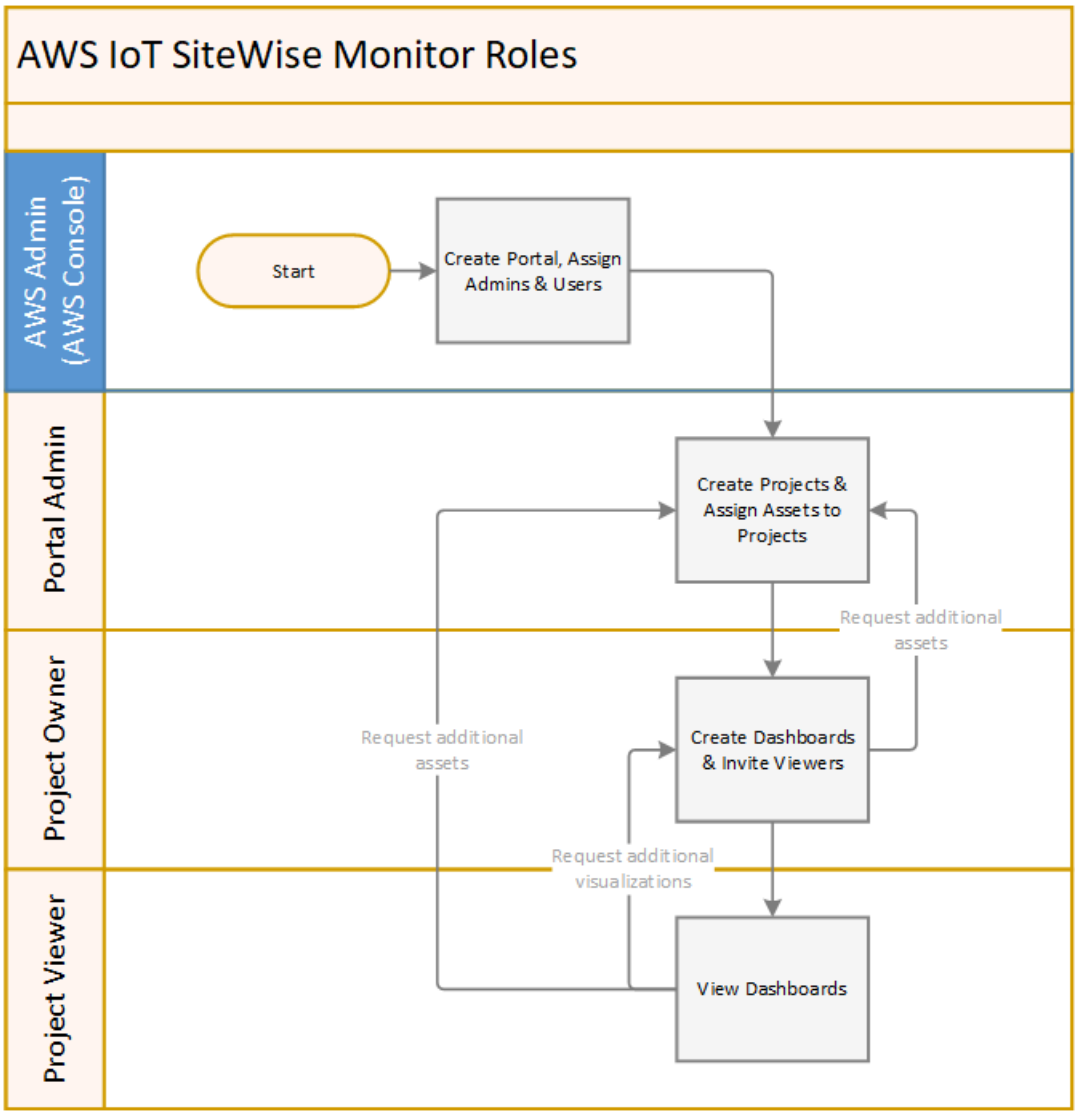
Cada proyecto de SiteWise Monitor tiene propietarios. Los propietarios de proyectos crean visualizaciones en forma de paneles para representar los datos operativos de manera coherente. Cuando los paneles están listos para compartirse, el propietario del proyecto puede invitar a lectores al proyecto. Los propietarios de proyectos también pueden asignar otros propietarios al proyecto. Los propietarios del proyecto pueden configurar los umbrales y los ajustes de notificación de las alarmas.

Observador de proyectos

Cada proyecto de SiteWise Monitor tiene visores. Los observadores de proyectos pueden conectarse al portal para ver los paneles creados por los propietarios de proyectos. En cada panel de control, los observadores de proyectos pueden ajustar el intervalo de tiempo para comprender mejor los datos operativos. Los observadores de proyectos solo pueden ver los paneles de los proyectos a los que tienen acceso. Los observadores de proyectos pueden confirmar y posponer alarmas.

En función de la organización, la misma persona puede desempeñar varios roles.

La siguiente imagen ilustra cómo interactúan estas cuatro funciones en el portal SiteWise Monitor.



Puede administrar quién tiene acceso a sus datos utilizando AWS IAM Identity Center o IAM. Sus usuarios de datos pueden iniciar sesión en SiteWise Monitor desde un navegador de escritorio o móvil con sus credenciales de IAM Identity Center o de IAM.

Federación de SAML

El Centro de identidades de IAM y IAM admiten la federación de identidades con SAML (lenguaje de marcado de aserción de seguridad) 2.0. SAML 2.0 es un estándar abierto que utilizan muchos proveedores de identidad externos (IdPs) para autenticar a los usuarios y transmitir su información de identidad y seguridad a los proveedores de servicios (SP). Los SP suelen ser aplicaciones o servicios. La federación SAML permite a los administradores y usuarios del portal SiteWise Monitor iniciar sesión en los portales asignados con credenciales externas, como sus nombres de usuario y contraseñas corporativos.

Puede configurar IAM Identity Center e IAM para que utilicen una federación basada en SAML para acceder a sus portales de Monitor. SiteWise

IAM Identity Center

Los administradores y usuarios del portal pueden iniciar sesión en el portal de AWS acceso con sus nombres de usuario y contraseñas corporativos. A continuación, pueden navegar hasta los portales de SiteWise Monitor que tengan asignados. El Centro de Identidad de IAM utiliza certificados para establecer una relación de confianza SAML entre su proveedor de identidad y. AWS Para obtener más información, consulte Implementación del perfil SCIM y de SAML 2.0 en la Guía del usuario de AWS IAM Identity Center .

IAM

Los administradores y usuarios del portal pueden solicitar credenciales de seguridad temporales para acceder a los portales de SiteWise Monitor asignados. Debe crear una identidad de proveedor de identidades SAML en IAM para establecer una relación de confianza entre su proveedor de identidades y. AWSPara obtener más información, consulte Uso de la federación basada en SAML para el acceso mediante API AWS, en la Guía del usuario de IAM.

Los administradores y usuarios del portal pueden iniciar sesión en el portal de su empresa y seleccionar la opción de ir a la AWS consola de administración. A continuación, pueden navegar hasta los portales de SiteWise Monitor que tengan asignados. El portal de su empresa gestiona el intercambio de confianza entre su proveedor de identidad y AWS. Para obtener más información, consulte Permitir que los usuarios federados de SAML 2.0 accedan a la consola de AWS administración en la Guía del usuario de IAM.

> **Note**
>
> Al añadir usuarios o administradores al portal, evite crear políticas de IAM que restrinjan los permisos de los usuarios, como IP limitada. Las políticas adjuntas con permisos restringidos no podrán conectarse al portal. AWS IoT SiteWise

SiteWise Conceptos de monitoreo

Para utilizar SiteWise Monitor, debe estar familiarizado con los siguientes conceptos:

Portal

Un AWS IoT SiteWise Monitor portal es una aplicación web que puede utilizar para visualizar y compartir sus AWS IoT SiteWise datos. Un portal tiene uno o varios administradores y contiene cero o más proyectos.

Proyecto

Cada portal de SiteWise Monitor contiene un conjunto de proyectos. Cada proyecto tiene un subconjunto de sus activos de AWS IoT SiteWise asociados al mismo. Los propietarios de proyectos crean uno o varios paneles para proporcionar una forma coherente de ver los datos asociados a esos activos. Los propietarios del proyecto pueden invitar a los lectores al proyecto para permitirles ver los activos y paneles del proyecto. El proyecto es la unidad básica para compartir en SiteWise Monitor. Los propietarios del proyecto pueden invitar a los usuarios a los que el AWS administrador les dio acceso al portal. Un usuario debe tener acceso a un portal antes de que un proyecto de ese portal pueda compartirse con ese usuario.

activo

Cuando se ingieren datos AWS IoT SiteWise de su equipo industrial, cada uno de sus dispositivos, equipos y procesos se representa como activos. Cada activo tiene propiedades y alarmas asociadas al mismo. El administrador del portal asigna conjuntos de activos a cada proyecto.

Propiedad

Las propiedades son datos de serie temporal asociados a los activos. Por ejemplo, un equipo podría tener un número de serie, una ubicación, una marca y un modelo y una fecha de instalación. También puede tener valores de series temporales para disponibilidad, rendimiento, calidad, temperatura, presión, etc.

Alarma

Las alarmas monitorean las propiedades para identificar cuando el equipo está fuera de su rango de operación. Cada alarma define un umbral y una propiedad por monitorear. Cuando la propiedad supera el umbral, la alarma se activa e indica que usted o alguien de su equipo debe ocuparse del problema. Los propietarios de proyectos pueden personalizar los umbrales y los ajustes de notificación de las alarmas. Los observadores de proyectos pueden confirmar y posponer las alarmas y pueden dejar un mensaje con detalles sobre la alarma o la acción que realizaron para solucionarla.

Panel de control

Cada proyecto contiene un conjunto de paneles. Los paneles proporcionan un conjunto de visualizaciones para los valores de un conjunto de activos. Los propietarios de proyectos crean los paneles y las visualizaciones que contiene. Cuando un propietario de proyecto está listo para compartir el conjunto de paneles, el propietario puede invitar a observadores al proyecto, lo que les da acceso a todos los paneles del mismo. Si desea un conjunto distinto de observadores para distintos paneles, debe dividir los paneles entre proyectos. Cuando los espectadores miran los paneles, pueden personalizar el intervalo de tiempo para ver datos específicos.

Visualización

En cada panel de control, los propietarios de proyectos deciden cómo mostrar las propiedades y alarmas de los activos asociados al proyecto. La disponibilidad se podría representar como un gráfico de líneas, mientras que otros valores se podrían mostrar como gráficos de barras o indicadores clave de rendimiento (KPI). Las alarmas se visualizan mejor como cuadrículas de estado y líneas temporales de estado. Los propietarios de proyectos personalizan cada visualización para ofrecer la mejor comprensión de los datos de ese activo.

Empezar con AWS IoT SiteWise Monitor

Si es el AWS administrador de su organización, puede crear portales desde la AWS IoT SiteWise consola. Complete los siguientes pasos para crear un portal para que los miembros de su organización puedan ver sus AWS IoT SiteWise datos:

1. Configure y cree un portal
2. Agregar administradores del portal y enviar correos electrónicos de invitación
3. Agregar usuarios al portal

Tras crear un portal, el administrador del portal puede ver sus AWS IoT SiteWise activos y asignarlos a los proyectos del portal. Los propietarios de proyectos pueden crear paneles para visualizar las propiedades de los activos que ayudan a los observadores de proyectos a comprender el rendimiento de sus dispositivos, procesos y equipos.

> **Note**
>
> Al añadir usuarios o administradores al portal, evite crear políticas AWS Identity and Access Management (de IAM) que restrinjan los permisos de los usuarios, como una IP limitada.

Las políticas adjuntas con permisos restringidos no podrán conectarse al AWS IoT SiteWise portal.

Puede seguir un tutorial que recorra los pasos necesarios para configurar un portal con un proyecto, paneles y varios usuarios para un escenario específico utilizando datos de parques eólicos. Para obtener más información, consulte Visualización y uso compartido de datos de parques eólicos en Monitor SiteWise .

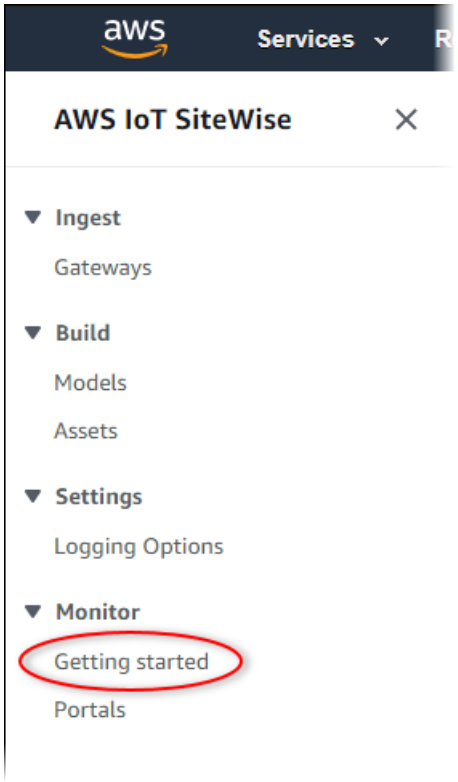
Temas

Creación de un portal

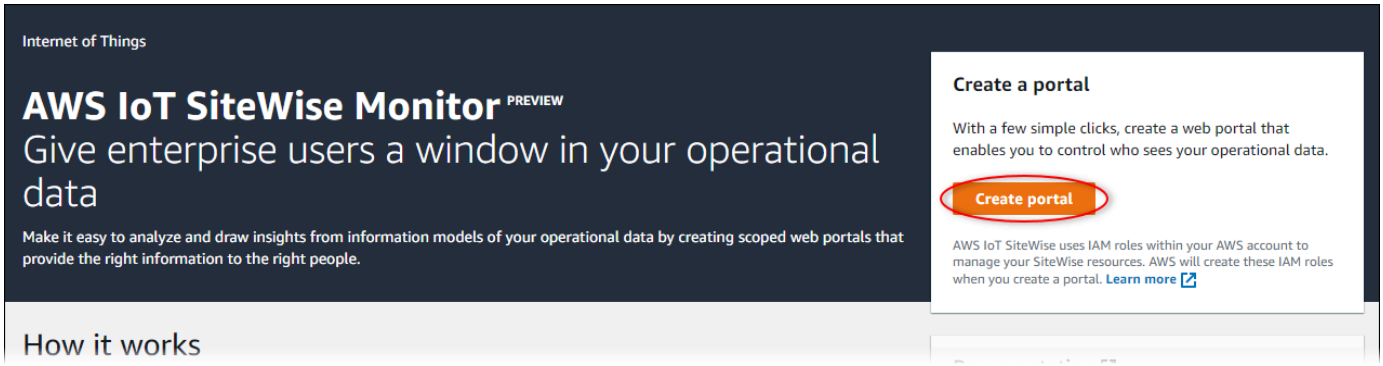
El portal SiteWise Monitor se crea en la AWS IoT SiteWise consola.

Para crear un portal

1. Inicie sesión en la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Monitor, luego Introducción.



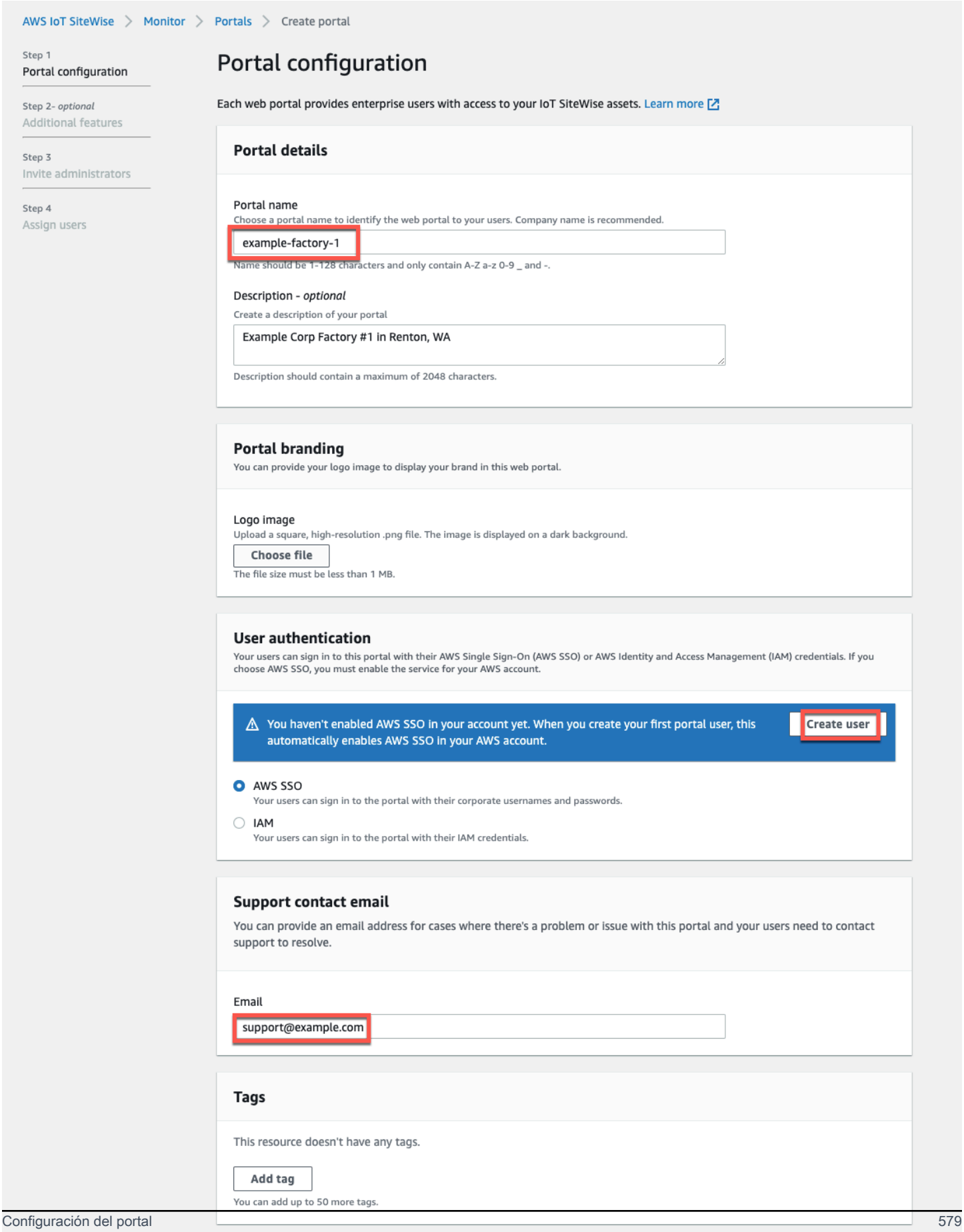
3. Elija Crear portal.



A continuación, debe proporcionar información básica para configurar el portal.

Configuración del portal

Sus usuarios utilizan los portales para ver sus datos. Puede personalizar el nombre, la descripción, la marca, la autenticación de usuario, el correo electrónico de contacto de asistencia y los permisos de un portal.


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

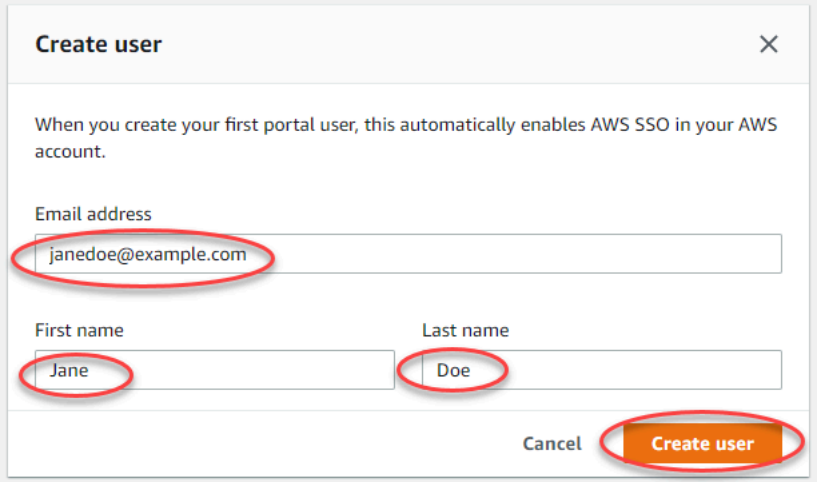
Para configurar un portal

1. Escriba un nombre para el portal.
2. (Opcional) Escriba una descripción para el portal. Si tiene varios portales, utilice descripciones significativas para ayudarle a realizar un seguimiento de lo que contiene cada portal.
3. (Opcional) Suba una imagen para mostrar su marca en el portal. Elija una imagen PNG cuadrada. Si carga una imagen no cuadrada, el portal escala la imagen a un cuadrado.
4. Seleccione una de las siguientes opciones:
   - Elija Centro de identidades de IAM si los usuarios de su portal inician sesión en este portal con sus nombres de usuario y contraseñas corporativos.

     Si no ha habilitado el Centro de identidades de IAM en su cuenta, haga lo siguiente:

     a. Seleccione la opción Crear usuario.

     b. En la página Crear usuario, para crear el primer portal, introduzca la dirección de correo electrónico, nombre y apellido del usuario y, a continuación, seleccione Crear usuario.



> **Note**
>
> - AWS habilita automáticamente el Centro de Identidad de IAM en su cuenta al crear el primer usuario del portal.
> - Solo puede configurar el Centro de identidades de IAM en una región a la vez. SiteWise El monitor se conecta a la región que configuró para el IAM Identity Center. Esto significa que utiliza una región para el acceso al Centro de identidades de IAM, pero puede crear portales en cualquier región.

- Elija IAM si los usuarios de su portal inician sesión en este portal con sus credenciales de IAM.

> **Important**
>
> Los usuarios o roles deben tener el permiso de `iotsitewise:DescribePortal` para iniciar sesión en el portal.

5. Introduzca una dirección de correo electrónico con la que los usuarios del portal puedan ponerse en contacto cuando tengan un problema con el portal y necesiten ayuda para resolverlo.
6. (Opcional) Agregue etiquetas para su portal. Para obtener más información, consulte Etiquetar sus recursos AWS IoT SiteWise.
7. Seleccione una de las siguientes opciones:

   - Elija Crear y utilizar un nuevo rol de servicio. De forma predeterminada, SiteWise Monitor crea automáticamente un rol de servicio para cada portal. Esta función permite a los usuarios del portal acceder a sus AWS IoT SiteWise recursos. Para obtener más información, consulte Uso de funciones de servicio para AWS IoT SiteWise Monitor.
   - Elija Utilizar un rol de servicio existente y, a continuación, el rol deseado.
8. Seleccione Siguiente
9. (Opcional) Habilite alarmas para su portal. Para obtener más información, consulte Habilitación de alarmas para sus portales.
10. Elija Crear. AWS IoT SiteWise creará tu portal.

> **Note**
>
> Si cierra la consola, puede finalizar el proceso de instalación agregando administradores y usuarios. Para obtener más información, consulte Agregar o quitar administradores del portal. Si no desea conservar este portal, elimínelo para que no consuma recursos. Para obtener más información, consulte Eliminación de un portal.

La columna Estado puede adoptar uno de los siguientes valores.

- CREATING - AWS IoT SiteWise está procesando su solicitud para crear el portal. Este proceso puede tardar varios minutos en completarse.
- ACTUALIZAR - AWS IoT SiteWise está procesando su solicitud de actualización del portal. Este proceso puede tardar varios minutos en completarse.
- PENDIENTE - AWS IoT SiteWise está esperando a que finalice la propagación del registro DNS. Este proceso puede tardar varios minutos en completarse. Durante el estado PENDIENTE puede eliminar el portal.
- ELIMINAR - AWS IoT SiteWise está procesando su solicitud de eliminación del portal. Este proceso puede tardar varios minutos en completarse.
- ACTIVO: cuando el portal se activa, los usuarios de su portal tienen acceso al mismo.
- ERROR: no se ha AWS IoT SiteWise podido procesar su solicitud de creación, actualización o eliminación del portal. Si has habilitado AWS IoT SiteWise el envío de registros a Amazon CloudWatch Logs, puedes usar estos registros para solucionar problemas. Para obtener más información, consulte Supervisión AWS IoT SiteWise con CloudWatch registros.

Aparece un mensaje cuando se crea el portal.

A continuación, debe invitar a uno o más administradores del portal al portal. Hasta ahora, ha creado un portal pero nadie puede acceder a él.

Invitación de administradores

Para comenzar en el nuevo portal, debe asignar un administrador del portal. El administrador del portal crea proyectos, elige los propietarios de proyectos y asigna activos a los proyectos. Los administradores del portal pueden ver todos sus AWS IoT SiteWise activos.

En función del servicio de autenticación de usuarios, elija una de las siguientes opciones:

IAM Identity Center

Si es la primera vez que utiliza SiteWise Monitor, puede elegir al usuario que creó anteriormente como administrador del portal. Si desea añadir otro usuario como administrador del portal, puede crear un usuario del Centro de identidades de IAM desde esta página. Si lo desea, puede conectar un proveedor de identidades externo al Centro de identidades de IAM. Para más información, consulte la Guía del usuario de AWS IAM Identity Center.

Para invitar a administradores

1. Active las casillas de verificación de los usuarios que quiera que sean administradores del portal. Esto añade los usuarios a la lista de Administradores del portal.

   > **Note**
   >
   > Si utiliza el Centro de identidades de IAM como almacén de identidades y ha iniciado sesión en su cuenta de administración de AWS Organizations , puede elegir Crear usuario para crear un usuario del Centro de identidades de IAM. El Centro de identidades de IAM enviará al nuevo usuario un correo electrónico para que establezca su contraseña. A continuación, puede asignar el usuario al portal como administrador. Para obtener más información, consulte Administrar identidades en el IAM Identity Center.

2. (Opcional) Elija Enviar invitación a los usuarios seleccionados. Se abrirá el cliente de correo electrónico y se rellenará una invitación en el cuerpo del mensaje.

   Puede personalizar el correo electrónico antes de enviarlo a los administradores del portal. También puede enviar el correo electrónico a los administradores de su portal más tarde. Si es la primera vez que prueba SiteWise Monitor y añade su nuevo usuario o rol del Centro de Identidad de IAM o de IAM como administrador del portal, no necesita enviarse un correo electrónico.

3. Si añade un usuario que no desea como administrador, desactive la casilla de verificación correspondiente a ese usuario.

4. Cuando haya terminado de invitar a los administradores del portal, seleccione Siguiente.

IAM

Puede elegir un usuario o rol para que sea el administrador del portal. Si desea añadir otro usuario o rol como administrador del portal, puede crear un usuario o rol en la consola de IAM. Para obtener más información, consulte Creación de un usuario de IAM en su cuenta de AWS y Creación de roles de IAM en la Guía del usuario de IAM.

Para invitar a administradores

1. Haga lo siguiente:

- Elija Usuarios de IAM para añadir un usuario de IAM como administrador de su portal.
- Elija Roles de IAM para añadir un rol de IAM como administrador de su portal.

2. Marque las casillas de verificación de los usuarios o roles que desee como administradores de su portal. Esto añade los usuarios o roles a la lista de Administradores del portal.
3. Si añade un usuario o rol que no desea como administrador, desmarque la casilla de verificación correspondiente a ese usuario o rol.
4. Cuando haya terminado de invitar a los administradores del portal, seleccione Siguiente.

> **Important**
>
> Los usuarios o roles deben tener el permiso de `iotsitewise:DescribePortal` para iniciar sesión en el portal.

> **Note**
>
> Si utiliza el Centro de identidades de IAM como almacén de identidades y ha iniciado sesión en su cuenta de administración de AWS Organizations , puede elegir Crear usuario para crear un usuario del Centro de identidades de IAM. El Centro de identidades de IAM enviará al nuevo usuario un correo electrónico para que establezca su contraseña. A continuación, puede asignar el usuario al portal como administrador. Para obtener más información, consulte Administrar identidades en el IAM Identity Center.

Puede cambiar la lista de administradores del portal más adelante. Para obtener más información, consulte Agregar o quitar administradores del portal.

> **Note**
>
> Dado que solo un administrador del portal puede crear proyectos y asignarles activos, debe especificar al menos un único administrador del portal.

Como último paso, añada usuarios que pueden acceder al nuevo portal.

Agregar usuarios al portal

Puede controlar qué usuarios tienen acceso a sus portales. En cada portal, los administradores del portal crean uno o varios proyectos y asignan usuarios del portal como propietarios o lectores para cada proyecto. Cada propietario del proyecto puede invitar a usuarios adicionales del portal para que sean propietarios del proyecto o lo vean.

En función del servicio de autenticación de usuarios, elija una de las siguientes opciones:

IAM Identity Center

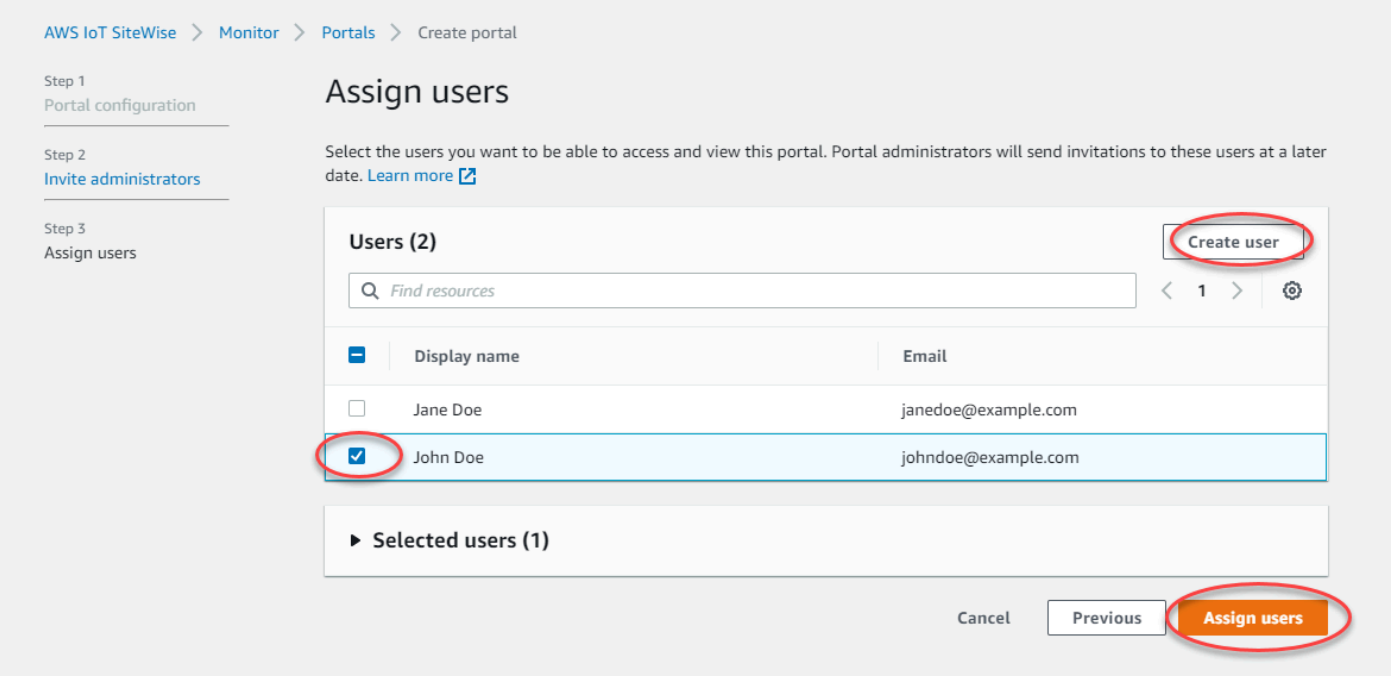
Si desea añadir un usuario a la lista Usuarios, realice los pasos siguientes.

Para añadir usuarios del portal

1. Elija usuarios en la lista Usuarios para añadirlos al portal. Esto añade los usuarios a la lista Usuarios del portal. Si es la primera vez que utiliza SiteWise Monitor, no necesita añadir al administrador del portal como usuario del portal.

   > **Note**
   >
   > Si utiliza el Centro de identidades de IAM como almacén de identidades y ha iniciado sesión en su cuenta de administración de AWS Organizations , puede elegir Crear usuario para crear un usuario del Centro de identidades de IAM. El Centro de identidades de IAM enviará al nuevo usuario un correo electrónico para que establezca su contraseña. A continuación, puede asignar el usuario al portal como usuario. Para obtener más información, consulte Administrar identidades en el IAM Identity Center.

2. Si añade un usuario al que no desea tener acceso al portal, desactive la casilla de verificación correspondiente.
3. Cuando haya terminado de seleccionar los usuarios, elija Asignar usuarios.



IAM

Si ve al usuario o rol que desea añadir en la lista Usuarios de IAM o Roles de IAM, complete los pasos siguientes.

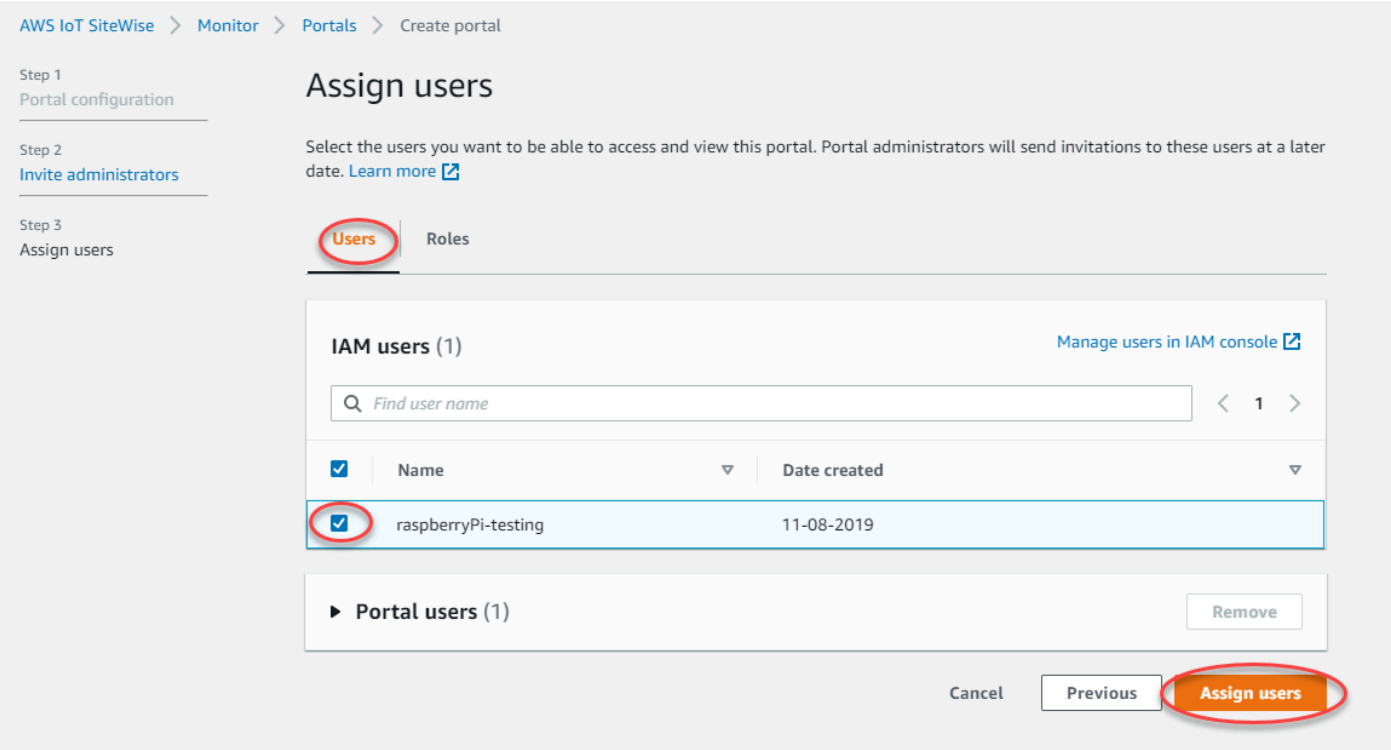
Para añadir usuarios del portal

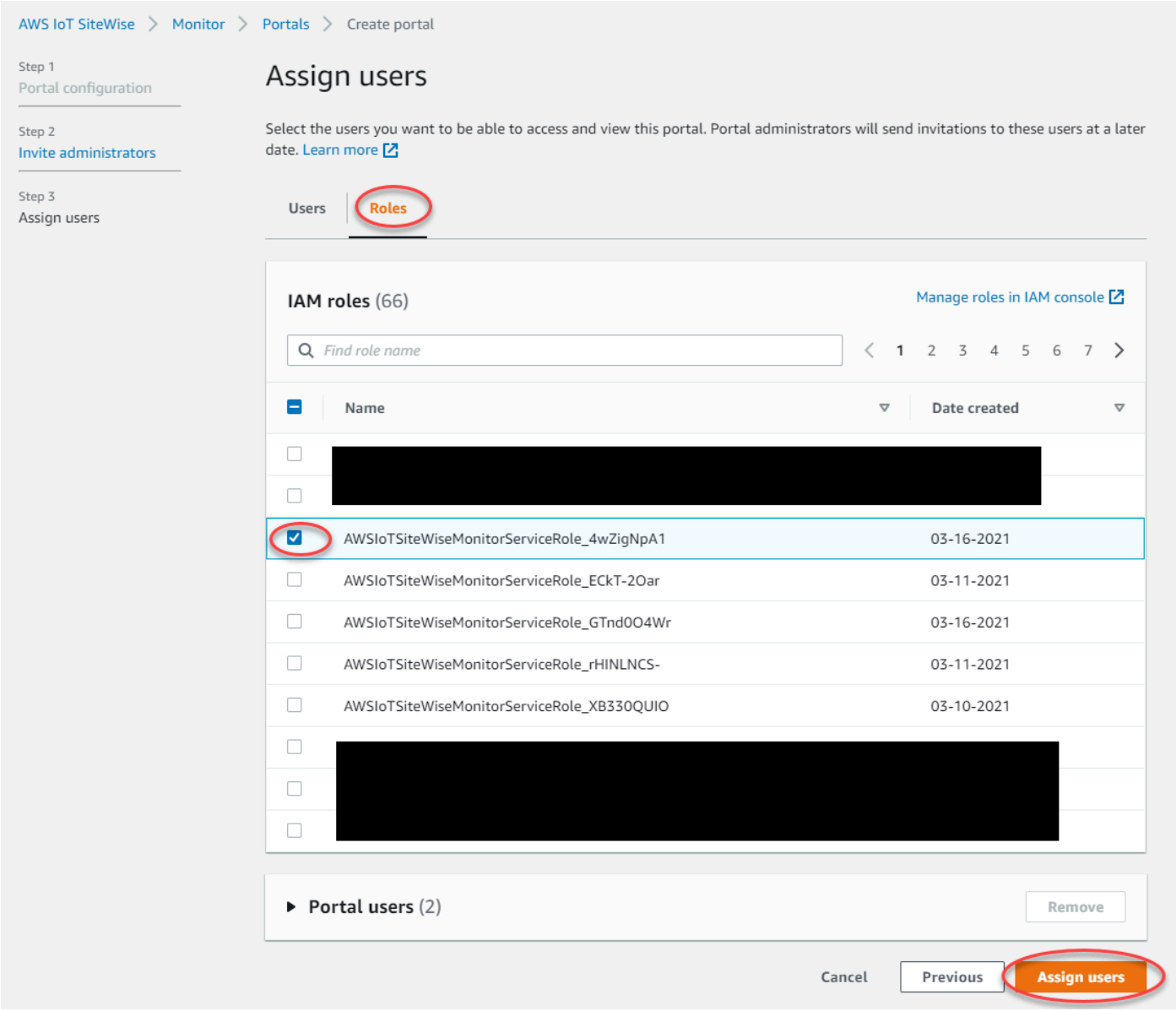
1. Realice las siguientes opciones:

   - Elija Usuarios de IAM para añadir un usuario de IAM como usuario del portal.
   - Elija Roles de IAM para añadir un rol de IAM como usuario de portal.

   Si es la primera vez que usa SiteWise Monitor, no necesita agregar al administrador del portal como usuario del portal.
2. Marque las casillas de verificación de los usuarios o roles que desee como usuarios del portal. Esto añade los usuarios o roles a la lista Usuarios del portal.
3. Si añade un usuario al que no desea tener acceso al portal, desactive la casilla de verificación correspondiente.
4. Cuando haya terminado de seleccionar los usuarios, elija Asignar usuarios.

> **Important**
>
> Los usuarios o roles deben tener el permiso de `iotsitewise:DescribePortal` para iniciar sesión en el portal.





¡Enhorabuena! Ha creado correctamente un portal y ha asignado administradores de portal y usuarios que pueden utilizar ese portal cuando se les invite a hacerlo. Los administradores del portal ahora pueden crear proyectos y agregar activos a esos proyectos. A continuación, los propietarios del proyecto pueden crear paneles para visualizar los datos de los activos de cada proyecto.

Puede cambiar la lista de usuarios del portal más adelante. Para obtener más información, consulte Agregar o quitar usuarios del portal.

Si necesita realizar cambios en el portal, consulte Administrar sus portales de SiteWise Monitor.

Para empezar a usar el portal, consulte Primeros pasos en la Guía de aplicaciones de SiteWise Monitor.

Creación de paneles de control (AWS Command Line Interface)

Al definir visualizaciones (o widgets) en paneles mediante la AWS CLI, debe especificar la siguiente información en el documento JSON `dashboardDefinition`. Esta definición es un parámetro de las UpdateDashboardoperaciones CreateDashboardy.

`widgets`

Llista de estructuras de definición de widgets que contiene cada una la siguiente información:

`type`

Tipo de widget. AWS IoT SiteWise proporciona los siguientes tipos de widget:

- `sc-line-chart`: un gráfico de líneas. Para obtener más información, consulte Gráficos de líneas en la Guía de la aplicación AWS IoT SiteWise Monitor.
- `sc-scatter-chart`: un gráfico de dispersión. Para obtener más información, consulte Gráficos de dispersión en la Guía de la aplicación AWS IoT SiteWise Monitor.
- `sc-bar-chart`: un gráfico de barras. Para obtener más información, consulte Gráficos de barras en la Guía de la aplicación AWS IoT SiteWise Monitor.
- `sc-status-grid`: un widget de estado que muestra el último valor de las propiedades de recursos en forma de cuadrícula. Para obtener más información, consulte Widgets de estado en la Guía de la aplicación AWS IoT SiteWise Monitor.
- `sc-status-timeline`: un widget de estado que muestra los valores históricos de las propiedades de recursos como línea temporal. Para obtener más información, consulte Widgets de estado en la Guía de la aplicación AWS IoT SiteWise Monitor.
- `sc-kpi`: una visualización de indicadores clave de rendimiento (KPI). Para obtener más información, consulte Widgets de KP en la Guía de la aplicación AWS IoT SiteWise Monitor.
- `sc-table`: un widget de tabla. Para obtener más información, consulte Widgets de tabla en la Guía de la aplicación AWS IoT SiteWise Monitor.

`title`

Título del widget.

`x`

Posición horizontal del widget, comenzando desde la izquierda de la cuadrícula. Este valor se refiere a la posición del widget en la cuadrícula del panel.

`y`

Posición vertical del widget, comenzando desde la parte superior de la cuadrícula. Este valor se refiere a la posición del widget en la cuadrícula del panel.

`width`

Anchura del widget, expresada en número de espacios en la cuadrícula del panel.

`height`

Altura del widget, expresada en número de espacios en la cuadrícula del panel.

`metrics`

Lista de estructuras métricas que definan cada una un flujo de datos para este widget. Cada estructura de la lista debe contener la siguiente información:

`label`

Etiqueta que se mostrará para esta métrica.

`type`

Tipo de origen de datos para esta métrica. AWS IoT SiteWise proporciona los siguientes tipos de métrica:

- `iotsitewise`: el panel de control obtiene datos de una propiedad de recurso en AWS IoT SiteWise. Si elige esta opción, deberá definir `assetId` y `propertyId` para esta métrica.

`assetId`

(Opcional) ID de un activo en AWS IoT SiteWise.

Este campo es obligatorio si elige `iotsitewise` para `type` en esta métrica.

`propertyId`

(Opcional) ID de una propiedad de activo en AWS IoT SiteWise.

Este campo es obligatorio si elige `iotsitewise` para `type` en esta métrica.

`analysis`

(Opcional) Una estructura que define el análisis, como líneas de tendencia, que se mostrará para el widget. Para obtener más información, consulte Configuración de líneas de tendencia en la Guía de la aplicación AWS IoT SiteWise Monitor. Puede añadir una línea de tendencia de cada tipo por propiedad en el widget. La estructura de análisis contiene la siguiente información:

`trends`

(Opcional) Lista de estructuras de tendencia que definan cada una un análisis de tendencia para este widget. Cada estructura de la lista contiene la siguiente información:

`type`

El tipo de línea de tendencia. Elija la opción siguiente:

- `linear-regression`— Mostrar una línea de regresión lineal. SiteWise El monitor utiliza el método de mínimos cuadrados para calcular la regresión lineal.

`annotations`

(Opcional) Una estructura de anotaciones que define umbrales para el widget. Para obtener más información, consulte Configuración de umbrales en la Guía de la aplicación AWS IoT SiteWise Monitor. Puede añadir hasta seis anotaciones por widget. La estructura de anotación contiene la siguiente información:

`y`

(Opcional) Lista de estructuras de anotación que definan cada una un umbral horizontal para este widget. Cada estructura de la lista contiene la siguiente información:

`comparisonOperator`

El operador de comparación para el umbral. Seleccione una de las siguientes opciones:

- `LT`: resalta las propiedades que tienen al menos un punto de datos menor que `value`.
- `GT`: resalta las propiedades que tienen al menos un punto de datos mayor que `value`.
- `LTE`: resalta las propiedades que tienen al menos un punto de datos menor o igual que `value`.

- `GTE`: resalta las propiedades que tienen al menos un punto de datos mayor o igual que `value`.
- `EQ`: Resalta las propiedades que tienen al menos un punto de datos igual que `value`.

`value`

El valor de umbral para comparar los puntos de datos con `comparisonOperator`.

`color`

(Opcional) El código hexadecimal de 6 dígitos del color del umbral. La visualización muestra leyendas de propiedades en este color para las propiedades con al menos un punto de datos que cumpla la regla de umbral. De forma predeterminada es negro (`#000000`).

`showValue`

(Opcional) Mostrar o no el valor del umbral en los márgenes del widget. El valor predeterminado es `true`.

`properties`

(Opcional) Un diccionario plano de propiedades para el widget. Los miembros de esta estructura dependen del contexto. AWS IoT SiteWise proporciona los siguientes widgets que utilizan `properties`:

- Los Gráficos de líneas, Gráficos de dispersión, y Gráficos de barras tienen la siguiente propiedad:

  `colorDataAcrossThresholds`

  (Opcional) Cambiar o no el color de los datos que cruzan los umbrales en este widget. Al habilitar esta opción, los datos que cruzan un umbral aparecen en el color que usted elija. El valor predeterminado es `true`.

- Las cuadrículas de estado tienen la siguiente propiedad:

  `labels`

  (Opcional) Una estructura que defina las etiquetas que se mostrarán en la cuadrícula de estado. La estructura de etiquetas contiene la siguiente información:

  `showValue`

  (Opcional) Mostrar o no la unidad y el valor de cada propiedad de recurso en este widget. El valor predeterminado es `true`.

Example Ejemplo de definición de panel

En el ejemplo siguiente se define un panel a partir de una carga almacenada en un archivo JSON.

```
aws iotsitewise create-dashboard \
  --project-id a1b2c3d4-5678-90ab-cdef-eeeeeEXAMPLE \
  --dashboard-name "Wind Farm Dashboard" \
  --dashboard-definition file://dashboard-definition.json
```

El siguiente ejemplo JSON para `dashboard-definition.json` define un panel con los siguientes widgets de visualización:

- Un gráfico de líneas que muestra la energía eólica total en la parte superior izquierda del panel. Este gráfico de líneas incluye un umbral que indica cuándo el parque eólico produce menos energía que su producción mínima prevista. Este gráfico de líneas también incluye una línea de tendencia de regresión lineal.
- Un gráfico de barras que muestra la velocidad del viento de cuatro turbinas en la parte superior derecha del panel.

> **Note**
>
> Este ejemplo representa visualizaciones de gráficos de líneas y barras en un panel de control. Este panel es similar al ejemplo de panel de energía eólica.

```
{
  "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"
        }
      ]
    }
  ]
}
```

Habilitación de alarmas para sus portales

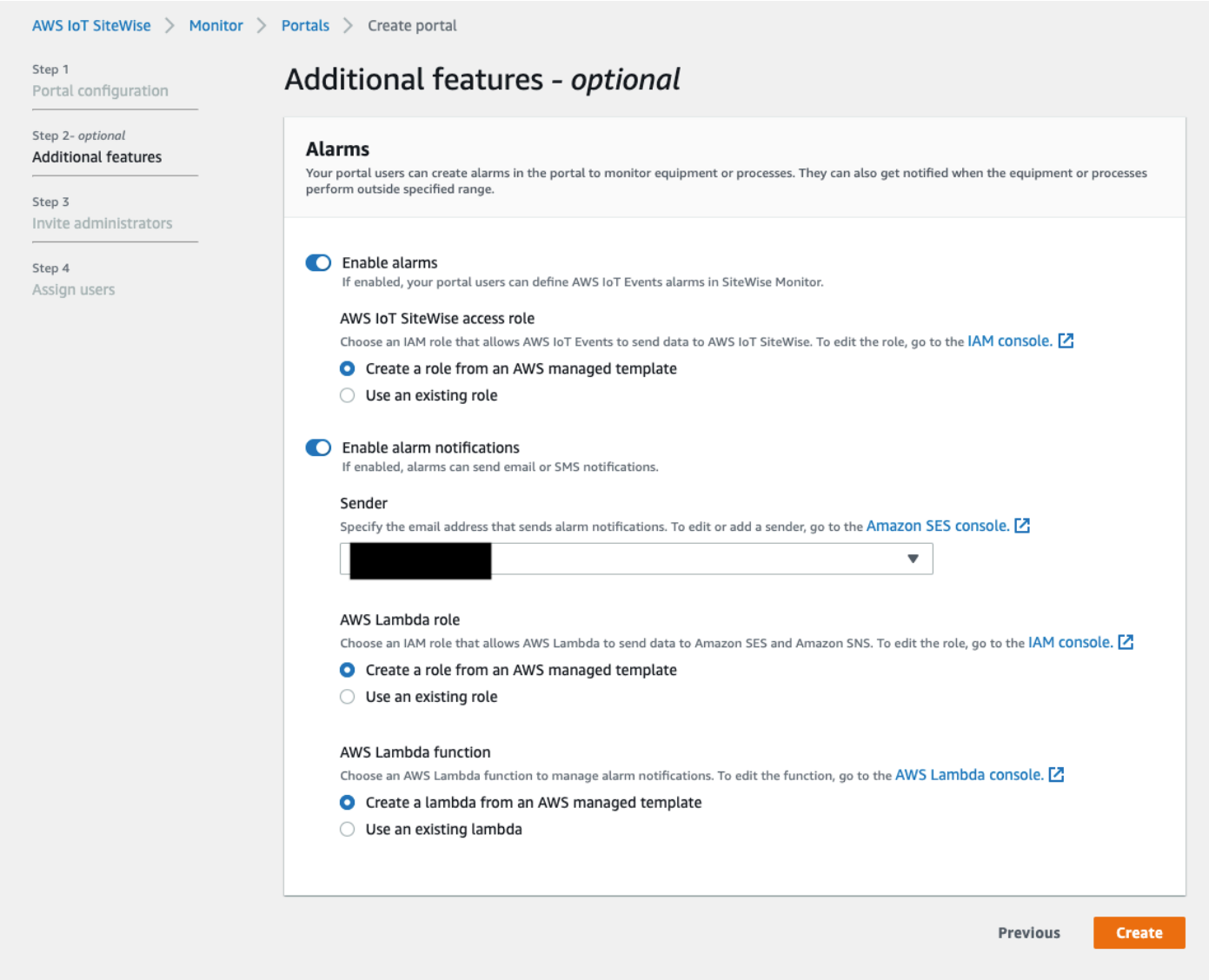
Puede habilitar la función de alarmas compatible con sus portales AWS IoT Events para que los administradores del portal puedan crear, editar y eliminar modelos de AWS IoT Events alarmas en sus portales de SiteWise Monitor. Los propietarios de proyectos pueden configurar alarmas. Los observadores de proyectos pueden ver los detalles de las alarmas. En esta sección se explica cómo puede utilizar la AWS IoT SiteWise consola para habilitar la función de alarmas en sus portales.

Important

- No puede crear alarmas externas en sus portales.
- Si desea enviar notificaciones de alarma, debe elegir el Centro de identidades de IAM para el servicio de autenticación de usuarios.
- La función de notificaciones de alarmas no está disponible en China (Pekín) Región de AWS.

Al configurar y crear un portal, puede habilitar las alarmas y las notificaciones de alarma en Paso 2 Características adicionales. En función del servicio de autenticación de usuarios, elija una de las siguientes opciones:

IAM Identity Center



Para habilitar alarmas para un portal

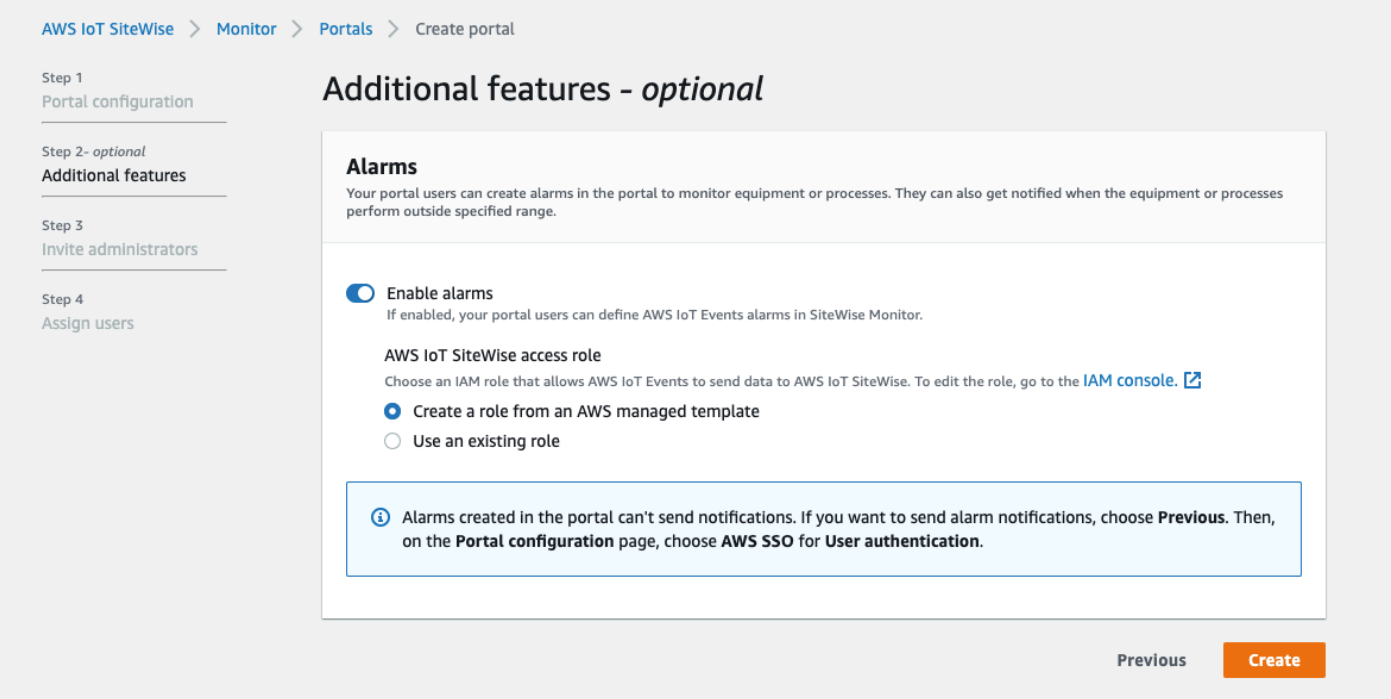
1. (Opcional) Seleccione Habilitar alarmas.
   - En Rol de acceso de AWS IoT SiteWise , utilice un rol existente o cree uno con los permisos necesarios. Este rol requiere el permiso `iotevents:BatchPutMessage` y una relación de confianza que permita a `iot.amazonaws.com` y `iotevents.amazonaws.com` asumir el rol.
2. (Opcional) Seleccione Habilitar notificaciones de alarma.
   a. En Remitente, elija el remitente.

> **Important**
>
> Debe verificar la dirección de correo electrónico del remitente en Amazon SES. Para obtener más información, consulte Verificación de direcciones de correo electrónico en Amazon SES, en la Guía para desarrolladores de Amazon Simple Email Service.

b. En Rol de AWS Lambda , utilice un rol existente o cree uno con los permisos necesarios. Este rol requiere los permisos `lambda:InvokeFunction` y `sso-directory:DescribeUser` y una relación de confianza que permita a `iotevents.amazonaws.com` y `lambda.amazonaws.com` asumir el rol.

c. En Funciones de AWS Lambda , elija una función de Lambda existente o cree una que administre las notificaciones de alarma. Para obtener más información, consulte Administración de notificaciones de alarma en la Guía para desarrolladores de AWS IoT Events .

IAM



Para habilitar alarmas para un portal

- (Opcional) Seleccione Habilitar alarmas.

- En Rol de acceso de AWS IoT SiteWise , utilice un rol existente o cree uno con los permisos necesarios. Este rol requiere el permiso `iotevents:BatchPutMessage` y una relación de confianza que permita a `iot.amazonaws.com` y `iotevents.amazonaws.com` asumir el rol.

Para obtener más información sobre las alarmas en SiteWise Monitor, consulte Supervisión con alarmas en la Guía de AWS IoT SiteWise aplicaciones.

Habilitación del portal en la periferia

Una vez que habilite su portal en el borde, este portal estará disponible en todas las puertas de enlace SiteWise Edge con el paquete de procesamiento de datos activado en su cuenta.

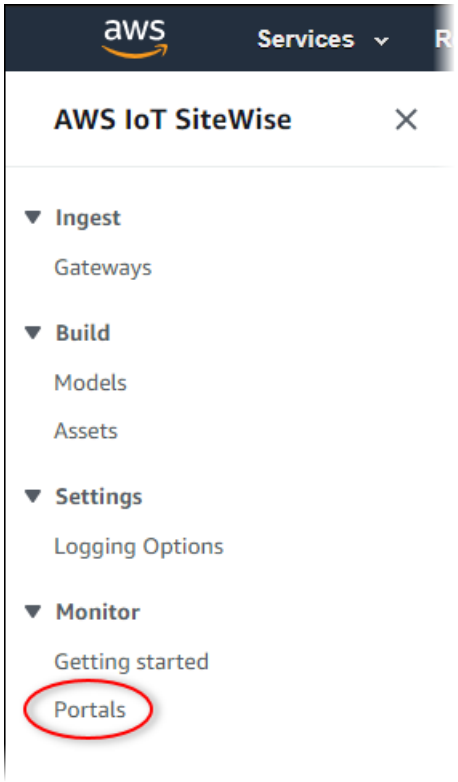
Para habilitar el portal en la periferia

1. En la sección Configuración de la periferia, active Habilitar este portal en la periferia.
2. Seleccione Crear.

Administrar sus portales de SiteWise Monitor

Es posible que deba actualizar los detalles del portal, cambiar de administrador o agregar usuarios a sus portales. En esta sección se explica cómo puede realizar estas tareas administrativas básicas para sus portales de SiteWise Monitor.

1. Inicie sesión en la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Monitor (Monitorizar), Portals (Portales).



3. Elija un portal y, a continuación, elija View details (Ver detalles) (o elija el Name (Nombre) del portal).
4. Puede realizar cualquiera de las siguientes tareas administrativas:

   - Cambio del nombre, la descripción, la marca, el email de soporte y los permisos de un portal
   - Agregar o quitar administradores del portal
   - Envío de invitaciones por correo electrónico a administradores del portal
   - Agregar o quitar usuarios del portal
   - Eliminación de un portal

Para obtener información sobre cómo crear un volumen, consulte Empezar con AWS IoT SiteWise Monitor.

Temas

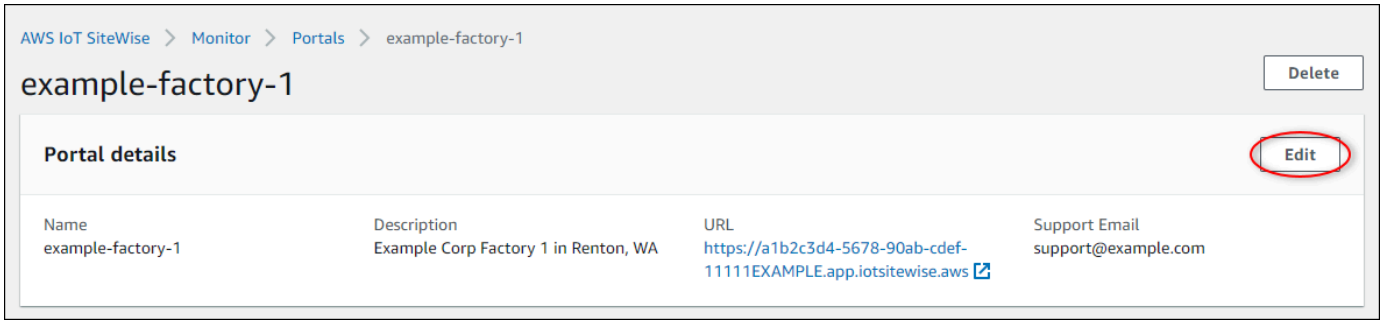
- Cambio del nombre, la descripción, la marca, el email de soporte y los permisos de un portal
- Agregar o quitar administradores del portal
- Envío de invitaciones por correo electrónico a administradores del portal
- Agregar o quitar usuarios del portal

- Eliminación de un portal

Cambio del nombre, la descripción, la marca, el email de soporte y los permisos de un portal

Puede cambiar el nombre, la descripción, la marca, el email de soporte y los permisos de un portal.

1. En la página de detalles del portal, en la sección Portal details (Detalles del portal) elija Edit (Editar).

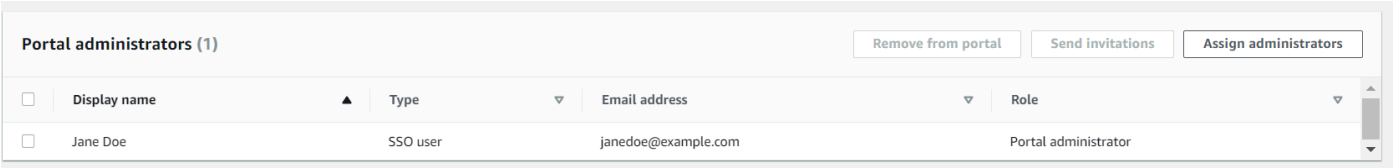


2. Actualice el nombre, la descripción, la marca del portal, el email de contacto de soporte o los permisos.
3. Cuando haya terminado, elija Save.

Agregar o quitar administradores del portal

En unos pocos pasos, puede añadir o quitar usuarios como administradores de un portal. En función del servicio de autenticación de usuarios, elija una de las siguientes opciones.

IAM Identity Center



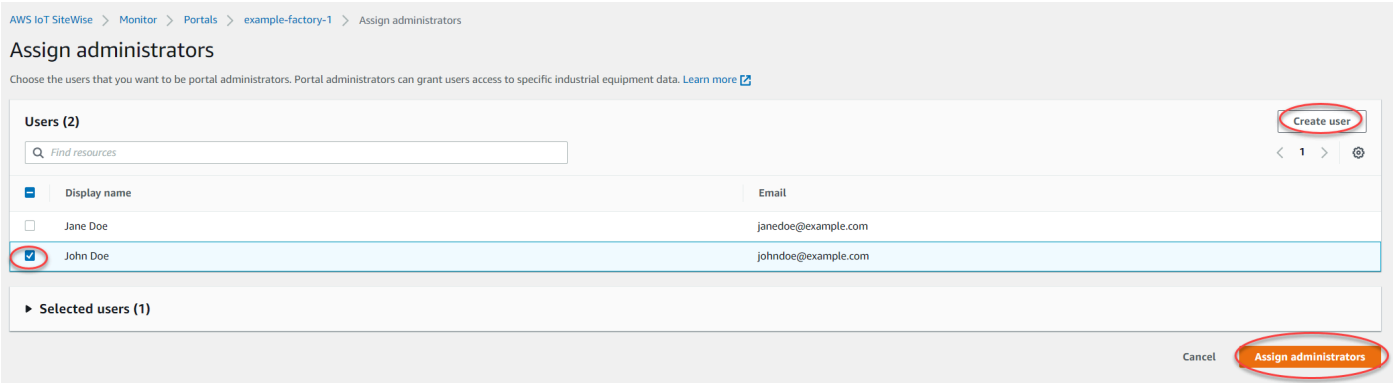
Para añadir administradores de portal

1. En la página de detalles del portal, en la sección Administradores del portal, seleccione Asignar administradores.

2. En la página Asignar administradores, seleccione las casillas de verificación de los usuarios que quiera añadir al portal como administradores.

> **Note**
>
> Si utiliza el Centro de identidades de IAM como almacén de identidades y ha iniciado sesión en su cuenta de administración de AWS Organizations , puede elegir Crear usuario para crear un usuario del Centro de identidades de IAM. El Centro de identidades de IAM enviará al nuevo usuario un correo electrónico para que establezca su contraseña. A continuación, puede asignar el usuario al portal como administrador. Para obtener más información, consulte Administrar identidades en el IAM Identity Center.

3. Seleccione Asignar administradores.

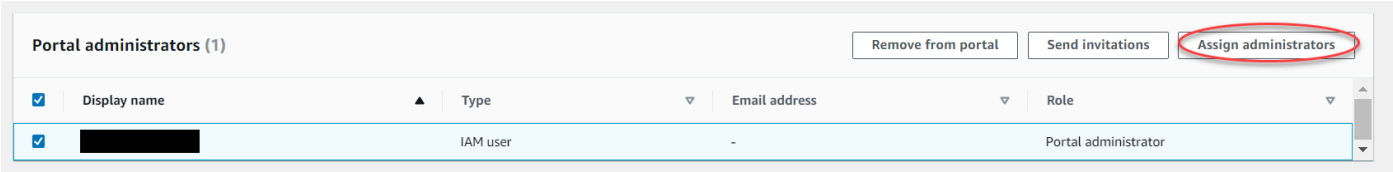


Para eliminar administradores del portal

- En la página de detalles del portal, en la sección Administradores del portal active la casilla de verificación de cada usuario que quiera eliminar y, a continuación, seleccione Eliminar del portal.

> **Note**
>
> Le recomendamos que seleccione al menos un administrador del portal.

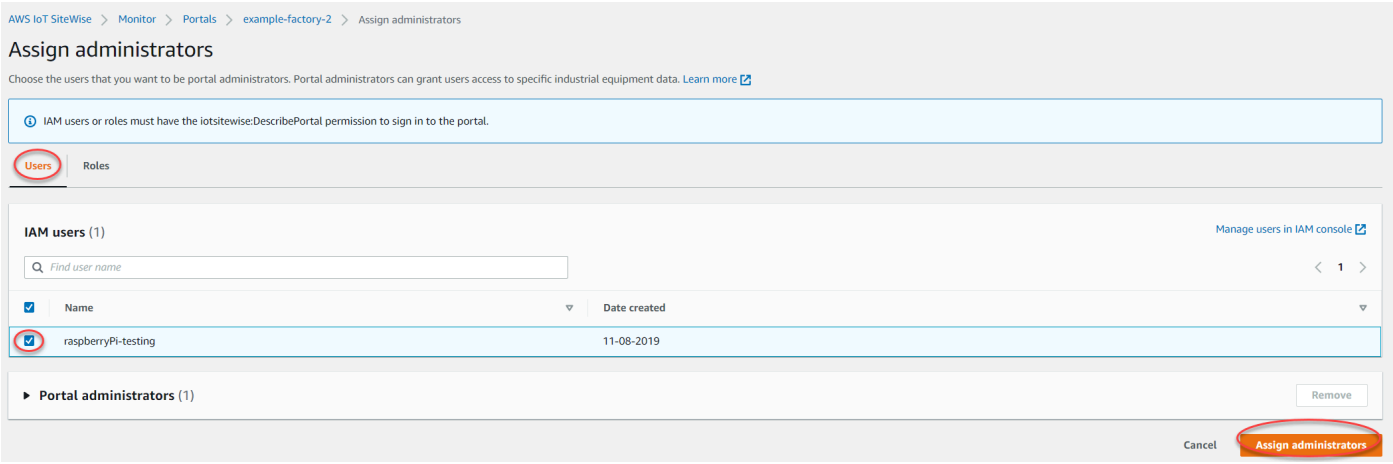
IAM

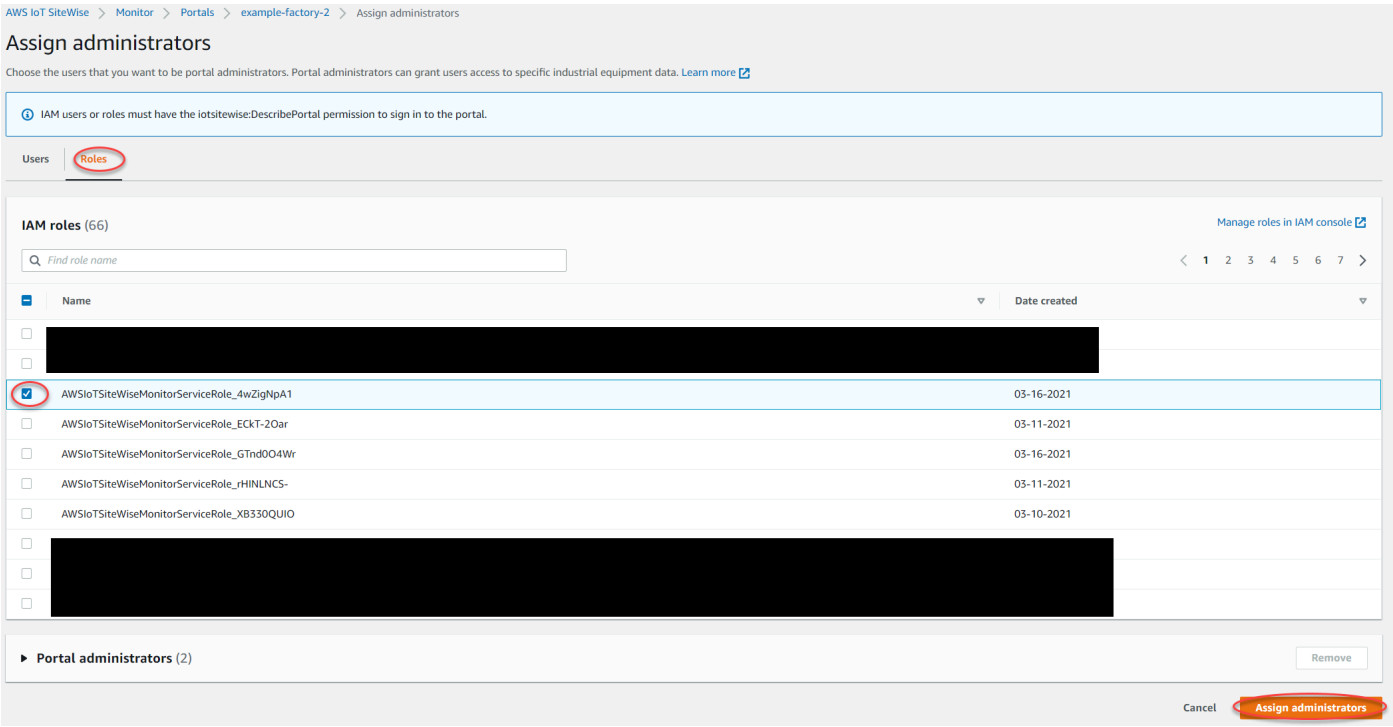


Para añadir administradores de portal

1. En la página de detalles del portal, en la sección Administradores del portal, seleccione Asignar administradores.
2. En la página Asignación de administradores, haga lo siguiente:
   - Elija Usuarios de IAM si lo que desea es añadir un usuario de IAM como administrador de su portal.
   - Elija Roles de IAM si lo que desea es añadir un rol de IAM como administrador de su portal.
3. Marque las casillas de verificación de los usuarios o roles que desee como administradores de su portal. Esto añade los usuarios o roles a la lista de Administradores del portal.
4. Seleccione Asignar administradores.

> **Important**
>
> Los usuarios o roles deben tener el permiso de `iotsitewise:DescribePortal` para iniciar sesión en el portal.





Para eliminar administradores del portal

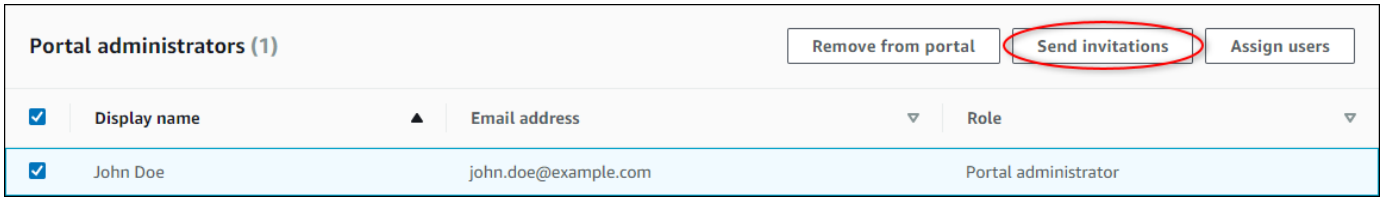
- En la página de detalles del portal, en la sección Administradores del portal active la casilla de verificación de cada usuario que quiera eliminar y, a continuación, seleccione Eliminar del portal.

> **Note**
>
> No se recomienda dejar un portal sin un administrador del portal.

Envío de invitaciones por correo electrónico a administradores del portal

Puede enviar invitaciones por correo electrónico a administradores del portal.

1. En la página de detalles del portal, en la sección Portal administrators (Administradores del portal), seleccione las casillas de verificación de los administradores del portal.



2. Seleccione Send invitations (Enviar invitaciones). Se abrirá el cliente de correo electrónico y se rellenará una invitación en el cuerpo del mensaje.

   Puede personalizar el correo electrónico antes de enviarlo a los administradores del portal.

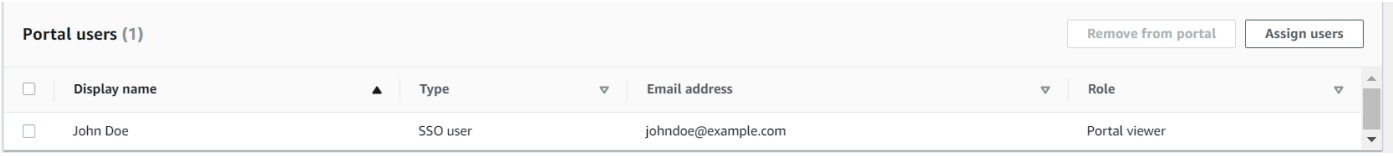
Agregar o quitar usuarios del portal

Elija los usuarios que tienen acceso a sus portales. Los usuarios del portal aparecen en la lista de usuarios de un portal de SiteWise Monitor. En esta lista, los administradores del portal pueden añadir propietarios de proyectos y los propietarios de proyectos pueden añadir observadores de proyectos.

> **Note**
>
> Los administradores del portal y los usuarios del portal pueden ponerse en contacto con usted a través del correo electrónico de soporte de un portal si tienen que agregar o quitar un usuario.

En función del servicio de autenticación de usuarios, elija una de las siguientes opciones.

IAM Identity Center



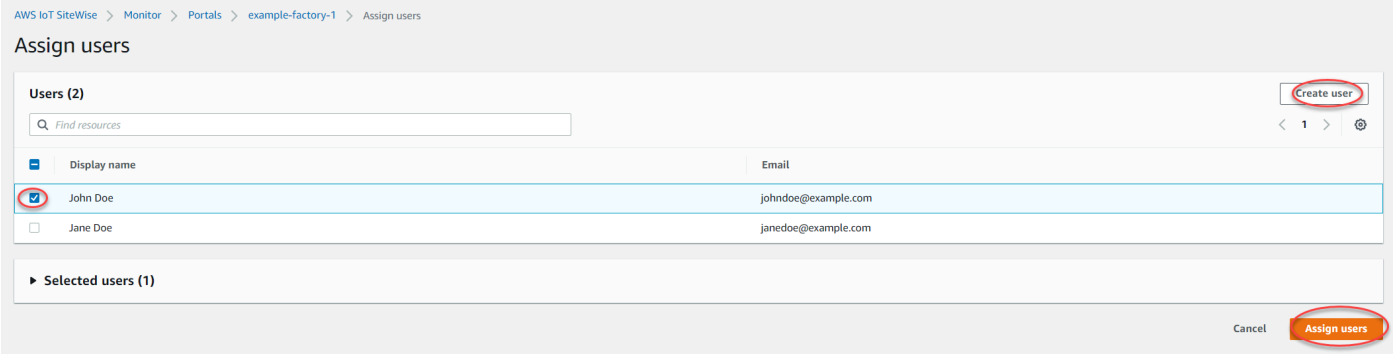
Para añadir usuarios del portal

1. En la página de detalles del portal, en la sección Portal users (Usuarios del portal), elija Assign users (Asignar usuarios).
2. En la página Asignar usuarios, seleccione la casilla de verificación de los usuarios que va a añadir al portal.

   > **Note**
   >
   > Si utiliza el Centro de identidades de IAM como almacén de identidades y ha iniciado sesión en su cuenta de administración de AWS Organizations , puede elegir Crear usuario para crear un usuario del Centro de identidades de IAM. El Centro de identidades de IAM enviará al nuevo usuario un correo electrónico para que

establezca su contraseña. A continuación, puede asignar el usuario al portal como usuario. Para obtener más información, consulte Administrar identidades en el IAM Identity Center.

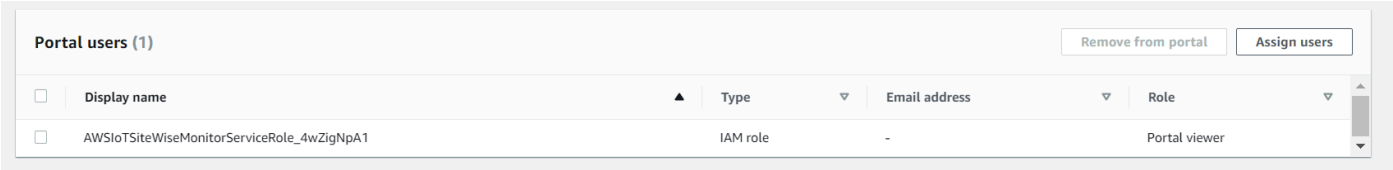
3. Elija Assign users (Asignar usuarios).



Para quitar usuarios del portal

- En la página de detalles del portal, en la sección Usuarios del portal, seleccione las casillas de verificación de los usuarios que va a eliminar del portal y, a continuación, Eliminar del portal.

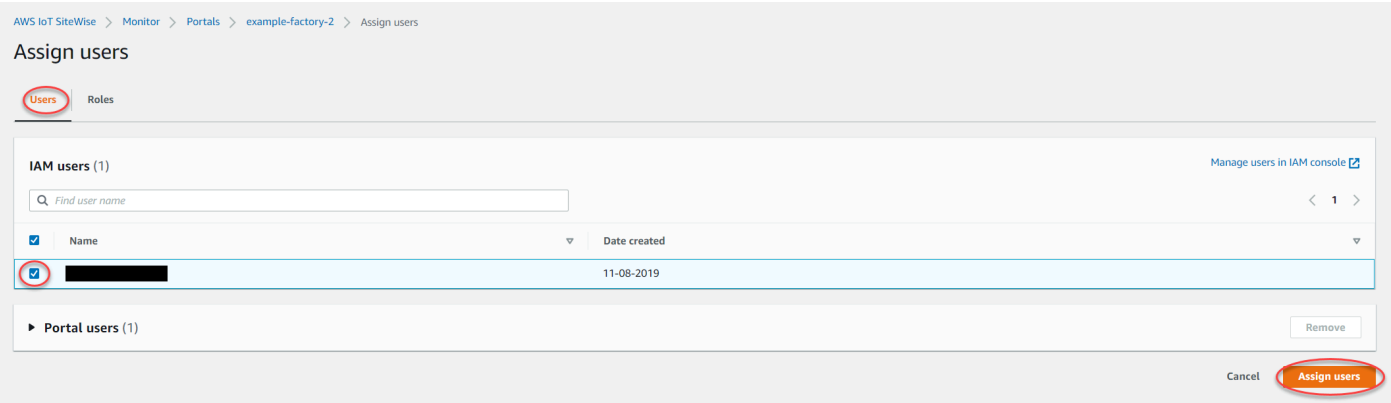
IAM

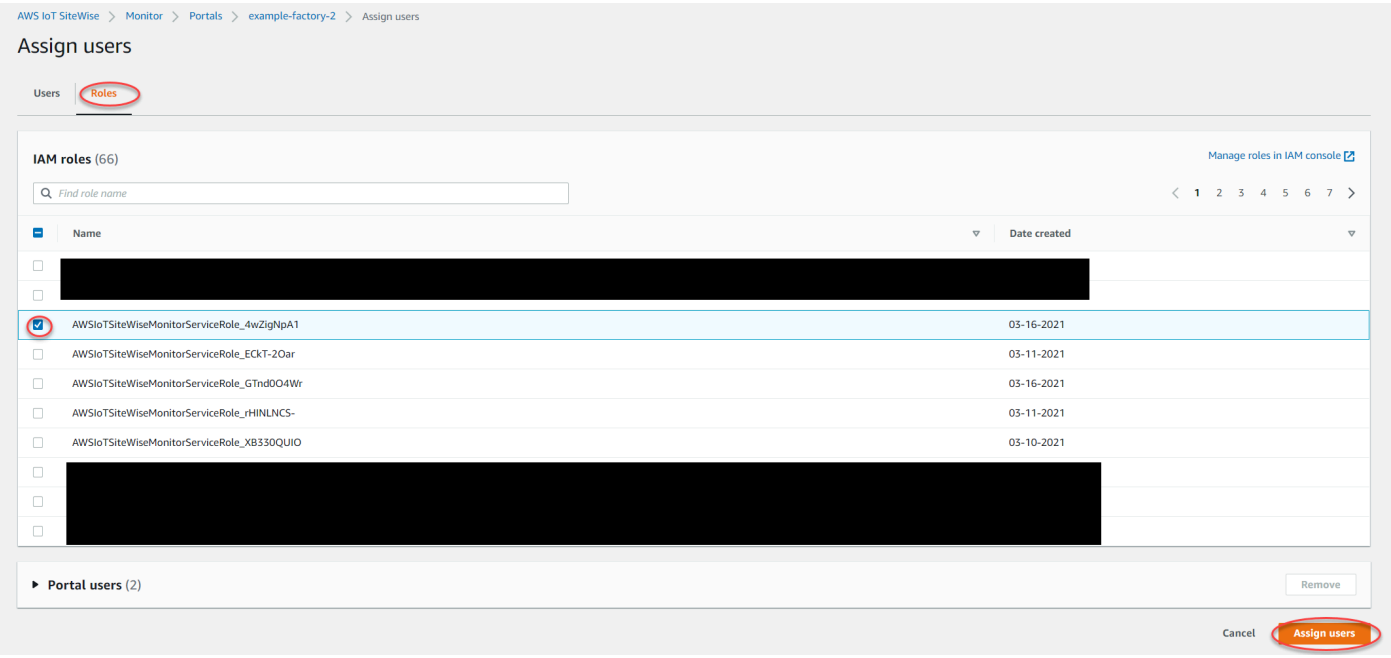


Para añadir usuarios del portal

1. En la página de detalles del portal, en la sección Portal users (Usuarios del portal), elija Assign users (Asignar usuarios).
2. En la página Asignación de usuarios, haga lo siguiente:
   - Elija Usuarios de IAM para añadir un usuario de IAM como usuario de su portal.
   - Elija Roles de IAM para añadir un rol de IAM como usuario de su portal.
3. Marque las casillas de verificación de los usuarios o roles que desee como usuarios de su portal. Esto añade los usuarios o roles a la lista Usuarios del portal.

4. Elija Assign users (Asignar usuarios).





Para quitar usuarios del portal

- En la página de detalles del portal, en la sección Usuarios del portal, seleccione las casillas de verificación de los usuarios que va a eliminar del portal y, a continuación, Eliminar del portal.

> **Important**
>
> Los usuarios o roles deben tener el permiso de `iotsitewise:DescribePortal` para iniciar sesión en el portal.

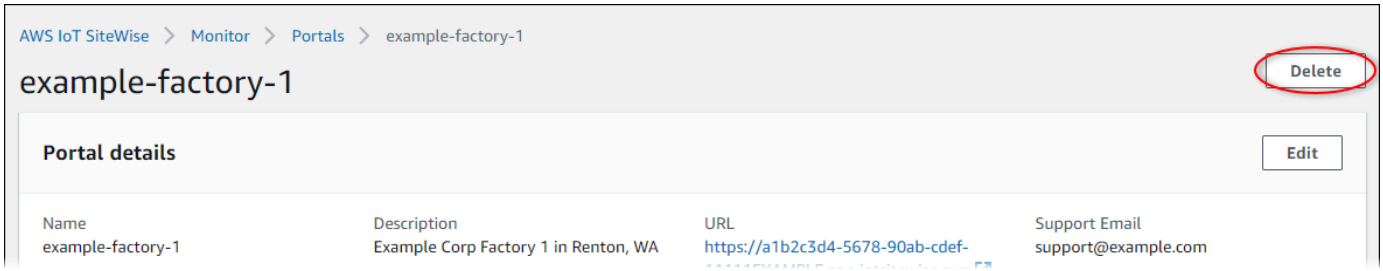
Eliminación de un portal

Puede eliminar un portal si lo ha creado con fines de prueba o si ha creado un duplicado de un portal que ya existe.

> **Note**
>
> Primero debe eliminar manualmente todos los paneles y proyectos del portal antes de poder eliminarlo. Para obtener más información, consulte Eliminar proyectos y Eliminar paneles en la Guía de aplicaciones de SiteWise Monitor.

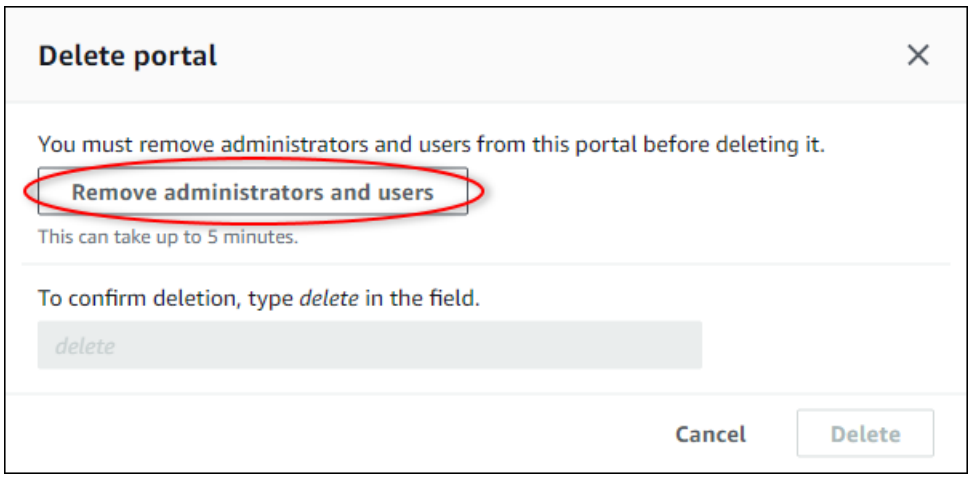
1. En la página de detalles del portal, elija Eliminar.

   > **Important**
   >
   > Cuando se elimina un portal, se pierden todos los proyectos que contiene el portal y todos los paneles de cada proyecto. Esta acción no se puede deshacer. Los datos de activos no se ven afectados.

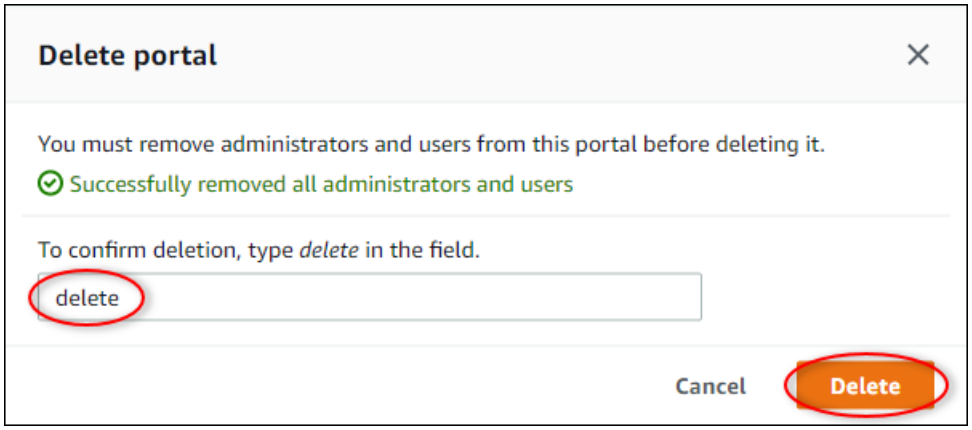


2. En el cuadro de diálogo Eliminar portales, seleccione Eliminar administradores y usuarios.

   Debe quitar los administradores y usuarios del portal antes de poder eliminarlo. Si el portal no tiene administradores o usuarios, el botón no aparece y puede pasar al siguiente paso.



3. Si está seguro de que desea eliminar todo el portal, escriba **`delete`** en el campo para confirmar la eliminación.



4. Seleccione Eliminar.

Supervisión de datos con la aplicación de panel de control de IoT

La aplicación de panel de IoT es una aplicación de panel de código abierto en la que puede visualizar e interactuar con los datos operativos. Puede utilizar la aplicación AWS Cloud Development Kit (AWS CDK) de panel de control de IoT.

Los siguientes son ejemplos de las funciones de visualización de datos personalizables en la aplicación de panel de control de IoT:

- Support para múltiples propiedades en un gráfico de una sola línea.
- Búsqueda mejorada de activos y propiedades.

Los clientes de los sectores de fabricación, logística, energía y otros sectores pueden utilizar la aplicación de panel de control de IoT para abordar desafíos específicos, como el seguimiento del rendimiento de los equipos, la optimización de la eficiencia operativa y las decisiones basadas en datos. Para obtener más información, consulte el GitHub repositorio de la aplicación de panel de control de IoT.

Consulta datos de AWS IoT SiteWise

Puede utilizar las operaciones de la AWS IoT SiteWise API para consultar los valores actuales, históricos y agregados de las propiedades de sus activos en intervalos de tiempo específicos.

Utilice estas funciones para obtener información sobre sus datos. Por ejemplo, descubra todos sus activos con un valor de propiedad determinado o cree una representación personalizada de sus datos. También puede utilizar las operaciones de la API para desarrollar soluciones de software que se integren con los datos industriales almacenados en sus AWS IoT SiteWise activos. También puede explorar los datos de sus activos en tiempo real en AWS IoT SiteWise Monitor. Para obtener información sobre cómo configurar SiteWise Monitor, consulteMonitorización de datos con AWS IoT SiteWise Monitor.

Las operaciones descritas en esta sección devuelven objetos con valores de propiedad que contienen estructuras de marca de tiempo, calidad y valor (TQV):

- El `timestamp` contiene el tiempo actual en formato de tiempo Unix en segundos con desplazamiento en nanosegundos.
- `quality` contiene una de las siguientes cadenas, que indican la calidad del punto de datos:
  - `GOOD`: los datos no se ven afectados por ningún problema.
  - `BAD`: los datos se ven afectados por un problema, como un fallo del sensor.
  - `UNCERTAIN`: los datos se ven afectados por un problema, como la falta de precisión de un sensor.
- El `value` contiene uno de los siguientes campos, en función del tipo de propiedad:
  - `booleanValue`
  - `doubleValue`
  - `integerValue`
  - `stringValue`

Temas

Consulta de los valores actuales de las propiedades de los activos

En este tutorial se muestran dos formas de obtener el valor actual de una propiedad de activo. Puede usar la AWS IoT SiteWise consola o la API en AWS Command Line Interface (AWS CLI).

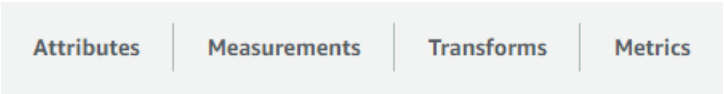
Temas

Consulta el valor actual de una propiedad de un activo (consola)

Puede utilizar la AWS IoT SiteWise consola para ver el valor actual de la propiedad de un activo.

Para obtener el valor actual de la propiedad de un activo (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija activos.
3. Elija el activo con la propiedad que desea consultar.
4. Seleccione el icono de flecha para expandir una jerarquía de activos y encontrar su activo.
5. Elija la pestaña para el tipo de propiedad. Por ejemplo, elija Medidas para consultar el valor actual de una propiedad de medida.



6. Encuentre la propiedad que desea consultar. El valor actual aparece en la columna Valor más reciente.

Consulta el valor actual de una propiedad de un activo (AWS CLI)

Puede usar AWS Command Line Interface (AWS CLI) para consultar el valor actual de una propiedad de activo.

Utilice la GetAssetPropertyValueoperación para consultar el valor actual de una propiedad de un activo.

Para identificar una propiedad de activo, especifique una de las siguientes opciones:

- El `assetId` extremo `propertyId` de la propiedad del activo a la que se envían los datos.
- El `propertyAlias`, que es un alias de flujo de datos (por ejemplo, `/company/windfarm/3/turbine/7/temperature`). Para utilizar esta opción, primero debe establecer el alias de la propiedad del activo. Para establecer los alias de las propiedades, consulteAsignación de flujos de datos industriales a propiedades de activos.

Para obtener el valor actual de una propiedad de activo ()AWS CLI

- Ejecute el siguiente comando para obtener el valor actual de la propiedad del activo. Reemplace *asset-id* por el ID del activo y *property-id* por el ID de la propiedad.

```
aws iotsitewise get-asset-property-value \
  --asset-id asset-id \
  --property-id property-id
```

La operación devuelve una respuesta que contiene el TQV actual de la propiedad en el siguiente formato.

```
{
  "propertyValue": {
    "value": {
      "booleanValue": Boolean,
      "doubleValue": Number,
      "integerValue": Number,
      "stringValue": "String"
    },
    "timestamp": {
      "timeInSeconds": Number,
      "offsetInNanos": Number
    },
    "quality": "String"
  }
}
```

Consulta de los valores históricos de las propiedades de los activos

Puede utilizar la GetAssetPropertyValueHistoryoperación de la AWS IoT SiteWise API para consultar los valores históricos de una propiedad de activo.

Para identificar una propiedad de un activo, especifique una de las siguientes opciones:

- El `assetId` extremo `propertyId` de la propiedad del activo a la que se envían los datos.
- El `propertyAlias`, que es un alias de flujo de datos (por ejemplo, `/company/windfarm/3/turbine/7/temperature`). Para utilizar esta opción, primero debe establecer el alias de la propiedad del activo. Para establecer los alias de las propiedades, consulteAsignación de flujos de datos industriales a propiedades de activos.

Pase los siguientes parámetros para refinar los resultados:

- `startDate`: el inicio inclusivo del rango del cual se consultan los datos históricos, expresado en segundos en tiempo epoch de Unix.
- `endDate`: el final inclusivo del rango del cual se consultan los datos históricos, expresado en segundos en tiempo epoch de Unix.
- `maxResults`: el número máximo de resultados por devolver en una petición. Predeterminado a `20` resultados.
- `nextToken`: un token de paginación devuelto por una llamada anterior de esta operación.
- `timeOrdering`: el orden por aplicar a los valores devueltos: `ASCENDING` o `DESCENDING`.
- `qualities`: calidad para filtrar los resultados: `GOOD`, `BAD`, o `UNCERTAIN`.

Temas

- Consulte el historial de valores de una propiedad de activo (AWS CLI)

Consulte el historial de valores de una propiedad de activo (AWS CLI)

Para consultar el historial de valores de una propiedad activa (AWS CLI)

1. Ejecute el siguiente comando para obtener el historial de valores de la propiedad del activo. Este comando consulta el historial de la propiedad durante un intervalo específico de 10 minutos. Reemplace *`asset-id`* por el ID del activo y *`property-id`* por el ID de la propiedad. Reemplace los parámetros de fecha por el intervalo que desea consultar.

```
aws iotsitewise get-asset-property-value-history \
  --asset-id asset-id \
  --property-id property-id \
  --start-date 1575216000 \
```

```
  --end-date 1575216600
```

La operación devuelve una respuesta que contiene los TQV históricos de la propiedad en el siguiente formato:

```
{
  "assetPropertyValueHistory": [
    {
      "value": {
        "booleanValue": Boolean,
        "doubleValue": Number,
        "integerValue": Number,
        "stringValue": "String"
      },
      "timestamp": {
        "timeInSeconds": Number,
        "offsetInNanos": Number
      },
      "quality": "String"
    }
  ],
  "nextToken": "String"
}
```

2. Si existen más entradas de valores, puede pasar el token de paginación del `nextToken` campo a una llamada posterior a la GetAssetPropertyValueHistoryoperación.

Consulta de agregados de propiedades de activos

AWS IoT SiteWise calcula automáticamente los valores agregados de las propiedades de los activos, que son un conjunto de métricas básicas calculadas en varios intervalos de tiempo. AWS IoT SiteWise calcula los siguientes agregados cada minuto, hora y día para las propiedades de sus activos:

- promedio: el promedio (media) de los valores de una propiedad en un intervalo de tiempo.
- recuento: el número de puntos de datos de una propiedad a lo largo de un intervalo de tiempo.
- máximo: el máximo de los valores de una propiedad en un intervalo de tiempo.
- mínimo: el mínimo de los valores de una propiedad en un intervalo de tiempo.

- desviación estándar: la desviación estándar de los valores de una propiedad en un intervalo de tiempo.
- suma: la suma de los valores de una propiedad en un intervalo de tiempo.

Para las propiedades no numéricas, como cadenas y valores booleanos, AWS IoT SiteWise calcula solo el recuento agregado.

También puede calcular métricas personalizadas para los datos de activos. Con las propiedades métricas, usted define las agregaciones que son específicas de su operación. Las propiedades métricas ofrecen funciones de agregación e intervalos de tiempo adicionales que no están precalculados para la AWS IoT SiteWise API. Para obtener más información, consulte Agregación de datos de propiedades y otros activos (métricas).

Temas

- Agregados de una propiedad de activo (API)
- Agregados de una propiedad de activo ()AWS CLI

Agregados de una propiedad de activo (API)

Puede usar la AWS IoT SiteWise API para obtener los agregados de una propiedad de activo.

Utilice la GetAssetPropertyAggregatesoperación para consultar los agregados de una propiedad de activo.

Para identificar una propiedad de activo, especifique una de las siguientes opciones:

- El `assetId` extremo `propertyId` de la propiedad del activo a la que se envían los datos.
- El `propertyAlias`, que es un alias de flujo de datos (por ejemplo, `/company/windfarm/3/turbine/7/temperature`). Para utilizar esta opción, primero debe establecer el alias de la propiedad del activo. Para establecer los alias de las propiedades, consulteAsignación de flujos de datos industriales a propiedades de activos.

También debe pasar los siguientes parámetros obligatorios:

- `aggregateTypes`: la lista de agregados que se va a recuperar. Puede especificar uno de estos: `AVERAGE`, `COUNT`, `MAXIMUM`, `MINIMUM`, `STANDARD_DEVIATION` y `SUM`.

- `resolution`: el intervalo de tiempo para el cual se recupera la métrica: `1m` (1 minuto), `1h` (1 hora) o `1d` (1 día).
- `startDate`: el inicio inclusivo del rango del cual se consultan los datos históricos, expresado en segundos en tiempo epoch de Unix.
- `endDate`: el final inclusivo del rango del cual se consultan los datos históricos, expresado en segundos en tiempo epoch de Unix.

También puede pasar cualquiera de los siguientes parámetros para refinar los resultados:

- `maxResults`: el número máximo de resultados por devolver en una petición. Predeterminado a `20` resultados.
- `nextToken`: un token de paginación devuelto por una llamada anterior de esta operación.
- `timeOrdering`: el orden por aplicar a los valores devueltos: `ASCENDING` o `DESCENDING`.
- `qualities`: calidad para filtrar los resultados: `GOOD`, `BAD`, o `UNCERTAIN`.

> **Note**
>
> La GetAssetPropertyAggregatesoperación devuelve un TQV con un formato diferente al de las demás operaciones descritas en esta sección. La estructura del `value` contiene un campo para cada uno de los `aggregateTypes` de la solicitud. En `timestamp` se incluye el tiempo en que se produjo la agregación, en segundos en formato Unix.

Agregados de una propiedad de activo ()AWS CLI

Para consultar los agregados de una propiedad de activo ()AWS CLI

1. Ejecute el siguiente comando para obtener agregados para la propiedad del activo. Este comando consulta la media y la suma con una resolución de 1 hora para un intervalo de 1 hora específico. Reemplace *`asset-id`* por el ID del activo y *`property-id`* por el ID de la propiedad. Reemplace los parámetros por los agregados y el intervalo a consultar.

```
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
```

La operación devuelve una respuesta que contiene los TQV históricos de la propiedad en el siguiente formato. La respuesta incluye solo los agregados solicitados.

```
{
  "aggregatedValues": [
    {
      "timestamp": Number,
      "quality": "String",
      "value": {
        "average": Number,
        "count": Number,
        "maximum": Number,
        "minimum": Number,
        "standardDeviation": Number,
        "sum": Number
      }
    }
  ],
  "nextToken": "String"
}
```

2. Si existen más entradas de valor, puede pasar el token de paginación del `nextToken` campo a una llamada posterior a la GetAssetPropertyAggregatesoperación.

AWS IoT SiteWise idioma de consulta

Con la operación de la ExecuteQueryAPI de recuperación de AWS IoT SiteWise datos, puede recuperar información sobre las definiciones estructurales declarativas y los datos de series temporales asociadas a ellas a partir de lo siguiente:

- modelos
- recursos
- medidas
- métricas
- transforma

- agregados

Esto se puede hacer con sentencias de consulta tipo SQL, en una sola solicitud de API.

> **Note**
>
> Esta función está disponible en todas las regiones en las que ambas AWS IoT TwinMaker están disponibles, excepto AWS GovCloud (EE. UU. AWS IoT SiteWise y oeste).

Temas

Requisitos previos

AWS IoT SiteWise requiere permisos para integrarse y AWS IoT TwinMaker poder organizar y modelar los datos industriales.

Antes de poder recuperar información sobre modelos, activos, medidas, métricas, transformaciones y agregados, asegúrese de que se cumplen los siguientes requisitos previos:

- Funciones vinculadas al servicio para ambos AWS IoT SiteWise y AWS IoT TwinMaker configuradas en su. Cuenta de AWS Para obtener más información acerca los roles vinculados a servicios, consulte Uso de roles vinculados a servicios en la Guía del usuario de IAM.
- Una AWS IoT SiteWise integración habilitada para su función de IAM. Para obtener más información, consulte Integración de AWS IoT SiteWise y AWS IoT TwinMaker.
- Un AWS IoT TwinMaker espacio de trabajo con un ID `IoTSiteWiseDefaultWorkspace` en tu cuenta en la región. Para obtener más información, consulte Utilización de IoTSiteWiseDefaultWorkspace en la Guía del usuario de AWS IoT TwinMaker ;.
- Los modos de precios por paquetes estándar o escalonados están AWS IoT TwinMaker activados. Para obtener más información, consulte Cambiar AWS IoT TwinMaker los modos de precios en la Guía del AWS IoT TwinMaker usuario.

Consulta el idioma de referencia

AWS IoT SiteWise admite un lenguaje de consulta enriquecido para trabajar con los datos. Los tipos de datos, operadores, funciones y construcciones disponibles se describen en los temas siguientes.

Consulte Consultas de ejemplo para escribir consultas con el lenguaje de AWS IoT SiteWise consultas.

Temas

Comprensión de las vistas

En esta sección se proporciona información que le ayudará a entender las vistas AWS IoT SiteWise, como los metadatos de los procesos y los datos de telemetría.

En las tablas siguientes se proporcionan los nombres y las descripciones de las vistas.

Modelo de datos

Nombre de la vista	Descripción de vista
asset	Contiene información sobre la derivación del activo y el modelo.
asset_property	Contiene información sobre la estructura de la propiedad del activo.
raw_time_series	Contiene los datos históricos de la serie temporal.
latest_value_time_series	Contiene el valor más reciente de la serie temporal.

Nombre de la vista	Descripción de vista
precomputed_aggregates	Contiene los valores agregados de las propiedades de los activos calculados automáticamente. Son un conjunto de métricas básicas calculadas en varios intervalos de tiempo.

Las siguientes vistas muestran los nombres de las columnas de las consultas junto con datos de ejemplo.

Vista: activo

asset_id	nombre_activo	descripción_activo	asset_model_id
88898498-0b8b-42b5-bf57-16180bc3d3a0	WindTurbine A	WindTurbine Activo A	17847250-5bf0-4f74-b775-cc03f05e7cb8
17847250-5bf0-4f74-b775-cc03f05e7cb8	Modelo de activos de turbinas eólicas	Representa una turbina en un parque eólico.	

Ver: asset_property

property_id	asset_id	nombre_propiedad	tipo_de_datos_propiedad	property_alias	asset_composite_model_id
b29be434-b000-4d74-b809-75287d83bcd6	88898498-0b8b-42b5-bf57-16180bc3d3a0	temperatura del motor	Doble	`Rochester 2/44///Line-5/Bus-2/Machine-5/Temperature`	
3b458f00-24e7-458a	88898498-0b8b-42b5	dirección del viento	Doble	`/company/windfarm/`	2f458n00-56e7-458h

property_id	asset_id	nombre_propiedad	tipo_de_datos_propiedad	property_alias	asset_composite_model_id
-b4e8-c6026eff654a	-bf57-16180bc3d3a0			3/turbine/7/winddirection	-b4e8-c6026eff985 g

Ver: RAW_Time_Series

asset_id	property_id	property_alias	event_timestamp	calidad	valor_booleano	valor_int	valor_doble	valor_cadena
888984980b8b-42b5-bf57-16180bc3d3a	b29be434-b000-4d74-b809-75287d83bcd	Rochest 2/44/// Line-5/Bus-2/Machine-5/Temperature	1575219600	BUENA			115,0	
888984980b8b-42b5-bf57-16180bc3d3a	3b458f00-24e7-458a-b4e8-c6026eff654a	/company/windfarm 3/turbine/7/winddirection	1575219337	BUENA			348,75	

> **Note**
>
> Debe incluir una cláusula de filtro en la `event_timestamp` columna para consultar la `raw_time_series` vista. Se trata de un filtro obligatorio y la consulta fallará sin él.
>
> Example consulta
>
> ```
> SELECT event_timestamp, double_value FROM raw_time_series WHERE event_timestamp
>  > 1234567890
> ```

Ver: serie LATEST_VALUE_TIME_SERIES

asset_id	property_id	property_alias	event_timestamp	calidad	valor_booleano	valor_int	valor_double	valor_cadena
88898498-0b8b-42b5-bf57-16180bc3d3a	3b458f00-24e7-458a-b4e8-c6026eff654a	/company/windfarm/3/turbine/7/winddirection	1575219600	BUENA			355,39	

Ver: precomputed_aggregates

asset_id	property_id	property_alias	event_timestamp	resolution	valor_suma	valor_recuento	valor_medio	valor_máximo	valor_mínimo	stdev_value
888984-0b8b-42-bf57-1680bc3d	b29be4-b000-4c-b809-7587d83b	Roches2/44//Line-5/Bus-2/Machin	157521-0	15 m	1105,48	15	73,4	80,6	68	3,64

asset_ic	property id	property alias	event_ti estamp	resolutic n	valor_su a	valor_re uento	valor_m io	valor_m imo	valor_m imo	stdev_val ue
		-5/ Temper ature								

Tipos de datos admitidos

AWS IoT SiteWise el lenguaje de consultas admite los siguientes tipos de datos.

Ver: activo

Tipo de datos	Descripción
`STRING`	Cadena con una longitud máxima de 1024 bytes.
`INTEGER`	Un entero de 32 bits con signo con un intervalo de`-2,147,483,648 to 2,147,483,647` .
`DOUBLE`	Un número de coma flotante con un rango desde `-10^100 to 10^100` y una precisión `IEEE 754` doble.
`BOOLEAN`	`true` o bien `false`.

> **Note**
>
> Los datos de doble precisión no son exactos. Algunos valores no se convierten exactamente y no representan todos los números reales debido a la precisión limitada. Es posible que los datos de punto flotante de la consulta no tengan el mismo valor representado internamente. El valor se redondea si la precisión de un número de entrada es demasiado alta.

Recupera datos con una sentencia SELECT

La `SELECT` sentencia se utiliza para recuperar datos de una o más vistas. AWS IoT SiteWise admite un punto `JOIN` de vista implícito. Puede enumerar las vistas a unir (en la `FROM` cláusula de la `SELECT` declaración), separándolas con comas.

Example

Utilice la siguiente `SELECT` afirmación:

```
SELECT select_expr [, ...]
[ FROM from_item [, ...] ]
[ WHERE [LIKE condition ESCAPE condition] ]
```

En el ejemplo anterior, la `LIKE` cláusula especifica las condiciones de búsqueda y filtrado mediante comodines. AWS IoT SiteWise admite `percentage (%)` el carácter comodín.

Example para usar **%** en una condición:

```
Prefix search: String%
Infix search: %String%
Suffix search: %String
```

Example para buscar un activo:

```
SELECT asset_name, asset_description FROM asset WHERE asset_name LIKE 'Wind%'
```

Example para buscar un activo mediante la condición ESCAPE:

```
SELECT asset_name, asset_description FROM asset WHERE asset_name LIKE 'room\%' ESCAPE
 '\'
```

Logical operators (Operadores lógicos)

AWS IoT SiteWise admite los siguientes operadores lógicos.

Logical operators (Operadores lógicos)

Operador	Descripción	Ejemplo
AND	TRUEsi ambos valores son verdaderos	a AND b

Si a o b sonFALSE, la expresión anterior se evalúa como falsa. Para que un AND operador dé como resultado verdadero, tanto a como b deben ser verdaderos.

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
```

Operadores de comparación

AWS IoT SiteWise admite los siguientes operadores de comparación.

Logical operators (Operadores lógicos)

Operador	Descripción
<	Menor que
>	Mayor que
<=	Menor o igual que
>=	Mayor o igual que
=	Igual a
!=	Desigualdad

Consultas de ejemplo

Filtrado de metadatos

El siguiente ejemplo es para filtrar metadatos con una `SELECT` sentencia con el lenguaje de AWS IoT SiteWise consulta:

```
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%'
```

Filtrado de valores

A continuación se muestra un ejemplo de filtrado de valores mediante una `SELECT` sentencia con el lenguaje de AWS IoT SiteWise consulta:

```
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
```

Interacción con otros AWS servicios

AWS IoT SiteWise puede publicar datos de activos en el intermediario de mensajes de publicación y suscripción de AWS IoT MQTT, de modo que pueda interactuar con los datos de sus activos desde otros servicios. AWS AWS IoT SiteWise asigna a cada propiedad de activo un tema de MQTT único que puede utilizar para dirigir los datos de sus activos a otros AWS servicios mediante las reglas básicas. AWS IoT Por ejemplo, puede configurar las reglas AWS IoT principales para realizar las siguientes tareas:

- Identificar fallos en los equipos y notificar al personal idóneo mediante el envío de datos a AWS IoT Events.
- Crear un historial de los datos de activos seleccionados para utilizarlos en soluciones de software externas mediante el envío de datos a Amazon DynamoDB.
- Generar informes semanales mediante la activación de una función de AWS Lambda.

Puede seguir un tutorial que recorre los pasos necesarios para configurar una regla que almacene valores de propiedad en DynamoDB. Para obtener más información, consulte Publicar actualizaciones de valor de propiedad en Amazon DynamoDB.

Para obtener más información sobre cómo configurar una regla, consulte Reglas en la Guía para desarrolladores de AWS IoT .

También puede volver a consumir datos de otros AWS servicios AWS IoT SiteWise. Para ingerir datos mediante la acción de la AWS IoT SiteWise regla, consulteIngerir datos mediante reglas AWS IoT Core.

Temas

- Descripción de los temas de MQTT sobre las propiedades de los activos
- Uso de las notificaciones de propiedad de activo
- Exporte datos a Amazon S3 con notificaciones de propiedad de activos
- Integración con Grafana
- Integración de AWS IoT SiteWise y AWS IoT TwinMaker
- Detección de anomalías en los equipos con Amazon Lookout for Equipment

Descripción de los temas de MQTT sobre las propiedades de los activos

Cada propiedad de activo tiene una ruta de tema MQTT única en el siguiente formato.

```
$aws/sitewise/asset-models/assetModelId/assets/assetId/properties/propertyId
```

> **Note**
>
> AWS IoT SiteWise no admite el comodín de filtro de temas # (de varios niveles) del AWS IoT motor de reglas principales. Puede utilizar el comodín + (de un solo nivel). Por ejemplo, puede utilizar el siguiente filtro de temas para que coincida con todas las actualizaciones de un modelo de activos concreto.
>
> ```
> $aws/sitewise/asset-models/assetModelId/assets/+/properties/+
> ```
>
> Para obtener más información sobre los comodines del filtro de temas, consulte Temas en la Guía para desarrolladores de AWS IoT .

Uso de las notificaciones de propiedad de activo

Puede activar las notificaciones de propiedades para publicar actualizaciones de los datos de los activos y AWS IoT Core, a continuación, ejecutar consultas sobre sus datos. Con las notificaciones de propiedades de los activos, AWS IoT SiteWise proporciona una AWS CloudFormation plantilla que puede utilizar para exportar AWS IoT SiteWise datos a Amazon S3.

> **Note**
>
> Los datos de los activos se envían AWS IoT Core cada vez que los reciben AWS IoT SiteWise, independientemente de si el valor ha cambiado.

Temas

- Habilitación de notificaciones de las propiedades de activos (consola)
- Habilitar las notificaciones de propiedades de los activos (AWS CLI)

- Consulta de mensajes de notificación sobre propiedades de los activos

Habilitación de notificaciones de las propiedades de activos (consola)

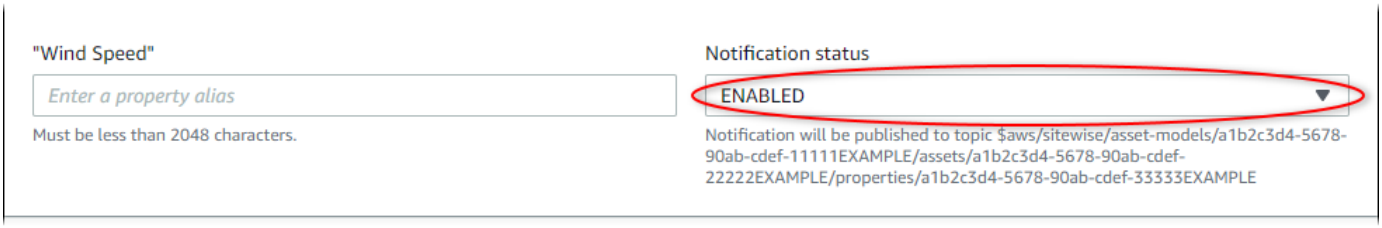
De forma predeterminada, AWS IoT SiteWise no publica las actualizaciones del valor de la propiedad. Puede utilizar la AWS IoT SiteWise consola para activar las notificaciones de una propiedad de un activo.

Para habilitar o desactivar las notificaciones de la propiedad de un activo (consola)

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija activos.
3. Elija el activo para habilitar las notificaciones de una propiedad.

> **Tip**
>
> Puede elegir el icono de flecha para expandir una jerarquía de activos y encontrar su activo.

4. Seleccione Editar.
5. Para el Estado de la notificación de la propiedad del activo, elija HABILITADO.



También puede elegir DESHABILITADO para desactivar las notificaciones de la propiedad del activo.

6. Seleccione Guardar.

Habilitar las notificaciones de propiedades de los activos (AWS CLI)

De forma predeterminada, AWS IoT SiteWise no publica las actualizaciones del valor de la propiedad. Puede utilizar el AWS Command Line Interface (AWS CLI) para activar o desactivar las notificaciones de una propiedad de un activo.

Debe conocer los `assetId` de sus activos y los `propertyId` de las propiedades para completar este procedimiento. También puede utilizar el identificador externo. Si has creado un activo y no lo sabes`assetId`, usa la ListAssetsAPI para enumerar todos los activos de un modelo específico. Utilice la DescribeAssetoperación para ver las propiedades de su activo, incluidos los identificadores de propiedad.

Utilice la UpdateAssetPropertyoperación para activar o desactivar las notificaciones de una propiedad de un activo. Especifique los siguientes parámetros:

- `assetId`: el ID del activo.
- `propertyId`: el ID de la propiedad del activo.
- `propertyNotificationState`: el estado de notificación del valor de la propiedad, `ENABLED` o `DISABLED`.
- `propertyAlias`: el alias de la propiedad. Especifique el alias existente de la propiedad cuando actualice el estado de notificación. Si omite este parámetro, se elimina el alias existente de la propiedad.

Para habilitar o desactivar las notificaciones de la propiedad de un activo (CLI)

1. Ejecute el siguiente comando para recuperar el alias de la propiedad del activo. Reemplace *`asset-id`* por el ID del activo y *`property-id`* por el ID de la propiedad.

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

   La operación devuelve una respuesta que contiene detalles de la propiedad del activo en el siguiente formato. El alias de propiedad se encuentra en `assetProperty.alias` en el objeto 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. Ejecute el siguiente comando para habilitar las notificaciones de la propiedad del activo. Reemplace *`property-alias`* por el alias de propiedad de la respuesta del comando anterior u omita `--property-alias` para actualizar la propiedad sin un alias.

```
aws iotsitewise update-asset-property \
  --asset-id asset-id \
  --property-id property-id \
  --property-notification-state ENABLED \
  --property-alias property-alias
```

   También puede pasar `--property-notification-state DISABLED` para desactivar las notificaciones de la propiedad del activo.

Consulta de mensajes de notificación sobre propiedades de los activos

Para consultar las notificaciones de propiedades de los activos, cree AWS IoT Core reglas compuestas por sentencias SQL.

AWS IoT SiteWise publica las actualizaciones de los datos de propiedades de los activos en AWS IoT Core en el siguiente 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"
        }
      }
    ]
  }
}
```

Cada estructura de la `values` lista es una estructura timestamp-quality-value (TQV).

- El `timestamp` contiene el tiempo actual en formato de tiempo Unix en segundos con desplazamiento en nanosegundos.
- `quality` contiene una de las siguientes cadenas, que indican la calidad del punto de datos:
  - `GOOD`: los datos no se ven afectados por ningún problema.
  - `BAD`: los datos se ven afectados por un problema, como un fallo del sensor.
  - `UNCERTAIN`: los datos se ven afectados por un problema, como la falta de precisión de un sensor.
- El `value` contiene uno de los siguientes campos, en función del tipo de propiedad:
  - `booleanValue`
  - `doubleValue`
  - `integerValue`
  - `stringValue`

Para analizar valores fuera de la matriz `values`, debe usar consultas complejas de objetos anidados en las instrucciones SQL de sus reglas. Para obtener más información, consulte Consultas de objetos anidados en la Guía para desarrolladores de AWS IoT , o consulte el tutorial de Publicar actualizaciones de valor de propiedad en Amazon DynamoDB para ver un ejemplo concreto de análisis sintáctico de mensajes de notificación de propiedades de activo.

Example Consulta de ejemplo para extraer la matriz de valores

La siguiente instrucción demuestra cómo consultar la matriz de valores de propiedad actualizados para una propiedad de tipo doble específica en todos los activos con esa propiedad.

```
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'
```

La instrucción de consulta de regla anterior genera los datos con el siguiente formato.

```
{
  "windspeed": [
    26.32020195042838,
    26.282584572975477,
    26.352566977372508,
    26.283084346171442,
    26.571883739599322,
    26.60684140743005,
    26.628738636715045,
    26.273486932802125,
    26.436379105473964,
    26.600590095377303
  ]
}
```

Example Consulta de ejemplo para extraer un solo valor

La siguiente instrucción demuestra cómo consultar el primer valor de la matriz de valores de propiedad para una propiedad de tipo doble específica en todos los activos con esa propiedad.

```
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'
```

La instrucción de consulta de regla anterior genera los datos con el siguiente formato.

```
{
  "windspeed": 26.32020195042838
}
```

> **Important**
>
> Esta instrucción de consulta de regla ignora las actualizaciones de valores distintas de la primera en cada lote. Cada lote puede contener hasta 10 valores. Si necesita incluir los valores restantes, debe configurar una solución más compleja para generar valores de propiedad de activos a otros servicios. Por ejemplo, puede configurar una regla con una AWS Lambda acción para volver a publicar cada valor de la matriz en otro tema y configurar otra regla para consultar ese tema y publicar cada valor en la acción de regla deseada.

Exporte datos a Amazon S3 con notificaciones de propiedad de activos

Puede exportar los datos entrantes AWS IoT SiteWise a un bucket de Amazon S3 de su cuenta. Puede realizar una copia de seguridad de los datos en un formato que le permita crear informes históricos o para analizar los datos con métodos complejos.

> **Note**
>
> AWS IoT SiteWise también es compatible con el almacenamiento de capa fría que le permite guardar datos en un bucket de Amazon S3 gestionado por el cliente. Para obtener más información acerca de los niveles de almacenamiento admitidos, consulte Administrar el almacenamiento de datos.

AWS IoT SiteWise proporciona esta función como plantilla. AWS CloudFormation Al crear una pila a partir de la plantilla, AWS CloudFormation crea los AWS recursos necesarios para transmitir los datos entrantes desde AWS IoT SiteWise un depósito de S3.

A continuación, el depósito de S3 recibe todos los datos de propiedad de los activos enviados desde los mensajes de actualización del valor de la AWS IoT SiteWise propiedad. El bucket de S3

también recibe los metadatos de los activos, que incluyen nombres de activos y de propiedades y otra información.

Para obtener más información acerca de cómo habilitar los mensajes de actualización de valor de propiedad para las propiedades de activos que se van exportar a Amazon S3, consulte Interacción con otros AWS servicios..

Esta característica almacena los datos de propiedades de activos y los metadatos de activos en Amazon S3 en formato Apache Parquet. Parquet es un formato de datos en columnas que ahorra espacio y permite realizar consultas más rápidas en comparación con los formatos orientados a filas como JSON.

> **Note**
>
> Cuando esta característica recupera metadatos de activos, admite hasta unos 1500 activos. Esta limitación solo se aplica a los metadatos de activos. Esta limitación no se aplica al número de activos admitidos cuando la característica exporta datos de propiedades de activos.

El nombre de cada recurso incluye un prefijo que se puede personalizar al crear la pila. A continuación presentamos algunos ejemplos:

- Un bucket de Amazon S3.
- AWS Lambda funciones
- ¿Una AWS IoT Core regla
- AWS Identity and Access Management roles
- Una transmisión de Amazon Data Firehose
- ¿ AWS Glue Una base de datos

Para ver una lista completa, consulte Recursos creados a partir de la plantilla.

> **Important**
>
> Se le cobrará por los recursos que cree y consuma esta AWS CloudFormation plantilla. Estos cargos incluyen el almacenamiento y la transferencia de datos para varios AWS servicios.

Temas

Crea la AWS CloudFormation pila

Debe crear una pila AWS CloudFormation para exportar los datos de sus activos a Amazon S3.

Exportar datos a Amazon S3

1. Abra la Plantilla de AWS CloudFormation e inicie sesión en la AWS Management Console.
2. En la página Create stack (Crear pila) elija Next (Siguiente) en la parte inferior de la página.
3. En la página Especificar los detalles de la pila, introduzca una BucketNamepara el depósito de S3 que crea esta plantilla para recibir los datos de los activos. El nombre del bucket tiene que ser único de forma global. Para obtener más información, consulte Reglas para nombrar buckets en la Guía del usuario de Amazon Simple Storage Service.
4. (Opcional) Cambie cualquiera de los demás parámetros de la plantilla:
   - GlobalResourcePrefix: prefijo para los nombres de los recursos globales, como los roles de IAM, creados a partir de esta plantilla.
   - LocalResourcePrefix: prefijo para los nombres de los recursos creados a partir de esta plantilla en la región actual.

   > **Note**
   >
   > Si crea esta plantilla varias veces, debería cambiar el nombre del bucket y los parámetros del prefijo del recurso para evitar conflictos de nombres de recursos.
5. Elija Siguiente.
6. En la página Configurar opciones de pila, elija Siguiente.
7. En la parte inferior de la página, active la casilla de verificación que indica Reconozco que AWS CloudFormation podría crear recursos de IAM.
8. Seleccione Crear pila.

La pila tarda unos minutos en crearse. Si la pila no se crea, es posible que su cuenta no tenga permisos suficientes o que haya escrito un nombre de bucket que ya existe. Siga estos pasos para eliminar la pila e inténtelo de nuevo:

a. Elija Delete (Eliminar) en la esquina superior derecha.

   La pila tarda unos minutos en borrarse.

   > **Note**
   >
   > AWS CloudFormation no elimina los depósitos ni los grupos de CloudWatch registros de S3. Puede eliminar estos recursos en las consolas de esos servicios.

b. Si la pila no se elimina, elija Delete (Eliminar) de nuevo.

c. Si la pila no se vuelve a eliminar, sigue los pasos de la AWS CloudFormation consola para omitir los recursos que no se pudieron eliminar e inténtalo de nuevo.

9. Una vez que la AWS CloudFormation pila se haya creado correctamente, siga el siguiente procedimiento para explorar los datos de propiedades de sus activos en Amazon S3.

> **Important**
>
> Tras crear la pila, podrá ver los nuevos recursos de su AWS cuenta. Esta característica podría dejar de funcionar correctamente si elimina o modifica estos recursos. Se recomienda que no modifique estos recursos a menos que desee dejar de enviar datos al bucket o personalizar esta característica.

Vea sus datos en Amazon S3

Después de crear la característica, puede ver los datos de propiedades de activos y los metadatos de activos en Amazon S3.

> **Note**
>
> Los metadatos de activos se actualizan cada seis horas. Es posible que tenga que esperar hasta seis horas para ver que los metadatos de activos aparecen en el bucket de S3.

Esta característica almacena datos de propiedades de activos en las columnas siguientes, donde cada fila contiene un punto de datos:

- tipo: el tipo de notificación de la propiedad (`PropertyValueUpdate`).
- asset_id: el ID del activo que recibió un punto de datos.
- asset_property_id: el ID de la propiedad que recibió un punto de datos para el activo.
- time_in_seconds: hora a la que se recibieron los datos, expresada en segundos, en formato Unix.
- offset_in_nanos: el desfase en nanosegundos respecto a `timeInSeconds`.
- asset_property_quality: la calidad del punto de datos: `GOOD`, `UNCERTAIN` o `BAD`.
- asset_property_value: el valor del punto de datos.
- asset_property_data_type: el tipo de datos de la propiedad del activo: `boolean`, `double`, `integer` o `string`.

Esta característica almacena metadatos de activos en las columnas siguientes, donde cada fila contiene una propiedad de activo:

- asset_id: el ID del activo.
- asset_name: el nombre del activo.
- asset_model_id: el ID del modelo de activos.
- asset_property_id: el ID de la propiedad del activo.
- asset_property_name: el nombre de la propiedad del activo.
- asset_property_data_type: el tipo de datos de la propiedad del activo: `BOOLEAN`, `DOUBLE`, `INTEGER` o `STRING`.
- asset_property_unit: la unidad de la propiedad del activo.
- asset_property_alias: el alias de la propiedad del activo.

Para ver sus AWS IoT SiteWise datos en Amazon S3

1. Vaya a la consola de Amazon S3.
2. En la lista de buckets, elija el bucket con el nombre que eligió al crear la plantilla.
3. En el bucket, elija una de las siguientes carpetas:

   - `asset-property-updates`— Esta carpeta contiene los datos de propiedades de los activos exportados desde AWS IoT SiteWise.

- `asset-metadata`— Esta carpeta contiene los detalles de los activos exportados desde AWS IoT SiteWise.

4. Elija el objeto que desea ver.
5. En la página del objeto, haga lo siguiente:

   a. Elija la pestaña Select from (Seleccionar desde).

      En este panel, puede obtener una vista previa de los registros de archivos Parquet.

   b. En File format (Formato de archivo), elija Parquet.

   c. Elija Mostrar vista previa del archivo para mostrar el contenido del archivo en formato JSON.

> **Note**
>
> Si no aparecen nuevos datos en el bucket, compruebe que haya habilitado las notificaciones de actualización de valor de propiedad para las propiedades de los activos. Para obtener más información, consulte Interacción con otros AWS servicios.

Para obtener más información acerca de cómo analizar los datos de activos almacenados en el bucket de S3, consulte Analice los datos exportados con Amazon Athena.

Analice los datos exportados con Amazon Athena

Una vez que tenga los datos de propiedades de sus activos en Amazon S3, puede utilizar varios AWS servicios para generar informes o analizar y consultar sus datos:

- Ejecute consultas SQL en los datos con Amazon Athena.
- Realice análisis de macrodatos con Amazon EMR.
- Busca y analiza tus datos con Amazon OpenSearch Service.

Puede encontrar otros AWS servicios que pueden interactuar con sus datos en Amazon S3 en la sección Análisis de AWS Management Console.

> **Note**
>
> La pila crea una AWS Glue base de datos para formatear los datos de propiedades de los activos. No puede consultar esta base de datos para datos de activos. Siga los pasos de esta sección para crear una AWS Glue base de datos que pueda consultar.

En este tutorial, aprenderá a configurar los requisitos previos para usar Amazon Athena y a usar Athena para ejecutar consultas SQL en los datos de activos exportados. AWS IoT SiteWise Para consultar datos con Athena, primero debe rellenarlos AWS Glue Data Catalog con los datos de sus activos. El catálogo de datos contiene bases de datos y tablas, y Athena puede acceder a los datos del catálogo de datos. Puede crear un AWS Glue rastreador que actualice periódicamente el catálogo de datos con los datos de activos exportados.

Temas

Configuración de un rastreador para rellenar el AWS Glue Data Catalog

AWS Glue los rastreadores rastrean los almacenes de datos para rellenar las tablas del. AWS Glue Data Catalog En este procedimiento, creará y ejecutará un AWS Glue rastreador para su bucket de S3 que contenga los datos de activos exportados. El rastreador crea una tabla para actualizaciones de propiedades de activos y una tabla para metadatos de activos. A continuación, puede realizar consultas SQL en estas tablas con Athena. Para obtener más información, consulte Rellenar el AWS Glue Data Catalog y Definir rastreadores en la Guía para desarrolladores de AWS Glue .

Para crear un rastreador AWS Glue

1. Vaya a la consola de AWS Glue.
2. En el panel de navegación, elija Crawlers (Rastreadores).
3. Elija Add crawler (Agregar rastreador).
4. En la página Add crawler (Agregar rastreador) haga lo siguiente:
    a. Escriba un nombre para el rastreador, como **`IoTSiteWiseDataCrawler`** y a continuación, elija Next (Siguiente).

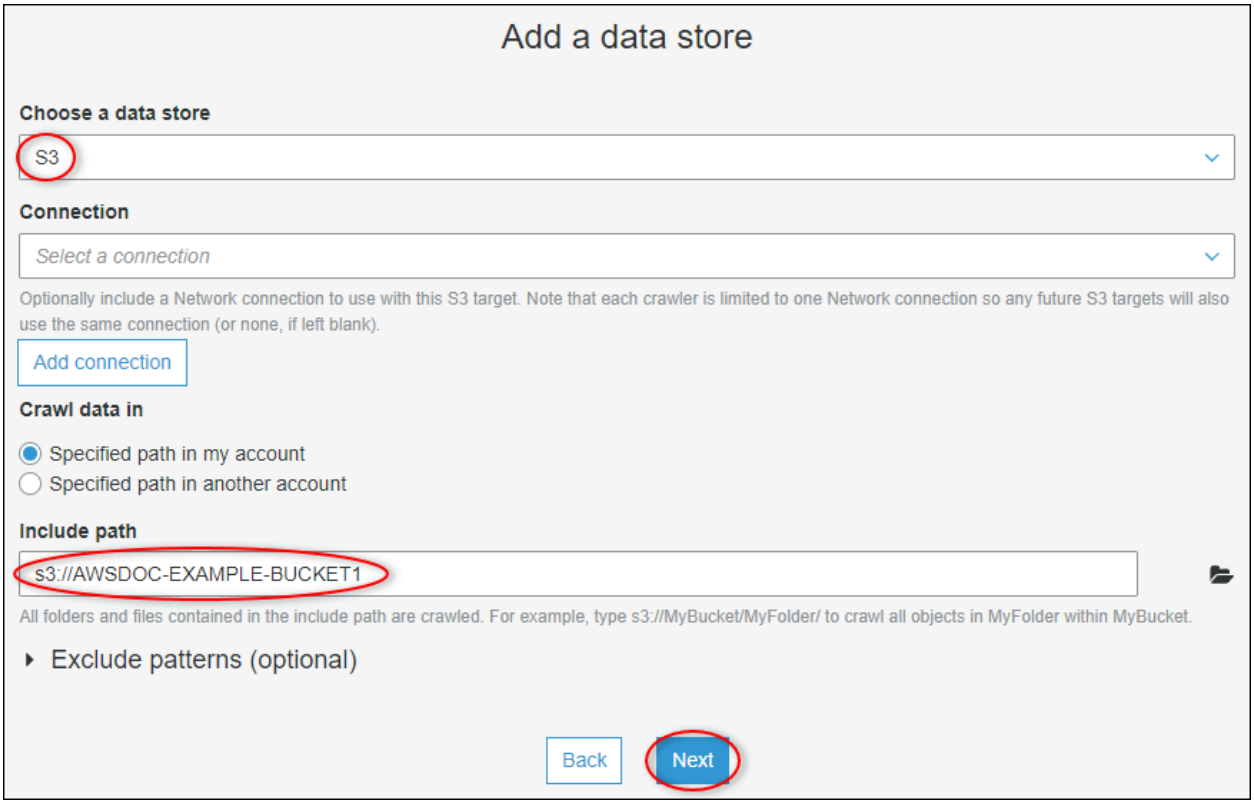
b. Para Crawler source type (Tipo de origen del rastreador), elija Data stores (Almacenes de datos) y a continuación, elija Next (Siguiente).

c. En la página Add a data store (Agregar un almacén de datos), haga lo siguiente:

   i. En Elegir un almacén de datos, elija S3.

   ii. En Include path (Incluir ruta), escriba **s3://*DOC-EXAMPLE-BUCKET1*** para agregar el bucket de datos de activos como almacén de datos. Reemplace *DOC-EXAMPLE-BUCKET1* por el nombre del bucket que eligió al crear la pila.

   iii. Elija Siguiente.



d. En la página Add another data store (Agregar otro almacén de datos) elija No y a continuación, elija Next (Siguiente).

e. En la página Elegir un rol de IAM haga lo siguiente:

   i. Para crear un nuevo rol de servicio que permita acceder AWS Glue al bucket de S3, elija Crear un rol de IAM.

   ii. Escriba un sufijo para el nombre del rol, como **`IoTSiteWiseDataCrawler`**.

   iii. Elija Siguiente.

f. En Frequency (Frecuencia), elija Hourly (cada hora) y a continuación, elija Next (Siguiente). El rastreador actualiza las tablas con nuevos datos cada vez que se ejecuta, de modo que puede elegir cualquier frecuencia que se ajuste a su caso de uso.

g. En la página Configure the crawler's output (Configurar la salida del rastreador) haga lo siguiente:

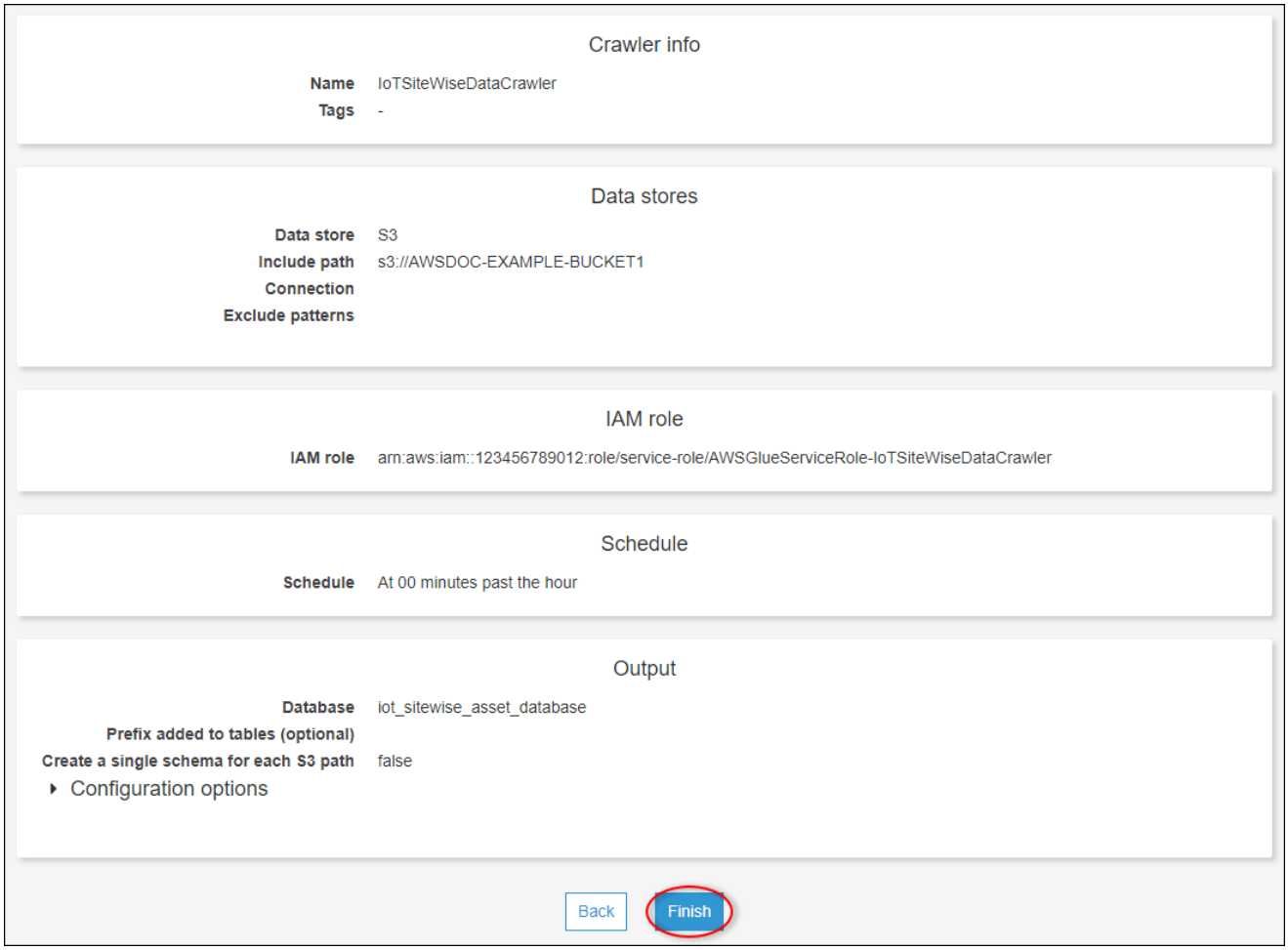
   i. Seleccione Añadir base de datos para crear una AWS Glue base de datos para los datos de sus activos.

   ii. Escriba un nombre para la base de datos, como **`iot_sitewise_asset_database`**.

   iii. Seleccione Crear.

   iv. Elija Siguiente.

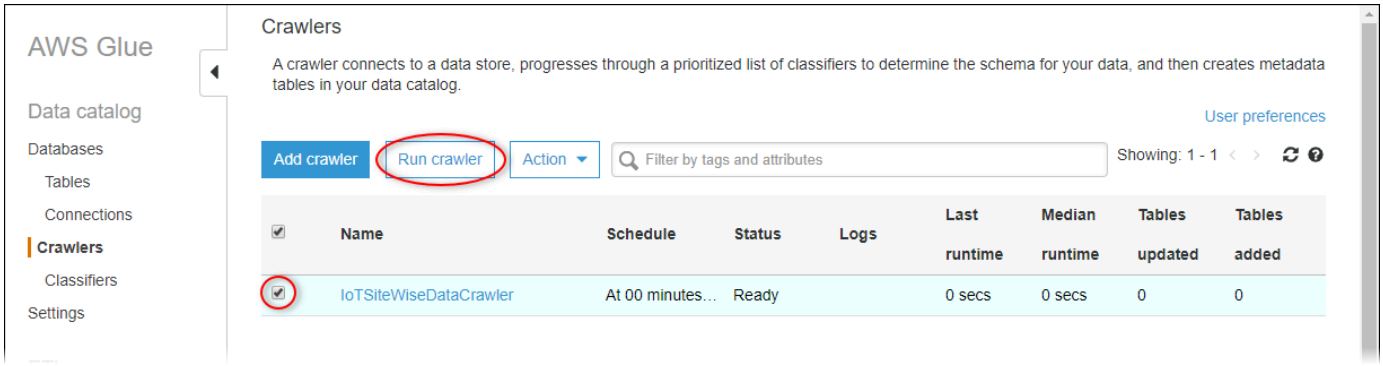
h. Revise los detalles del rastreador y, a continuación, elija Finish (Finalizar).



De forma predeterminada, el nuevo rastreador no se ejecuta inmediatamente. Debe ejecutarlo manualmente o esperar hasta que se ejecute según su programación configurada.

Para ejecutar un rastreador

1. En la página Crawlers (Rastreadores) active la casilla de verificación del nuevo rastreador y a continuación, elija Run crawler (Ejecutar rastreador).



2. Espere hasta que finalice el rastreador y tenga el estado Ready (Listo).

   El rastreador puede tardar varios minutos en ejecutarse y su estado se actualiza automáticamente.

3. En el panel de navegación, elija Tablas.

   Debería ver dos tablas nuevas: asset_metadata y asset_property_updates.

Consulta de datos con Athena

Athena descubre automáticamente las tablas de datos de sus activos en. AWS Glue Data Catalog Para realizar consultas en la intersección de estas tablas, puede crear una vista, que es una tabla de datos lógicos. Para obtener más información, consulte Uso con vistas en la Guía del usuario de Amazon Athena.

Después de crear una vista que combine datos de propiedades de activos y metadatos, puede ejecutar consultas que generen valores de propiedades con nombres de activos y propiedades adjuntos. Si desea obtener más información, consulte Ejecución de consultas SQL mediante Amazon Athena en la Guía del usuario de Amazon Athena.

Para consultar datos de activos con Athena

1. Vaya a la consola de Athena.

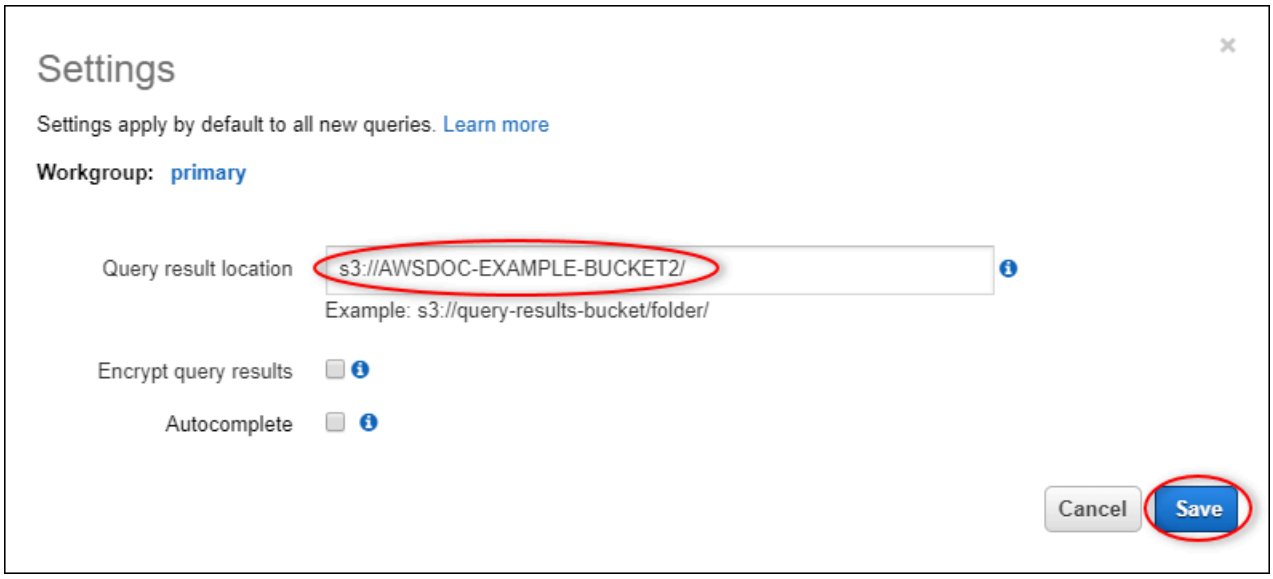
   Si aparece la página Getting started (Introducción) elija Get Started (Empezar).

2. Si está utilizando Athena por primera vez, siga los siguientes pasos para configurar un bucket de S3 para almacenar los resultados de consultas. Athena almacena los resultados de sus consultas en este bucket.

> **Important**
>
> Utilice un bucket diferente al del bucket de datos de activos, de modo que el rastreador que creó anteriormente no rastree los resultados de la consulta. Se recomienda crear un bucket para utilizarlo solo para los resultados de la consulta de Athena. Para obtener más información, consulte ¿Cómo creo un bucket de S3? en la Guía del usuario de Amazon Simple Storage Service.

   a. Elija Configuración.

   b. En Ubicación de resultados de consulta, escriba el bucket de S3 para los resultados de la consulta de Athena. El bucket debe terminar con /.

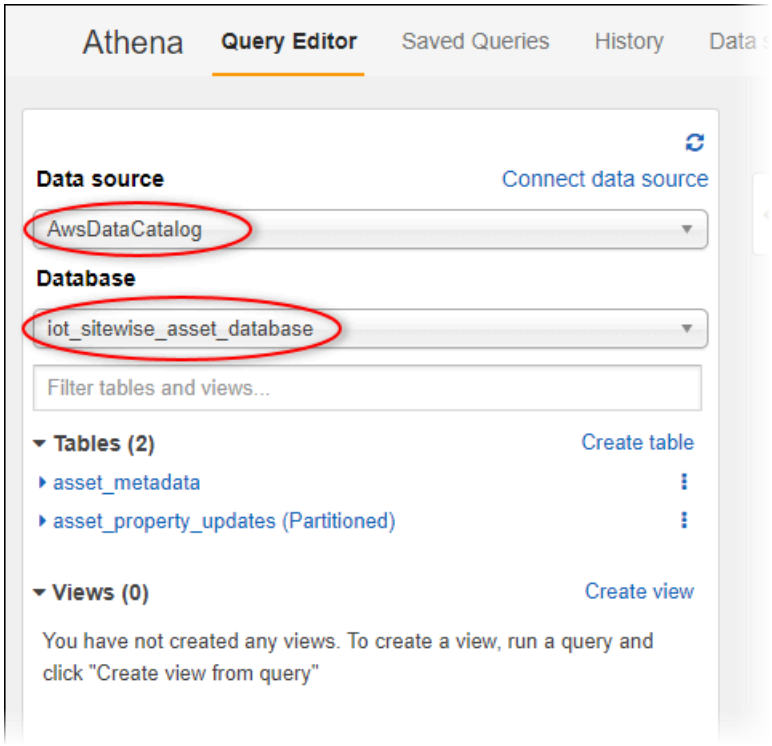


   c. Seleccione Guardar.

3. El panel izquierdo contiene el origen de datos que desea consultar. Haga lo siguiente:

   a. Para la fuente de datos, elija AwsDataCatalogutilizar la AWS Glue Data Catalog.

   b. En Base de datos, elija la AWS Glue base de datos que creó con el rastreador.



Debería ver dos tablas: asset_metadata yasset_property_updates.

4. Para crear una vista a partir de la combinación de datos y metadatos de propiedades de activos, escriba la siguiente consulta y a continuación, elija Run query (Ejecutar consulta).

```
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") ) );
```

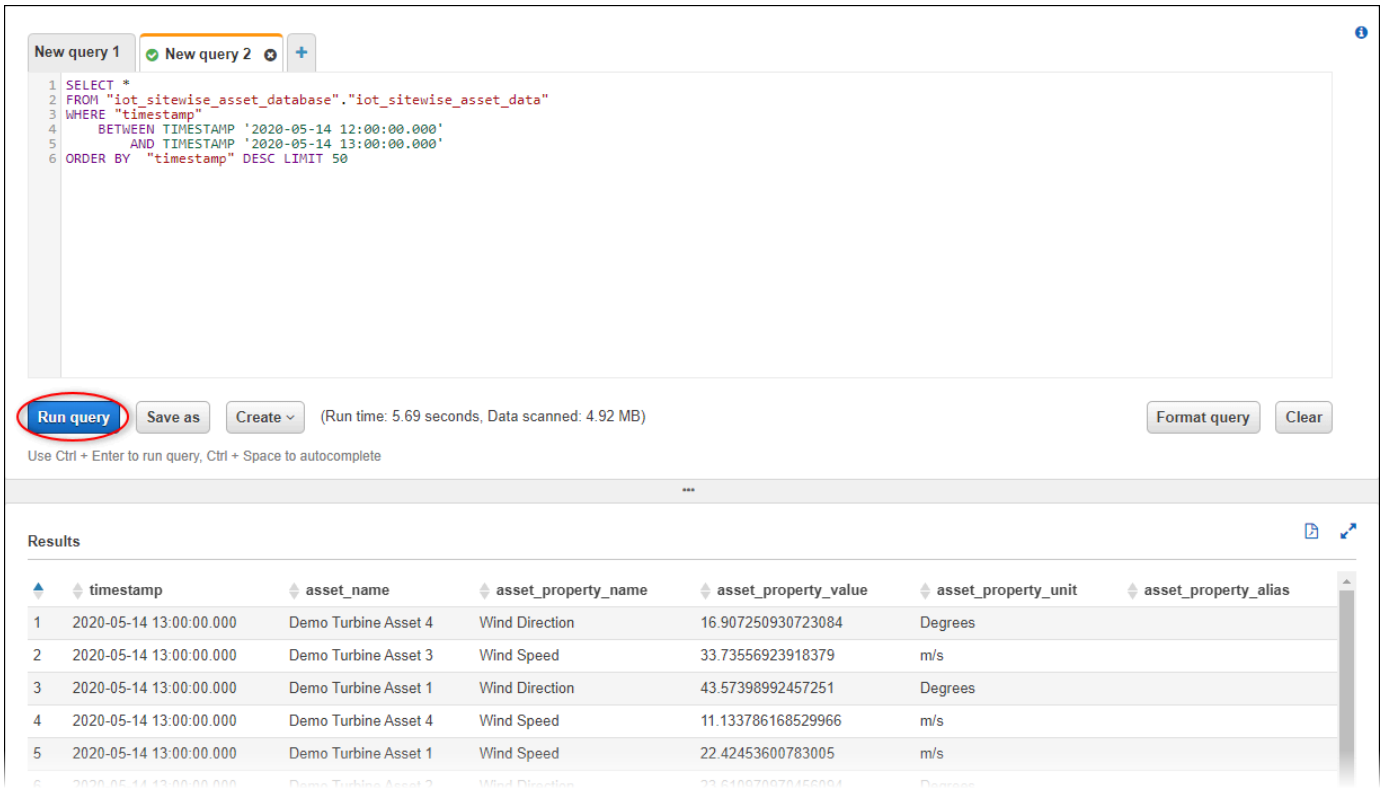
Esta consulta une los datos de propiedad de activos y las tablas de metadatos en el ID de activo y el ID de propiedad para crear una vista. Puede ejecutar esta consulta varias veces porque reemplaza la vista existente si la vista ya existe.

5. Elija el icono + para agregar una nueva consulta.
6. Para ver un ejemplo de datos de activos, escriba la siguiente consulta y a continuación, elija Run query (Ejecutar consulta). Reemplace las marcas de tiempo por un intervalo para el que el bucket tenga datos.

```
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;
```

Esta consulta genera hasta 50 puntos de datos entre dos marcas de tiempo, con las entradas más recientes mostradas primero.

El resultado de la consulta puede ser similar a los siguientes resultados.



Ahora puede ejecutar consultas útiles para su AWS IoT SiteWise aplicación. Para obtener más información, consulte Referencia SQL para Amazon Athena en la Guía del usuario de Amazon Athena.

Recursos creados a partir de la plantilla

Al crear una pila a partir de la plantilla, AWS CloudFormation crea los siguientes recursos. La mayoría de los nombres de los recursos incluyen un prefijo que puede personalizar al crear la pila.

Parámetros del nombre del recurso

- `BucketName`: el nombre del bucket de S3 creado a partir de esta plantilla que recibe los datos del activo.
- `GlobalResourcePrefix`: prefijo para los nombres de los recursos globales creados a partir de esta plantilla. El valor predeterminado es `sitewise-export-to-s3`.
- `LocalResourcePrefix`: prefijo para los nombres de los recursos creados a partir de esta plantilla en la región actual. El valor predeterminado es `sitewise_export_to_s3`.

Recursos creados por la AWS CloudFormation plantilla

Recurso	Descripción	Nombre
Bucket de S3 para datos procesados	Este bucket contiene dos carpetas. Una carpeta recibe los datos aplanados y formateados del flujo de entrega de Firehose y la otra carpeta recibe los metadatos de los activos.	`${BucketName}`
Base de datos de AWS Glue	Esta base de datos contiene la AWS Glue tabla que crea esta pila.	`${LocalResourcePrefix}_firehose_glue_database`
Tabla de AWS Glue	El flujo de entrega de Firehose utiliza esta tabla para formatear los datos en formato Parquet.	`${LocalResourcePrefix}_firehose_glue_table`
Función AWS Lambda que transforma los datos	Esta función aplana la matriz de valores de los mensajes de notificación del valor de la	`${LocalResourcePrefix}_lambda_transform_function`

Recurso	Descripción	Nombre
	propiedad desde los que se envían. AWS IoT SiteWise	
Rol de IAM de la función de Lambda de transformación	Este rol permite que Lambda almacene registros de tiempo de ejecución para la función de transformación.	`${GlobalResourcePrefix}-lambda-transform-role`
Política de IAM para el rol de la función de Lambda de transformación	Esta política permite a Lambda almacenar registros de ejecución para la función de transformación.	`${GlobalResourcePrefix}-lambda-transform-policy`
CloudWatch Registra el grupo de registros para la función de transformación	Este grupo de registros contiene registros para la función de transformación.	`/aws/lambda/${LocalResourcePrefix}_lambda_transform_function`
Función de Lambda que recopila metadatos de activos	Esta función recupera los detalles sobre los activos AWS IoT SiteWise y los almacena en un bucket de Amazon S3 que crea esta pila.	`${LocalResourcePrefix}_lambda_metadata_function`
Capa de Lambda para la función de metadatos	Esta capa proporciona un AWS SDK que contiene AWS IoT SiteWise las operaciones que utiliza la función de metadatos.	`${LocalResourcePrefix}_lambda_metadata_layer`
Rol de IAM para la función de Lambda de metadatos	Esta función permite a Lambda recuperar detalles sobre los activos en. AWS IoT SiteWise	`${GlobalResourcePrefix}-lambda-metadata-role`

Recurso	Descripción	Nombre
Política de IAM para el rol de función de Lambda de metadatos	Esta política permite a Lambda recuperar detalles sobre los activos en. AWS IoT SiteWise	`${GlobalResourcePrefix}-lambda-metadata-policy`
EventBridgeevento programado para la función Lambda de metadatos	Este evento programado ejecuta los metadatos de Lambda cada 6 horas para actualizar el bucket de metadatos de activos.	`${LocalResourcePrefix}-metadata-event`
CloudWatch Registra el grupo de registros para la función de metadatos	Este grupo de registros contiene registros para la función de metadatos.	`/aws/lambda/${LocalResourcePrefix}_lambda_metadata_function`
Regla de AWS IoT	Esta regla consulta los mensajes de notificación del valor de la propiedad y envía los datos de los activos a una transmisión de entrega de Amazon Data Firehose.	`${LocalResourcePrefix}_iot_topic_rule`
Función de IAM para la regla AWS IoT	Esta función permite AWS IoT enviar datos al flujo de entrega de Firehose.	`${GlobalResourcePrefix}-core-firehose-role`
Política de IAM para el rol de regla AWS IoT	Esta política permite AWS IoT enviar datos al flujo de entrega de Firehose.	`${GlobalResourcePrefix}-core-firehose-policy`
Flujo de entrega de Firehose	Esta transmisión de entrega consume datos de la AWS IoT regla, aplana los datos con una función Lambda y entrega los datos a Amazon S3.	`${LocalResourcePrefix}_firehose_delivery_stream`

Recurso	Descripción	Nombre
Rol de IAM para el flujo de entrega	Esta función permite a Firehose realizar operaciones en el depósito, la AWS Glue tabla, las funciones de Lambda y CloudWatch el grupo de registros de S3.	`${GlobalResourcePrefix}-firehose-delivery-role`
CloudWatch Registra el grupo de registros para el flujo de entrega	Este grupo de registros contiene un flujo de registros ,`S3 Delivery`, que recibe registros sobre el flujo de entrega de Firehose.	`/aws/kinesisfirehose/${LocalResourcePrefix}_firehose_delivery_stream`

Integración con Grafana

Grafana es una plataforma de visualización de datos que puede utilizar para visualizar y monitorear datos en paneles de control. En la versión 7.3.0 y posteriores de Grafana, puede utilizar el complemento de AWS IoT SiteWise para visualizar sus datos de activos de AWS IoT SiteWise en los paneles de control de Grafana. Puede visualizar datos de varias AWS fuentes (como AWS IoT SiteWise Amazon Timestream y CloudWatch Amazon) y otras fuentes de datos con un único panel de Grafana.

Tiene dos opciones para utilizar el complemento de AWS IoT SiteWise:

- Servidores locales de Grafana

  Puede configurar el complemento de AWS IoT SiteWise en un servidor de Grafana que usted administre. Para obtener más información sobre cómo añadir y usar el complemento, consulta el archivo README de la AWS IoT SiteWise fuente de datos en el sitio web. GitHub

- Servicio administrado de AWS para Grafana

  Puede utilizar el complemento de AWS IoT SiteWise en AWS Managed Service for Grafana (AMG). AMG administra los servidores de Grafana por usted para que pueda visualizar sus datos sin tener que construir, empaquetar ni implementar ningún hardware ni cualquier otra

infraestructura de Grafana. Para obtener más información, consulte los siguientes temas en la Guía del usuario de AWS Managed Service for Grafana:

- ¿Qué es Amazon Managed Service for Grafana (AMG)?
- Uso del origen de datos de AWS IoT SiteWise

Example Ejemplo de panel de control de Grafana

El siguiente panel de control de Grafana visualiza el parque eólico de demostración. Puede acceder a este panel de control de demostración en el sitio web Grafana Play.

Integración de AWS IoT SiteWise y AWS IoT TwinMaker

La integración con AWS IoT TwinMaker proporciona acceso a funciones sólidasAWS IoT SiteWise, como la `ExecuteQuery` API de recuperación de AWS IoT SiteWise datos y la búsqueda avanzada de activos en la AWS IoT SiteWise consola. Para integrar los servicios y utilizar estas funciones, primero debe habilitar la integración.

Temas

Habilitación de la integración

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones. El elemento `Action` de una política JSON describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Para obtener más información sobre las acciones admitidas por AWS IoT SiteWise, consulte Acciones definidas por AWS IoT SiteWise en la Referencia de autorización de servicios.

Para obtener más información sobre las funciones AWS IoT TwinMaker vinculadas a servicios, consulte Funciones vinculadas a servicios AWS IoT TwinMaker en la Guía del usuario. AWS IoT TwinMaker

Antes de poder realizar la integración AWS IoT SiteWiseAWS IoT TwinMaker, debe conceder los siguientes permisos que le permitan integrarse en un espacio de trabajo AWS IoT SiteWise vinculado: AWS IoT TwinMaker

- `iotsitewise:EnableSiteWiseIntegration`— Permite AWS IoT SiteWise integrarse con un espacio de AWS IoT TwinMaker trabajo vinculado. Esta integración permite AWS IoT TwinMaker leer toda la información de modelado AWS IoT SiteWise a través de una función AWS IoT TwinMaker vinculada al servicio. Para habilitar este permiso, añada la siguiente política a su función de IAM:

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

```
      "Effect": "Allow",
      "Action": [
        "iotsitewise:EnableSiteWiseIntegration"
      ],
      "Resource": "*"
    }
  ]
}
```

Integración de AWS IoT SiteWise y AWS IoT TwinMaker

Para integrarlo AWS IoT SiteWiseAWS IoT TwinMaker, debe tener lo siguiente:

- AWS IoT SiteWisefunción vinculada al servicio configurada en su cuenta
- AWS IoT TwinMakerfunción vinculada a un servicio configurada en tu cuenta
- AWS IoT TwinMakerespacio de trabajo con un ID `IoTSiteWiseDefaultWorkspace` en tu cuenta en la región.

Para integrarlo mediante la AWS IoT SiteWise consola

Cuando veas el AWS IoT TwinMaker banner Integrar con en la consola, selecciona Conceder permiso. Los requisitos previos se crean en su cuenta.

Para realizar la integración mediante el AWS CLI

Para integrar AWS IoT SiteWise y AWS IoT TwinMaker utilizar elAWS CLI, introduzca los siguientes comandos:

1. Llame `CreateServiceLinkedRole` con un `AWSServiceName` `deiotsitewise.amazonaws.com`.

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

2. Llama `CreateServiceLinkedRole` con un `AWSServiceName` of `iottwinmaker.amazonaws.com`.

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

3. Llama `CreateWorkspace` con un `ID` of`IoTSiteWiseDefaultWorkspace`.

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

Detección de anomalías en los equipos con Amazon Lookout for Equipment

> **Note**
>
> La detección de anomalías solo está disponible en las regiones en las que está disponible Amazon Lookout for Equipment.

Puede realizar la integración AWS IoT SiteWise con Amazon Lookout for Equipment para obtener información sobre sus equipos industriales mediante la detección de anomalías y el mantenimiento predictivo de los equipos industriales. Lookout for Equipment es un servicio de aprendizaje automático (ML) para monitorear equipos industriales que detecta un comportamiento anormal del equipo e identifica posibles fallas. Con Lookout for Equipment, puede implementar programas de mantenimiento predictivo e identificar los procesos de los equipos que no son óptimos. Para obtener más información sobre Lookout for Equipment, consulta ¿Qué es Amazon Lookout for Equipment? en la Guía del usuario de Amazon Lookout for Equipment.

Al crear una predicción para entrenar un modelo de aprendizaje automático a fin de detectar el comportamiento anómalo del equipo, AWS IoT SiteWise envía los valores de las propiedades de los activos a Lookout for Equipment para entrenar un modelo de aprendizaje automático a fin de detectar el comportamiento anómalo del equipo. Para definir una definición de predicción en un modelo de activos, debe especificar las funciones de IAM necesarias para que Lookout for Equipment acceda a sus datos y las propiedades que envíe a Lookout for Equipment y envíe los datos procesados a Amazon S3. Para obtener más información, consulte Creación de modelos de activos.

Para integrar AWS IoT SiteWise Lookout for Equipment, realizarás los siguientes pasos de alto nivel:

- Añada una definición de predicción a un modelo de activos que describa las propiedades de las que quiere hacer un seguimiento. La definición de predicción es un conjunto reutilizable de medidas, transformaciones y métricas que se utiliza para crear predicciones sobre los activos que se basan en ese modelo de activos.
- Entrene la predicción en función de los datos históricos que proporcione.

- Programa la inferencia, que indica la AWS IoT SiteWise frecuencia con la que se debe ejecutar una predicción específica.

Una vez programada la inferencia, el modelo Lookout for Equipment monitorea los datos que recibe de su equipo y busca anomalías en el comportamiento del equipo. Puede ver y analizar los resultados en SiteWise Monitor, mediante las operaciones de la API AWS IoT SiteWise GET o la consola Lookout for Equipment. También puede crear alarmas utilizando detectores de alarmas del modelo de activos para alertarlo sobre el comportamiento anormal del equipo.

Temas

Añadir una definición de predicción (consola)

Para empezar a enviar los datos recopilados por AWS IoT SiteWise Lookout for Equipment, debes añadir AWS IoT SiteWise una definición de predicción a un modelo de activos.

Para añadir una definición de predicción a un modelo de AWS IoT SiteWise activos

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Modelos y seleccione el modelo de activo al que desee añadir la definición de predicción.
3. Elija Predicciones.
4. Seleccione Añadir definición de predicción.
5. Defina los detalles sobre la definición de predicción.

    a. Introduzca un nombre único y una descripción para la definición de predicción. Elija el nombre con cuidado, ya que después de crear la definición de predicción, no podrá cambiarlo.

b. Cree o seleccione un rol de permisos de IAM que le permita AWS IoT SiteWise compartir los datos de sus activos con Amazon Lookout for Equipment. El rol debe tener las siguientes políticas de confianza y de IAM. Para obtener ayuda para crear el rol, consulte Crear un rol mediante políticas de confianza personalizadas (consola).

Política de 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/*"
        }
    ]
}
```

Política de confianza

```
{
    "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. Elija Siguiente.

6. Selecciona los atributos de datos (medidas, transformaciones y métricas) que quieras enviar a Lookout for Equipment.

   a. (Opcional) Seleccione las medidas.

   b. (Opcional) Seleccione las transformaciones.

   c. (Opcional) Seleccione las métricas.

   d. Elija Siguiente.

7. Revise sus selecciones. Para añadir la definición de predicción al modelo de activos, en la página de resumen, seleccione Añadir definición de predicción.

También puede editar o eliminar una definición de predicción existente que tenga predicciones activas adjuntas.

Entrenar una predicción (consola)

Después de añadir una definición de predicción a un modelo de activos, puede entrenar las predicciones que se incluyen en sus activos.

Para entrenar una predicción en AWS IoT SiteWise

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Activos y seleccione el activo que desee supervisar.
3. Elija Predicciones.
4. Selecciona las predicciones que quieres entrenar.
5. En Acciones, selecciona Empezar a entrenar y haz lo siguiente:

   a. En Detalles de la predicción, selecciona un rol de permisos de IAM que te permita AWS IoT SiteWise compartir los datos de tus activos con Lookout for Equipment. Si necesitas crear un nuevo rol, selecciona Crear un nuevo rol.

   b. En la configuración de los datos de entrenamiento, introduce un rango de tiempo de datos de entrenamiento para seleccionar qué datos usar para entrenar la predicción.

c. (Opcional) En el caso de las etiquetas de datos, proporciona un depósito y un prefijo de Amazon S3 que contengan los datos de etiquetado. Para obtener más información sobre el etiquetado de datos, consulta Cómo etiquetar tus datos en la Guía del usuario de Amazon Lookout for Equipment.

d. Elija Siguiente.

6. (Opcional) Si quieres que la predicción esté activa en cuanto termine el entrenamiento, en Configuración avanzada, selecciona Activar automáticamente la predicción después del entrenamiento y, a continuación, haz lo siguiente:

   a. En Datos de entrada, en Frecuencia de carga de datos, define la frecuencia con la que se cargan los datos y, en Tiempo de retardo de compensación, define la cantidad de búfer que se va a utilizar.

   b. Elija Siguiente.

7. Revisa los detalles de la predicción y selecciona Guardar e iniciar.

Iniciar o detener la inferencia en una predicción (consola)

> **Note**
>
> Los cargos de Lookout for Equipment se aplican a las inferencias programadas con los datos transferidos AWS IoT SiteWise entre Lookout for Equipment y Lookout for Equipment. Para obtener más información, consulta los precios de Amazon Lookout for Equipment.

Si has añadido una predicción pero no has decidido activarla después del entrenamiento, debes activarla para que pueda empezar a monitorizar tus activos.

Para iniciar la inferencia de una predicción

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Activos y seleccione el activo al que se añade la predicción.
3. Elija Predicciones.
4. Seleccione las predicciones que desee activar.
5. En Acciones, elija Iniciar inferencia y haga lo siguiente:

a. En Datos de entrada, en Frecuencia de carga de datos, defina la frecuencia con la que se cargan los datos y, en Tiempo de retardo de compensación, defina la cantidad de búfer que se va a utilizar.

b. Selecciona Guardar e iniciar.

Para detener la inferencia de una predicción

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Activos y seleccione el activo al que se añade la predicción.
3. Elija Predicciones.
4. Seleccione las predicciones que desee detener.
5. En Acciones, elija Detener la inferencia.

Añadir una definición de predicción (CLI)

Para definir una definición de predicción en un modelo de activos nuevo o existente, puede usar AWS Command Line Interface (AWS CLI). Tras definir la definición de predicción en el modelo de activos, entrena y programa la inferencia de una predicción sobre un activo para detectar anomalías con Lookout for Equipment. AWS IoT SiteWise

Requisitos previos

Para completar estos pasos, debe tener un modelo de activos y crear al menos un activo. Para obtener más información, consulte Crear un modelo de activos (AWS CLI) y Crear un activo ()AWS CLI.

Si es la primera vez que lo usa AWS IoT SiteWise, debe llamar a la operación de la `CreateBulkImportJob` API para importar los valores de las propiedades de los activos AWS IoT SiteWise, que se utilizarán para entrenar el modelo. Para obtener más información, consulte Crea un trabajo de importación por lotes (AWS CLI).

Para añadir una definición de predicción

1. Cree un archivo denominado `asset-model-payload.json`. Siga los pasos de estas otras secciones para añadir los detalles de su modelo de activo al archivo, pero no envíe la solicitud para crear o actualizar el modelo de activo.

- Para obtener más información sobre cómo crear un modelo de activos, consulte Crear un modelo de activos (AWS CLI)
- Para obtener más información sobre cómo actualizar un modelo de activos existente, consulte Actualización de un modelo de activo o componente (AWS CLI)

2. Añada un modelo compuesto de Lookout for Equipment `assetModelCompositeModels` () al modelo de activos añadiendo el siguiente código.

   - *`Property`*Sustitúyalo por el ID de las propiedades que desee incluir. Para obtener esos identificadores, llame `DescribeAssetModel`.
   - *`RoleARN`*Sustitúyalo por el ARN de un rol de IAM que permita a Lookout for Equipment acceder a tus datos. 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. Cree el modelo de activo o actualice el modelo de activo existente. Realice una de las acciones siguientes:

   - Para crear el modelo de activos, ejecute el siguiente comando:

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

   - Ejecute el siguiente comando para actualizar el modelo de activo existente. *asset-model-id*Sustitúyalo por el ID del modelo de activos que desee actualizar.

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

Después de ejecutar el comando, anote `assetModelId` en la respuesta.

Entrenamiento de una predicción e inferencia inicial (CLI)

Ahora que la definición de predicción está definida, puede entrenar los activos en función de ella e iniciar la inferencia. Si quiere entrenar su predicción pero no iniciar la inferencia, pase a. Entrenamiento de una predicción (CLI) Para entrenar la predicción e iniciar la inferencia sobre el activo, necesitará el `assetId` recurso objetivo.

Para entrenar e iniciar la inferencia de la predicción

1. Ejecute el siguiente comando para encontrar la parte `assetModelCompositeModelId` inferior`assetModelCompositeModelSummaries`. *asset-model-id*Sustitúyalo por el ID

del modelo de activos en el que lo creasteActualización de un modelo de activo o componente (AWS CLI).

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

2. Ejecute el siguiente comando para encontrar `actionDefinitionId` la `TrainingWithInference` acción. *asset-model-id*Sustitúyala por la ID utilizada en el paso anterior y *asset-model-composite-model-id*sustitúyala por la ID devuelta en el paso anterior.

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

3. Cree un archivo llamado `train-start-inference-prediction.json` y añada el siguiente código, sustituyendo el siguiente:

   - *asset-id*con el ID del activo de destino
   - *action-definition-id*con el ID de la TrainingWithInference acción
   - *StartTime*con el inicio de los datos de entrenamiento, proporcionados en segundos
   - *EndTime*con el final de los datos de entrenamiento, proporcionados en segundos de época

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

4. Ejecute el siguiente comando para iniciar el entrenamiento y la inferencia:

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

Entrenamiento de una predicción (CLI)

Ahora que la definición de predicción está definida, puede entrenar los activos en función de ella. Para entrenar la predicción sobre el activo, necesitará la `assetId` del recurso objetivo.

Para entrenar la predicción

1. Ejecuta el siguiente comando para encontrar la parte `assetModelCompositeModelId` inferior`assetModelCompositeModelSummaries`. *`asset-model-id`*Sustitúyalo por el ID del modelo de activos en el que lo creasteActualización de un modelo de activo o componente (AWS CLI).

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

2. Ejecute el siguiente comando para encontrar `actionDefinitionId` la `Training` acción. *`asset-model-id`*Sustitúyala por la ID utilizada en el paso anterior y *`asset-model-composite-model-id`*sustitúyala por la ID devuelta en el paso anterior.

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

3. Cree un archivo llamado `train-prediction.json` y añada el siguiente código, sustituyendo el siguiente:

   - *`asset-id`*con el ID del activo de destino
   - *`action-definition-id`*con el ID de la acción formativa
   - *`StartTime`*con el inicio de los datos de entrenamiento, proporcionados en segundos
   - *`EndTime`*con el final de los datos de entrenamiento, proporcionados en segundos de época
   - (Opcional) *`BucketName`* con el nombre del depósito de Amazon S3 que contiene los datos de la etiqueta
   - (Opcional) *`Prefix`* con el prefijo asociado al bucket de Amazon S3.

> **Note**
>
> Incluya el nombre y el prefijo del bucket o ninguno de ellos.

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

4. Ejecute el siguiente comando para iniciar el entrenamiento:

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

Antes de poder iniciar la inferencia, se debe completar el entrenamiento. Para comprobar el estado de la formación, realice una de las siguientes acciones:

- Desde la consola, navega hasta el activo en el que se encuentra la predicción.
- Desde el AWS CLI, llame `BatchGetAssetPropertyValue` utilizando el `propertyId` de la `trainingStatus` propiedad.

Iniciar o detener la inferencia de una predicción (CLI)

Una vez entrenada la predicción, puedes iniciar la inferencia para decirle a Lookout for Equipment que comience a monitorizar tus activos. Para iniciar o detener la inferencia, necesitarás el recurso `assetId` objetivo.

Para iniciar la inferencia

1. Ejecute el siguiente comando para encontrar la parte `assetModelCompositeModelId` inferior`assetModelCompositeModelSummaries`. *`asset-model-id`*Sustitúyalo por el ID del modelo de activos en el que lo creasteActualización de un modelo de activo o componente (AWS CLI).

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

2. Ejecute el siguiente comando para encontrar `actionDefinitionId` la `Inference` acción. *`asset-model-id`*Sustitúyala por la ID utilizada en el paso anterior y *`asset-model-composite-model-id`*sustitúyala por la ID devuelta en el paso anterior.

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

3. Cree un archivo llamado `start-inference.json` y añada el siguiente código, sustituyendo el siguiente:

   - *`asset-id`*con el ID del activo de destino
   - *`action-definition-id`*con el ID de la acción de inferencia inicial
   - *`Offset`*con la cantidad de búfer a utilizar
   - *`Frequency`*con qué frecuencia se cargan los datos

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

4. Ejecute el siguiente comando para iniciar la inferencia:

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

Para detener la inferencia

1. Ejecute el siguiente comando para encontrar la parte `assetModelCompositeModelId` inferior`assetModelCompositeModelSummaries`. *`asset-model-id`*Sustitúyalo por el ID del modelo de activos en el que lo creasteActualización de un modelo de activo o componente (AWS CLI).

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

2. Ejecute el siguiente comando para encontrar `actionDefinitionId` la `Inference` acción. *`asset-model-id`*Sustitúyala por la ID utilizada en el paso anterior y *`asset-model-composite-model-id`*sustitúyala por la ID devuelta en el paso anterior.

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

3. Cree un archivo llamado `stop-inference.json` y añada el siguiente código, sustituyendo el siguiente:

   - *`asset-id`*con el ID del activo de destino
   - *`action-definition-id`*con el ID de la acción de inferencia inicial

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

4. Ejecute el siguiente comando para detener la inferencia:

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

Administrar el almacenamiento de datos

Puede configurarlo AWS IoT SiteWise para guardar sus datos en los siguientes niveles de almacenamiento:

Nivel de acceso frecuente

El nivel de almacenamiento activo es un almacenamiento de series temporales AWS IoT SiteWise gestionado. El nivel activo es más eficaz para los datos a los que se accede con frecuencia, con baja write-to-read latencia. Los datos almacenados en la capa activa son utilizados por aplicaciones industriales que necesitan un acceso rápido a los valores más recientes de las mediciones de su equipo. Esto incluye aplicaciones que visualizan métricas en tiempo real con un panel interactivo o aplicaciones que monitorean las operaciones y activan alarmas para identificar problemas de rendimiento.

De forma predeterminada, los datos ingresados AWS IoT SiteWise se almacenan en la capa activa. Puede definir un período de retención para el nivel activo, tras el cual AWS IoT SiteWise se transfieren los datos del nivel activo a un almacenamiento de nivel caliente o frío, según su configuración. Para obtener el mejor rendimiento y rentabilidad, configure el período de retención del nivel activo para que sea más largo que el tiempo que se tarda en recuperar los datos con frecuencia. Esto se usa para métricas, alarmas y escenarios de monitoreo en tiempo real. Si no se establece un período de retención, sus datos se almacenan indefinidamente en la capa activa.

Nivel cálido

El nivel de almacenamiento en caliente es un nivel AWS IoT SiteWise gestionado que resulta eficaz para el almacenamiento rentable de datos históricos. Se utiliza mejor para recuperar grandes volúmenes de datos con características de write-to-read latencia media. Utilice el nivel cálido para almacenar los datos históricos necesarios para grandes cargas de trabajo. Por ejemplo, se utiliza para la recuperación de datos para el análisis, las aplicaciones de inteligencia empresarial (BI), las herramientas de elaboración de informes y el entrenamiento de modelos de aprendizaje automático (ML). Si habilita el nivel de almacenamiento en frío, puede definir un período de retención del nivel cálido. Una vez finalizado el período de retención, AWS IoT SiteWise elimina los datos del nivel cálido.

Nivel inactivo

La capa de almacenamiento en frío utiliza un depósito de Amazon S3 para almacenar datos que se utilizan con poca frecuencia. Con la capa fría habilitada, AWS IoT SiteWise replica las series

temporales, incluidas las mediciones, las métricas, las transformaciones y los agregados, y las definiciones de los modelos de activos cada 6 horas. La capa fría se utiliza para almacenar datos que toleran una latencia de lectura alta para los informes históricos y las copias de seguridad.

Temas

Configurar los ajustes de almacenamiento

Puede configurar los ajustes de almacenamiento para optar por el almacenamiento de nivel cálido gestionado por el servicio y también para replicar los datos en el nivel frío. Para obtener más información sobre el período de retención de los niveles cálido y caliente, consulteImpacto en la retención de datos. Al configurar los ajustes de almacenamiento, haga lo siguiente:

- Retención en la capa activa: establece un período de retención durante el cual tus datos se almacenan en la capa activa antes de que se eliminen y se transfieren al almacenamiento en capa caliente o almacenamiento en capa fría gestionado por el servicio en función de tu configuración de almacenamiento. AWS IoT SiteWise eliminará todos los datos de la capa activa que existieran antes de que finalice el período de retención. Si no estableces un período de retención, tus datos se almacenan indefinidamente en la capa activa.
- Retención en la capa cálida: establece un período de retención para el tiempo que tus datos permanecerán almacenados en la capa cálida antes de que se eliminen del AWS IoT SiteWise almacenamiento y se trasladen al almacenamiento en la capa fría gestionada por el cliente. AWS IoT SiteWise elimina todos los datos de la capa cálida que existían antes de que finalizara el período de retención. Si no se establece un período de retención, sus datos se almacenan indefinidamente en el nivel cálido.

> **Note**
>
> Para mejorar el rendimiento de las consultas, establece un período de retención en el nivel activo con el almacenamiento en el nivel cálido.

Impacto de la retención de datos en el almacenamiento de nivel caliente y caliente

- Al reducir el período de retención del almacenamiento de capa activa, los datos se mueven permanentemente de la capa activa a la capa caliente o fría. Al reducir el período de retención de la capa cálida, los datos se mueven a la capa fría y se eliminan permanentemente de la capa cálida.
- Al aumentar el período de retención del almacenamiento de nivel caliente o caliente, el cambio afecta a los datos que se envíen a AWS IoT SiteWise partir de ese momento. AWS IoT SiteWise no recupera los datos del almacenamiento caliente o frío para poblarlos en el nivel activo. Por ejemplo, si el período de retención del almacenamiento de capa activa se establece inicialmente en 30 días y luego se aumenta a 60 días, el almacenamiento de capa activa tarda 30 días en contener datos de 60 días.

Temas

Configure los ajustes de almacenamiento para el nivel cálido (consola)

El siguiente procedimiento muestra cómo configurar los ajustes de almacenamiento para replicar los datos en el nivel cálido de la AWS IoT SiteWise consola.

Para configurar los parámetros de disponibilidad en la consola

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, en Configuración, seleccione Listas.
3. En la esquina superior derecha, elija Edit (Editar).
4. En la página Editar acción, haga lo siguiente:
5. Para configurar el nivel activo, haga lo siguiente:

- Si quieres establecer un período de retención durante el cual tus datos se almacenarán en la capa activa antes de que se eliminen y se trasladen a la capa caliente gestionada por el servicio, selecciona Habilitar el período de retención.
- Para configurar un período de retención, introduzca un número entero y elija una unidad. El periodo de retención debe ser mayor o igual a 30 días.

AWS IoT SiteWise elimina todos los datos de la capa activa que sean anteriores al período de retención. Si no establece un período de retención, sus datos se almacenarán indefinidamente.

6. (Recomendado) Para la configuración del nivel cálido, haga lo siguiente:

- Para optar por el almacenamiento en el nivel cálido, selecciona Confirmo la suscripción al almacenamiento en el nivel cálido para optar por el almacenamiento en el nivel cálido.
- (Opcional) Para configurar un período de retención, introduce un número entero y elige una unidad. El período de retención debe ser superior o igual a 365 días.

AWS IoT SiteWise elimina los datos del nivel cálido que existían antes del período de retención. Si no establece un período de retención, sus datos se almacenarán indefinidamente.

> **Note**
>
> - Si opta por el nivel cálido, la configuración se muestra solo una vez.
> - Para configurar la retención en el nivel caliente, debe tener un almacenamiento en el nivel caliente o frío. Para lograr una mayor rentabilidad y recuperar datos históricos, se AWS IoT SiteWise recomienda almacenar los datos a largo plazo en el nivel cálido.
> - Para configurar la retención en el nivel cálido, debe tener un almacenamiento en el nivel frío.

7. Selecciona Guardar para guardar la configuración de almacenamiento.

En la sección AWS IoT SiteWise de almacenamiento, el almacenamiento de nivel cálido se encuentra en uno de estos estados:

- Habilitado: si sus datos existían antes del período de retención del nivel AWS IoT SiteWise activo, los mueve al nivel cálido».

- Desactivado: el almacenamiento en el nivel cálido está desactivado.

Configure los ajustes de almacenamiento para el nivel cálido (AWS CLI)

Puede configurar los ajustes de almacenamiento para mover los datos al nivel cálido mediante AWS CLI los siguientes comandos.

Para evitar anular la configuración existente, recupere la información de configuración de almacenamiento actual ejecutando el siguiente comando:

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

Example respuesta sin la configuración de capa fría existente

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

Example respuesta con la configuración de niveles fríos existente

```
{
      "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"
}
```

Configure los ajustes de almacenamiento para el nivel cálido con AWS CLI

Ejecute el siguiente comando para configurar los ajustes de almacenamiento. `file-name`Sustitúyalo por el nombre del archivo que contiene la configuración AWS IoT SiteWise de almacenamiento.

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

Example AWS IoT SiteWise configuración con niveles caliente y cálido

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

}
```

`hot-tier-retention-in-days`debe ser un número entero mayor o igual a 30 días.

Example Respuesta

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

Si tiene activado el almacenamiento en niveles de refrigeración, consulte[Configure los ajustes de almacenamiento con AWS CLI un nivel de refrigeración existente](#).

Configure los ajustes de almacenamiento con AWS CLI un nivel de refrigeración existente

Configure los ajustes de almacenamiento utilizando AWS CLI el almacenamiento en capa fría existente

- Ejecute el siguiente comando para configurar los ajustes de almacenamiento. Sustituya *file-name* por el nombre del archivo que contiene la configuración de almacenamiento de AWS IoT SiteWise .

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

Example AWS IoT SiteWise configuración de almacenamiento

- Sustituya *bucketname* por el nombre del bucket de Amazon S3.
- Sustituya *prefix* por el prefijo de Amazon S3.
- *aws-account-id*Sustitúyala por tu ID de AWS cuenta.
- Sustituya el *nombre del rol* por el nombre del rol de acceso de Amazon S3 que permite AWS IoT SiteWise enviar datos a Amazon S3.
- Sustituya *hot-tier-retention-in-days* por un número entero mayor o igual a 30 días.
- Sustituya *warm-tier-retention-in-days* por un número entero mayor o igual a 365 días.

> **Note**
>
> AWS IoT SiteWise eliminará todos los datos del nivel cálido que sean anteriores al período de retención del nivel frío. Si no establece un período de retención, sus datos se almacenarán indefinidamente.

```
{
      "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 Respuesta

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

Configure los ajustes de almacenamiento para el nivel frío (consola)

El siguiente procedimiento muestra cómo configurar los ajustes de almacenamiento para replicar los datos en la capa fría de la AWS IoT SiteWise consola.

Para configurar los parámetros de disponibilidad en la consola

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, en Configuración, seleccione Listas.
3. En la esquina superior derecha, elija Edit (Editar).
4. En la página Editar acción, haga lo siguiente:

    a. En la Configuración de almacenamiento, seleccione Habilitar el almacenamiento en el nivel inactivo. El almacenamiento en el nivel inactivo está desactivado de forma predeterminada.

    b. En Ubicación del bucket de S3, introduzca el nombre de un bucket de Amazon S3 existente y un prefijo.

> **Note**
>
> - Amazon S3 utiliza el prefijo como nombre de carpeta en el bucket de Amazon S3. El prefijo debe tener entre 1 y 255 caracteres y terminar con una barra diagonal (/). Sus AWS IoT SiteWise datos se guardan en esta carpeta.
> - Si no dispone de un bucket de Amazon S3, seleccione Ver y, a continuación, cree uno en la consola de Amazon S3. Para obtener más información, consulte Creación del primer bucket de S3 en la Guía del usuario de Amazon S3.

c. Para rol de acceso a S3, realice una de las operaciones siguientes:

- Si selecciona Crear un rol a partir de una plantilla AWS gestionada, crea AWS automáticamente un rol de IAM que permite AWS IoT SiteWise enviar datos a Amazon S3.
- Elija Usar un rol existente y, a continuación, elija el rol que creó de la lista.

> **Note**
>
> - Debe usar el mismo nombre de bucket de Amazon S3 para la Ubicación del bucket de S3 que utilizó en el paso anterior y en su política de IAM.
> - Asegúrese de que el rol tenga los permisos que se muestran en el siguiente ejemplo.
>
>   Example política de permisos:
>
> ```
> {
>       "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/*"
            ]
        }
    ]
}
```

Reemplace *bucket-name* con el nombre de su bucket de Amazon S3.

d. Para configurar el nivel activo, consulte el paso 5 de[Configure los ajustes de almacenamiento para el nivel cálido (consola)](#).

e. (Opcional) Para la integración de AWS IoT Analytics , haga lo siguiente.

   i. Si desea utilizarlo AWS IoT Analytics para consultar sus datos, elija Almacén de AWS IoT Analytics datos activado.

   ii. AWS IoT SiteWise genera un nombre para el banco de datos o puede introducir un nombre diferente.

   AWS IoT SiteWise crea automáticamente un almacén de datos AWS IoT Analytics para guardar sus datos. Para consultar los datos, puede utilizarlos AWS IoT Analytics para crear conjuntos de datos. Para obtener más información, consulte [Trabajar con AWS IoT SiteWise datos](#) en la Guía del AWS IoT Analytics usuario.

f. Seleccione Guardar.

En la sección Almacenamiento de AWS IoT SiteWise , el Almacenamiento en el nivel inactivo puede tener uno de los siguientes valores:

- Habilitado: AWS IoT SiteWise replica los datos en el bucket de Amazon S3 especificado.
- Habilitación: AWS IoT SiteWise está procesando su solicitud para habilitar el almacenamiento en capas frías. Este proceso puede tardar varios minutos en completarse.
- Enable_Failed: no se ha AWS IoT SiteWise podido procesar tu solicitud para habilitar el almacenamiento en capa fría. Si has habilitado AWS IoT SiteWise el envío de registros a Amazon CloudWatch Logs, puedes usar estos registros para solucionar problemas. Para obtener más información, consulte [Supervisión con Amazon CloudWatch Logs](#).
- Deshabilitado: el almacenamiento en el nivel inactivo está desactivado.

Configure los ajustes de almacenamiento para la capa inactiva ()AWS CLI

El siguiente procedimiento muestra cómo configurar los ajustes de almacenamiento para replicar datos en el nivel inactivo mediante AWS CLI.

Para configurar los ajustes de almacenamiento mediante AWS CLI

1. Para exportar datos a un bucket de Amazon S3 en su cuenta, ejecute el siguiente comando para configurar los ajustes de almacenamiento. Sustituya *el nombre de archivo* por el nombre del archivo que contiene la configuración de AWS IoT SiteWise almacenamiento.

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

   Example AWS IoT SiteWise configuración de almacenamiento

   - Sustituya *bucketname* por el nombre del bucket de Amazon S3.
   - Sustituya *prefix* por el prefijo de Amazon S3.
   - *aws-account-id*Sustitúyala por tu ID de AWS cuenta.
   - Sustituya el *nombre del rol* por el nombre del rol de acceso de Amazon S3 que permite AWS IoT SiteWise enviar datos a Amazon S3.
   - *retention-in-days*Sustitúyalo por un número entero que sea mayor o igual a 30 días.

   ```
   {
         "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

- Debe usar el mismo nombre de bucket de Amazon S3 en la configuración de AWS IoT SiteWise almacenamiento y en la política de IAM.
- Asegúrese de que el rol tenga los permisos que se muestran en el siguiente ejemplo.

  Example política de permisos:

```
{
      "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/*"
              ]
          }
      ]
  }
```

  Reemplace *bucket-name* con el nombre de su bucket de Amazon S3.

Example Respuesta

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

```
        "state": "UPDATE_IN_PROGRESS"
    }
}
```

> **Note**
>
> La actualización de la configuración de AWS IoT SiteWise almacenamiento puede tardar unos minutos.

2. Para recuperar la información de configuración del almacenamiento, ejecute el siguiente comando.

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

Example respuesta

```
{
      "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. Para detener la exportación de datos al bucket de Amazon S3, ejecute el siguiente comando para configurar los ajustes de almacenamiento.

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

> **Note**
>
> De forma predeterminada, los datos solo se almacenan en la capa activa de AWS IoT SiteWise.

Example Respuesta

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

4. Para recuperar la información de configuración del almacenamiento, ejecute el siguiente comando.

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

Example respuesta

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

(Opcional) Cree un almacén AWS IoT Analytics de datos (AWS CLI)

Un AWS IoT Analytics banco de datos es un repositorio escalable y consultable que recibe y almacena datos. Puede usar la AWS IoT SiteWise consola o AWS IoT Analytics las API para crear un banco de AWS IoT Analytics datos para guardar AWS IoT SiteWise los datos. Para consultar los datos, cree conjuntos de datos mediante AWS IoT Analytics. Para obtener más información, consulte Trabajo con datos de AWS IoT SiteWise en la Guía del usuario de AWS IoT Analytics .

Los siguientes pasos se utilizan AWS CLI para crear un almacén de datos en AWS IoT Analytics.

Ejecute el siguiente comando para crear un almacén de datos. Sustituya *file-name* por el nombre del archivo que contiene la configuración del almacén de datos.

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

> **Note**
>
> - Debe especificar el nombre de un bucket de Amazon S3 existente. Si no dispone de un bucket de Amazon S3, cree uno primero. Para obtener más información, consulte Creación del primer bucket de S3 en la Guía del usuario de Amazon S3.
> - Debe usar el mismo nombre de bucket de Amazon S3 en la configuración de AWS IoT SiteWise almacenamiento, la política de IAM y la configuración del almacén de AWS IoT Analytics datos.

Example AWS IoT Analytics configuración del almacén de datos

Sustituya *data-store-name*y *s3-bucket-name por el nombre del* almacén de AWS IoT Analytics datos y el nombre del bucket de Amazon S3.

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

Example Respuesta

```
{
      "datastoreName": "datastore_IoTSiteWise_demo",
```

```
      "datastoreArn": "arn:aws:iotanalytics:us-west-2:123456789012:datastore/
datastore_IoTSiteWise_demo",
      "retentionPeriod": {
          "numberOfDays": 90,
          "unlimited": false
      }
  }
```

Solucionar problemas de configuración de almacenamiento

Utilice la siguiente información como ayuda para solucionar problemas con la configuración de almacenamiento.

Problemas

- Error: el bucket no existe
- Error: acceso denegado a la ruta de Amazon S3
- Error: no se puede asumir el ARN del rol
- Error: no se pudo acceder al bucket de Amazon S3 entre regiones

Error: el bucket no existe

Solución: no AWS IoT SiteWise ha podido encontrar su bucket de Amazon S3. Asegúrese de introducir el nombre de un bucket de Amazon S3 existente en la región actual.

Error: acceso denegado a la ruta de Amazon S3

Solución: no AWS IoT SiteWise ha podido acceder a su bucket de Amazon S3. Haga lo siguiente:

- Asegúrese de utilizar el mismo bucket de Amazon S3 que especificó en la política de IAM.
- Asegúrese de que el rol tenga los permisos que se muestran en el siguiente ejemplo.

  Example política de permisos

```
{
      "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/*"
            ]
        }
    ]
}
```

Reemplace *bucket-name* con el nombre de su bucket de Amazon S3.

Error: no se puede asumir el ARN del rol

Solución: no AWS IoT SiteWise pude asumir la función de IAM en su nombre. Asegúrese de que su rol confíe en el siguiente servicio: `iotsitewise.amazonaws.com`. Para obtener más información, consulte No puedo asumir un rol en la Guía del usuario de IAM.

Error: no se pudo acceder al bucket de Amazon S3 entre regiones

Solución: el bucket de Amazon S3 que especificó se encuentra en una AWS región diferente. Asegúrese de que su depósito de Amazon S3 y AWS IoT SiteWise sus activos estén en la misma región.

Rutas de archivos y esquemas de datos guardados en el nivel inactivo

AWS IoT SiteWise almacena sus datos en la capa fría replicando series temporales, incluidas las mediciones, las métricas, las transformaciones y los agregados, así como las definiciones de activos y modelos de activos. A continuación se describen las rutas de los archivos y los esquemas de datos que se envían al nivel inactivo.

Temas

- Datos del equipo (mediciones)

- Métricas, transformaciones y agregados
- Metadatos de los activos
- Metadatos de jerarquía de los activos
- Almacenamiento de archivos índice de datos

Datos del equipo (mediciones)

AWS IoT SiteWise exporta los datos del equipo (mediciones) a la capa fría una vez cada seis horas. Los datos sin procesar se guardan en el nivel inactivo en formato Apache AVRO (`.avro`).

Ruta de archivo

AWS IoT SiteWise almacena los datos del equipo (mediciones) en la capa fría mediante la siguiente plantilla.

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

Cada ruta de archivo a datos sin procesar en Amazon S3 contiene los siguientes componentes.

Componente de ruta	Descripción
`keyPrefix`	El prefijo de Amazon S3 que especificó en la configuración AWS IoT SiteWise de almacenamiento. Amazon S3 utiliza el prefijo como nombre de carpeta en el bucket.
`raw`	La carpeta que almacena los datos de serie temporal del equipo (mediciones). La carpeta `raw` se guarda en la carpeta de prefijos.
`seriesBucket`	Un número hexadecimal entre 00 y ff. Este número se deriva de `timeSeriesId` . Esta partición se utiliza para aumentar el rendimien to cuando se AWS IoT SiteWise escribe en la capa fría. Cuando se utiliza Amazon Athena para ejecutar consultas, la partición puede

Componente de ruta	Descripción
	servir para realizar particiones refinadas a fin de mejorar la precisión de las consultas. `seriesBucket` y `timeSeriesBucket` son el mismo número en los metadatos del activo.
`startYear`	El año de la hora de inicio exclusiva asociada a los datos de serie temporal.
`startMonth`	El mes de la hora de inicio exclusiva asociada a los datos de serie temporal.
`startDay`	El día del mes de la hora de inicio exclusiva asociada a los datos de serie temporal.
`fileName`	El nombre del archivo utiliza el carácter de subrayado (_) como delimitador para separar lo siguiente: • El prefijo `raw`. • El valor `timeSeriesId` . • La marca temporal de fecha de inicio exclusiva asociada a los datos de serie temporal. • La calidad de datos. Valores aceptados: `GOOD`, `BAD` y `UNCERTAIN` . Para obtener más información, consulte AssetPropertyValuela referencia de la AWS IoT SiteWise API. El archivo se guarda en el formato `.avro` mediante la compresión Snappy.

Example ruta del archivo a los datos sin procesar en el nivel inactivo

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

Campos

El esquema de datos sin procesar que se exporta al nivel inactivo contiene los siguientes campos.

Nombre del campo	Tipos admitidos	Tipo predeterminado	Descripción
`seriesId`	`string`	N/A	El identificador que identifica los datos de serie temporal del equipo (mediciones). Puede usar este campo para unir datos sin procesar y metadatos de activos en las consultas.
`timeInSeconds`	`long`	N/A	La marca temporal, en segundos, en formato de tiempo Unix. Los datos fraccionarios de nanosegundos los proporciona `offsetInNanos` .
`offsetInNanos`	`long`	N/A	El desfase de nanosegundos procedente de `timeInSeconds` .
`quality`	`string`	N/A	La calidad del valor de la serie temporal.

Nombre del campo	Tipos admitidos	Tipo predeterminado	Descripción
`doubleValue`	`double` o `null`	`null`	Datos de serie temporal de tipo doble (número de punto flotante).
`stringValue`	`string` o `null`	`null`	Datos de serie temporal de tipo cadena (secuencia de caracteres).
`integerValue`	`int` o `null`	`null`	Datos de serie temporal de tipo entero (número entero).
`booleanValue`	`boolean` o `null`	`null`	Datos de serie temporal de tipo booleano (verdadero o falso).
`jsonValue`	`string` o `null`	`null`	Datos de serie temporal de tipo JSON (tipos de datos complejos almacenados como una cadena).
`recordVersion`	`long` o `null`	`null`	El número de versión para el registro. Puede usar el número de versión para seleccionar el registro más reciente. Los registros más recientes tienen números de versión más grandes.

Example datos sin procesar en el nivel inactivo


```
{"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
```


Métricas, transformaciones y agregados

AWS IoT SiteWise exporta métricas, transforma y agrega a la capa fría una vez cada seis horas. Las métricas, las transformaciones y los agregados se guardan en el nivel inactivo en el formato Apache AVRO (`.avro`).

Ruta de archivo

AWS IoT SiteWise almacena las métricas, las transformaciones y los agregados en la capa fría mediante la siguiente plantilla.

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

Cada ruta de archivo a las métricas, las transformaciones y los agregados en Amazon S3 contiene los siguientes componentes.

Componente de ruta	Descripción
`keyPrefix`	El prefijo de Amazon S3 que especificó en la configuración AWS IoT SiteWise de

Componente de ruta	Descripción
	almacenamiento. Amazon S3 utiliza el prefijo como nombre de carpeta en el bucket.
`agg`	La carpeta que almacena los datos de serie temporal de las métricas. La carpeta `agg` se guarda en la carpeta de prefijos.
`seriesBucket`	Un número hexadecimal entre 00 y ff. Este número se deriva de `timeSeriesId` . Esta partición se utiliza para aumentar el rendimien to cuando se AWS IoT SiteWise escribe en la capa fría. Cuando se utiliza Amazon Athena para ejecutar consultas, la partición puede servir para realizar particiones refinadas a fin de mejorar la precisión de las consultas. `seriesBucket` y `timeSeriesBucket` son el mismo número en los metadatos del activo.
`startYear`	El año de la hora de inicio exclusiva asociada a los datos de serie temporal.
`startMonth`	El mes de la hora de inicio exclusiva asociada a los datos de serie temporal.
`startDay`	El día del mes de la hora de inicio exclusiva asociada a los datos de serie temporal.

Componente de ruta	Descripción
`fileName`	El nombre del archivo utiliza el carácter de subrayado (_) como delimitador para separar lo siguiente: • El prefijo `raw`. • El valor `timeSeriesId` . • La marca temporal de fecha de inicio exclusiva asociada a los datos de serie temporal. • La calidad de datos. Valores aceptados: `GOOD`, `BAD` y `UNCERTAIN` . Para obtener más información, consulte AssetPropertyValuela referencia de la AWS IoT SiteWise API. El archivo se guarda en el formato `.avro` mediante la compresión Snappy.

Example ruta del archivo a las métricas en el nivel inactivo

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

Campos

El esquema de las métricas, las transformaciones y los agregados que se exportan al nivel inactivo contiene los siguientes campos.

Nombre del campo	Tipos admitidos	Tipo predeterminado	Descripción
`seriesId`	`string`	N/A	El ID que identifica los datos de serie temporal procedent

Nombre del campo	Tipos admitidos	Tipo predeterminado	Descripción
			es del equipo, de las métricas o de las transformaciones. Puede usar este campo para unir datos sin procesar y metadatos de activos en las consultas.
`timeInSeconds`	`long`	N/A	La marca temporal, en segundos, en formato de tiempo Unix. Los datos fraccionarios de nanosegundos los proporciona `offsetInNanos` .
`offsetInNanos`	`long`	N/A	El desfase de nanosegundos procedente de `timeInSeconds` .
`quality`	`string`	N/A	La calidad con la que se filtran los datos de los activos.
`resolution`	`string`	N/A	El intervalo de tiempo durante el que se van a agregar los datos.
`count`	`double` o `null`	`null`	El número total de puntos de datos para las variables dadas durante el intervalo de tiempo actual.

Nombre del campo	Tipos admitidos	Tipo predeterminado	Descripción
`average`	`double` o `null`	`null`	La media de los valores de las variables dadas durante el intervalo de tiempo actual.
`min`	`double` o `null`	`null`	El mínimo de los valores de las variables dadas durante el intervalo de tiempo actual.
`max`	`boolean` o `null`	`null`	El máximo de los valores de las variables dadas durante el intervalo de tiempo actual.
`sum`	`string` o `null`	`null`	La suma de los valores de las variables dadas durante el intervalo de tiempo actual.
`recordVersion`	`long` o `null`	`null`	El número de versión para el registro. Puede usar el número de versión para seleccionar el registro más reciente. Los registros más recientes tienen números de versión más grandes.

Example Datos métricos en el nivel inactivo


```
{"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}
```


Metadatos de los activos

Cuando habilitas AWS IoT SiteWise la exportación de datos a la capa fría por primera vez, los metadatos de los activos se exportan a la capa fría. Tras la configuración inicial, AWS IoT SiteWise exporta los metadatos de los activos al nivel solo cuando se cambian las definiciones del modelo de activos o las definiciones de activos. Los metadatos de los activos se guardan en la capa fría en el formato JSON (`.ndjson`) delimitado por líneas nuevas.

Ruta de archivo

AWS IoT SiteWise almacena los metadatos de los activos en la capa fría mediante la siguiente plantilla.

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

Cada ruta de archivo a los metadatos de los activos en el nivel inactivo contiene los siguientes componentes.

Componente de ruta	Descripción
`keyPrefix`	El prefijo de Amazon S3 que especificó en la configuración de almacenamiento AWS IoT SiteWise s. Amazon S3 utiliza el prefijo como nombre de carpeta en el bucket.
`asset_metadata`	La carpeta que almacena los metadatos de los activos. La carpeta `asset_metadata` se guarda en la carpeta de prefijos.
`fileName`	El nombre del archivo utiliza el carácter de subrayado (_) como delimitador para separar lo siguiente: • El prefijo `asset`. • El valor `assetId`. El archivo se guarda en el formato `.ndjson`.

Example ruta del archivo a los metadatos de los activos en el nivel inferior

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

Campos

El esquema de metadatos de activos que se exporta al nivel inactivo contiene los siguientes campos.

Nombre del campo	Descripción
`assetId`	El ID del activo.
`assetName`	Nombre del activo.
`assetExternalId`	El ID externo del activo.
`assetModelId`	Id. del modelo de activo usado para crear el activo.

Nombre del campo	Descripción
`assetModelName`	El nombre del modelo del activo.
`assetModelExternalId`	El identificador externo del modelo de activo.
`assetPropertyId`	El ID de la propiedad del activo.
`assetPropertyName`	El nombre de la propiedad del activo.
`assetPropertyExternalId`	El identificador externo de la propiedad del activo.
`assetPropertyDataType`	El tipo de datos de la propiedad del activo.
`assetPropertyUnit`	La unidad que usa la propiedad del activo (por ejemplo, `Newtons` y `RPM`).
`assetPropertyAlias`	El alias que identifica la propiedad del activo, como una ruta de flujo de datos del servidor OPC-UA (por ejemplo, `/company/windfarm/3/turbine/7/temperature`).
`timeSeriesId`	El ID que identifica los datos de serie temporal procedentes del equipo, de las métricas o de las transformaciones. Puede usar este campo para unir datos sin procesar y metadatos de activos en las consultas.

Nombre del campo	Descripción
`timeSeriesBucket`	Un número hexadecimal entre 00 y ff. Este número se deriva de `timeSeriesId` . Esta partición se utiliza para aumentar el rendimien to cuando se AWS IoT SiteWise escribe en la capa fría. Cuando se utiliza Amazon Athena para ejecutar consultas, la partición puede servir para realizar particiones refinadas a fin de mejorar la precisión de las consultas. `timeSeriesBucket` y `seriesBucket` son el mismo número en la ruta del archivo a los datos sin procesar.
`assetCompositeModelId`	El ID del modelo compuesto.
`assetCompositeModelExternalId`	El identificador externo del modelo compuesto.
`assetCompositeModelDescription`	La descripción del modelo compuesto.
`assetCompositeModelName`	El nombre del modelo compuesto.
`assetCompositeModelType`	El tipo del modelo compuesto. Para los modelos compuestos de alarma, este tipo es `AWS/ALARM` .
`assetCreationDate`	La fecha en que se creó el activo, en formato de tiempo UNIX.
`assetLastUpdateDate`	La fecha en que el activo se actualizó por última vez, en fecha de inicio Unix.
`assetStatusErrorCode`	Código de error.
`assetStatusErrorMessage`	Mensaje de error.
`assetStatusState`	El estado actual del activo.

Example metadatos de activos en el nivel inactivo


```
  {"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
```


Metadatos de jerarquía de los activos

Cuando habilita AWS IoT SiteWise guardar datos en la capa fría por primera vez, los metadatos de la jerarquía de activos se exportan a la capa fría. Tras la configuración inicial, AWS IoT SiteWise exporta los metadatos de la jerarquía de activos a la capa fría solo cuando se realizan cambios en

el modelo de activos o en las definiciones de activos. Los metadatos de la jerarquía de activos se guardan en la capa fría en el formato JSON (`.ndjson`) delimitado por líneas nuevas.

Al llamar a la API, se recupera un identificador externo de la jerarquía, el activo de destino o el DescribeAssetactivo de origen.

Ruta de archivo

AWS IoT SiteWise almacena los metadatos de la jerarquía de activos en la capa fría mediante la siguiente plantilla.

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

Cada ruta de archivo a los metadatos de jerarquía de los activos en el nivel inactivo contiene los siguientes componentes.

Componente de ruta	Descripción
`keyPrefix`	El prefijo de Amazon S3 que especificó en la configuración AWS IoT SiteWise de almacenamiento. Amazon S3 utiliza el prefijo como nombre de carpeta en el bucket.
`asset_hierarchy_metadata`	La carpeta que almacena los metadatos de jerarquía de los activos. La carpeta `asset_hierarchy_metadata` se guarda en la carpeta de prefijos.
`fileName`	El nombre del archivo utiliza el carácter de subrayado (_) como delimitador para separar lo siguiente: • El valor `parentAssetId` . • El valor `hierarchyId` . El archivo se guarda en el formato `.ndjson`.

Example ruta del archivo a los metadatos de la jerarquía de activos en el nivel inactivo

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

Campos

El esquema de los metadatos de la jerarquía de activos que se exporta al nivel inactivo contiene los siguientes campos.

Nombre del campo	Descripción
`sourceAssetId`	El ID del activo de origen en esta relación de activos.
`targetAssetId`	El ID del activo de destino en esta relación de activos.
`hierarchyId`	El ID de la jerarquía.
`associationType`	El tipo de asociación de esta relación de activos. El valor debe ser `CHILD`. El activo de destino es una entidad secundaria del activo de origen.

Example los metadatos de jerarquía de los activos en el nivel inactivo

```
{"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"}
```

Para ver los datos en el nivel inactivo

1. Vaya a la consola de Amazon S3.

2. En el panel de navegación, elija Buckets y, a continuación, elija el bucket de Amazon S3.
3. Navegue hasta la carpeta que contiene los datos sin procesar, los metadatos de los activos o los metadatos de jerarquía de los activos.
4. Seleccione los archivos y, a continuación, en Acciones, elija Descargar.

Almacenamiento de archivos índice de datos

AWS IoT SiteWise utiliza estos archivos para optimizar el rendimiento de las consultas de datos. Aparecen en u bucket de Amazon S3, pero no es necesario que los utilice.

Ruta de archivo

AWS IoT SiteWise almacena los archivos de índice de datos en la capa fría mediante la siguiente plantilla.

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

Example ruta del archivo al archivo índice de almacenamiento de datos

```
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
```

Seguridad en AWS IoT SiteWise

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de cumplimiento aplicables AWS IoT SiteWise, consulte AWS los servicios clasificados por programa de cumplimiento y AWS los servicios incluidos .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza AWS IoT SiteWise. Los siguientes temas muestran cómo configurarlo AWS IoT SiteWise para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus AWS IoT SiteWise recursos.

Temas

Protección de datos en AWS IoT SiteWise

El modelo de responsabilidad AWS compartida modelo se aplica a la protección de datos en AWS IoT SiteWise. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja AWS IoT SiteWise o Servicios de AWS utiliza la consola, la API o los SDK. AWS CLI AWS Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o

diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Temas

Privacidad del tráfico entre redes

Las conexiones entre aplicaciones locales AWS IoT SiteWise y entre ellas, como las puertas de enlace SiteWise Edge, se protegen mediante conexiones de seguridad de capa de transporte (TLS). Para obtener más información, consulte Cifrado en tránsito.

AWS IoT SiteWise no admite conexiones entre zonas de disponibilidad dentro de una AWS región ni conexiones entre cuentas. AWS

Solo puede configurar el Centro de identidades de IAM en una región a la vez. SiteWise El monitor se conecta a la región que configuró para el IAM Identity Center. Esto significa que utiliza una región para el acceso al Centro de identidades de IAM, pero puede crear portales en cualquier región.

Cifrado de datos

El cifrado de datos se refiere a la protección de los datos mientras están en tránsito (cuando viajan hacia y desde AWS IoT SiteWise las puertas de enlace SiteWise Edge y los servidores y entre ellos) y en reposo (mientras están almacenados en dispositivos o AWS servicios locales). Puede proteger los datos en tránsito mediante seguridad de la capa de transporte (TLS) o en reposo mediante el cifrado del cliente.

> **Note**
>
> AWS IoT SiteWise El procesamiento perimetral expone las API que están alojadas en las puertas de enlace SiteWise Edge y a las que se puede acceder a ellas a través de la red local. Estas API se exponen a través de una conexión TLS respaldada por un certificado de servidor propiedad del conector Edge. AWS IoT SiteWise Para la autenticación de los clientes, estas API utilizan una contraseña de control de acceso. Tanto la clave privada del certificado del servidor como la contraseña de control de acceso se almacenan en el disco. AWS IoT SiteWise El procesamiento perimetral se basa en el cifrado del sistema de archivos para garantizar la seguridad de estas credenciales inactivas.

Para obtener más información sobre el cifrado del lado del servidor y el cifrado del cliente, revise los temas que se enumeran a continuación.

Temas

Cifrado en reposo

AWS IoT SiteWise almacena sus datos en la AWS nube y en las pasarelas AWS IoT SiteWise Edge.

Datos en reposo en la nube AWS

AWS IoT SiteWise almacena los datos en otros AWS servicios que cifran los datos en reposo de forma predeterminada. Encryption at rest se integra con AWS Key Management Service (AWS KMS) para administrar la clave de cifrado que se utiliza para cifrar los valores de las propiedades de los activos y los valores agregados. AWS IoT SiteWise Puede optar por utilizar una clave administrada por el cliente para cifrar los valores de propiedad de activo y los valores agregados en AWS IoT SiteWise. Puede crear, administrar y ver la clave de cifrado mediante AWS KMS.

Puede elegir una clave Clave propiedad de AWS para cifrar sus datos o elegir una clave gestionada por el cliente para cifrar los valores de las propiedades de sus activos y los valores agregados:

Cómo funcionan

El cifrado en reposo se integra AWS KMS para administrar la clave de cifrado que se utiliza para cifrar los datos.

- Clave propiedad de AWS — Clave de cifrado predeterminada. AWS IoT SiteWise es el propietario de esta clave. No puedes ver esta clave en tu AWS cuenta. Tampoco puede ver las operaciones de la clave en los registros de AWS CloudTrail . Puede usar esta clave sin cargo adicional.
- Clave administrada por el cliente: la clave se almacena en la cuenta y usted la crea, posee y administra. Usted controla plenamente la clave KMS. Se aplican AWS KMS cargos adicionales.

Claves propiedad de AWS

Claves propiedad de AWS no están guardados en tu cuenta. Forman parte de una colección de claves de KMS que AWS posee y administra para su uso en varias AWS cuentas. AWS los servicios que puede utilizar Claves propiedad de AWS para proteger sus datos.

No puede ver, administrar Claves propiedad de AWS, usar ni auditar su uso. Sin embargo, no es necesario que realice ninguna acción ni que cambie programas para proteger las claves que cifran sus datos.

No se te cobra una cuota mensual ni una cuota de uso si las utilizas Claves propiedad de AWS, y estas no se tienen en cuenta para AWS KMS las cuotas de tu cuenta.

Claves administradas por el cliente

Las claves administradas por el cliente son claves KMS en su cuenta que usted ha creado, posee y administra. Tiene el control total sobre estas claves KMS, lo que significa que puede hacer lo siguiente:

- Establecer y mantener sus políticas de claves, políticas de IAM y concesiones.
- Activarlas y desactivarlas.
- Rotar sus materiales criptográficos.
- Agregar etiquetas.
- Crear alias que hagan referencia a ellas.
- Programar su eliminación.

También puedes usar CloudTrail Amazon CloudWatch Logs para realizar un seguimiento de las solicitudes que se AWS IoT SiteWise envían AWS KMS en tu nombre.

Si utilizas claves administradas por el cliente, debes conceder AWS IoT SiteWise acceso a la clave de KMS almacenada en tu cuenta. AWS IoT SiteWise utiliza el cifrado de sobres y la jerarquía de claves para cifrar los datos. La clave de AWS KMS cifrado se utiliza para cifrar la clave raíz de esta jerarquía de claves. Para obtener más información, consulte Cifrado de sobre en la Guía para desarrolladores de AWS Key Management Service .

El siguiente ejemplo de política concede AWS IoT SiteWise permisos para crear una clave gestionada por el cliente en su nombre. Al crear la clave, debe permitir las acciones `kms:CreateGrant` y `kms:DescribeKey`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1603902045292",
      "Action": [
        "kms:CreateGrant",
        "kms:DescribeKey"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

El contexto de cifrado para su concesión creada utiliza su `aws:iotsitewise:subscriberId` y su ID de cuenta.

Datos en reposo en las puertas de enlace SiteWise Edge

AWS IoT SiteWise las pasarelas almacenan los siguientes datos en el sistema de archivos local:

- Información de configuración de origen OPC-UA
- Conjunto de rutas de flujo de datos OPC-UA desde orígenes OPC-UA conectados
- Los datos industriales se almacenan en caché cuando la puerta de enlace SiteWise Edge pierde la conexión a Internet

SiteWise Las puertas de enlace Edge se ejecutan en funcionamiento. AWS IoT Greengrass AWS IoT Greengrass se basa en los permisos de archivos de Unix y en el cifrado de disco completo (si está activado) para proteger los datos almacenados en el núcleo. Es su responsabilidad proteger el sistema de archivos y el dispositivo.

Sin AWS IoT Greengrass embargo, cifra las copias locales de los secretos de su servidor OPC-UA recuperados de Secrets Manager. Para obtener más información, consulte Cifrado de secretos en la Guía para desarrolladores de AWS IoT Greengrass Version 1 .

Para obtener más información sobre el cifrado en reposo en AWS IoT Greengrass núcleos, consulte Cifrado en reposo en la AWS IoT Greengrass Version 1 Guía para desarrolladores.

Cifrado en tránsito

AWS IoT SiteWise tiene tres modos de comunicación en los que los datos están en tránsito:

- A través de Internet: la comunicación entre dispositivos locales (incluidas las puertas de enlace SiteWise Edge) AWS IoT SiteWise está cifrada.
- A través de la red local: la comunicación entre las puertas de OpsHub enlace de SiteWise la aplicación y las de SiteWise Edge siempre está cifrada. La comunicación entre la aplicación de SiteWise monitorización que se ejecuta en el navegador y las pasarelas de SiteWise Edge siempre está cifrada. La comunicación entre las puertas de enlace SiteWise Edge y las fuentes OPC-UA se puede cifrar.
- Entre los componentes de las puertas de enlace SiteWise Edge: la comunicación entre AWS IoT Greengrass los componentes de las puertas de enlace SiteWise Edge no está cifrada.

Temas

Datos en tránsito a través de Internet

AWS IoT SiteWise utiliza Transport Layer Security (TLS) para cifrar todas las comunicaciones a través de Internet. Todos los datos que se envían a la AWS nube se envían a través de una conexión TLS mediante los protocolos MQTT o HTTPS, por lo que son seguros de forma predeterminada. SiteWise Las pasarelas perimetrales, que se ejecutan en ellas AWS IoT Greengrass, y las notificaciones del valor de las propiedades utilizan el modelo de seguridad del AWS IoT transporte. Para obtener más información, consulte Seguridad de transporte en la Guía del desarrollador de AWS IoT .

Datos en tránsito a través de la red local

SiteWise Las pasarelas perimetrales siguen las especificaciones del OPC-UA para la comunicación con las fuentes OPC-UA locales. Es su responsabilidad configurar los orígenes para utilizar un modo de seguridad de mensajes que cifre los datos en tránsito.

Si elige un modo de seguridad de mensajes de firma, los datos en tránsito entre las puertas de enlace y las fuentes de SiteWise Edge se firman pero no se cifran. Si elige un modo de seguridad

para firmar y cifrar los mensajes, los datos en tránsito entre las puertas de enlace y las fuentes de SiteWise Edge se firman y cifran. Para obtener más información sobre la configuración de orígenes, consulte Configuración de orígenes de datos.

La comunicación entre la aplicación de consola perimetral y las puertas de enlace SiteWise Edge siempre se cifra mediante TLS. El conector SiteWise Edge de la puerta de enlace SiteWise Edge genera y almacena un certificado autofirmado para poder establecer una conexión TLS con la consola Edge para la aplicación. AWS IoT SiteWise Deberá copiar este certificado de la puerta de enlace SiteWise Edge a la consola de Edge para su AWS IoT SiteWise aplicación antes de conectar la aplicación a la puerta de enlace SiteWise Edge. Esto garantiza que la consola perimetral de AWS IoT SiteWise la aplicación pueda comprobar que se ha conectado a la puerta de enlace SiteWise Edge de confianza.

Además del TLS para garantizar el secreto y la autenticidad del servidor, SiteWise Edge utiliza el protocolo SiGv4 para establecer la autenticidad de la aplicación de la consola perimetral. El conector SiteWise Edge de la puerta de enlace SiteWise Edge acepta y almacena una contraseña para poder verificar las conexiones entrantes desde la aplicación de consola perimetral, la aplicación de SiteWise supervisión que se ejecuta en los navegadores y otros clientes según el AWS IoT SiteWise SDK.

Para obtener más información sobre generación de la contraseña y el certificado del servidor, consulte the section called “Administración de puertas de enlace SiteWise perimetrales”.

Datos en tránsito entre los componentes locales de las puertas de enlace SiteWise Edge

SiteWise Las puertas de enlace Edge funcionan AWS IoT Greengrass, lo que no cifra los datos intercambiados localmente en el AWS IoT Greengrass núcleo porque los datos no salen del dispositivo. Esto incluye la comunicación entre AWS IoT Greengrass componentes, como el AWS IoT SiteWise conector. Para obtener más información, consulte Datos en el dispositivo central en la Guía para desarrolladores de AWS IoT Greengrass Version 1 .

Administración de claves

AWS IoT SiteWise administración de claves en la nube

De forma predeterminada, Claves administradas por AWS se AWS IoT SiteWise utiliza para proteger sus datos en la AWS nube. Puede actualizar sus ajustes para utilizar una clave administrada por el

cliente para cifrar algunos datos en AWS IoT SiteWise. Puede crear, administrar y ver la clave de cifrado mediante AWS Key Management Service (AWS KMS).

AWS IoT SiteWise admite el cifrado del lado del servidor con claves administradas por el cliente almacenadas AWS KMS para cifrar los siguientes datos:

- Valores de propiedades de activos
- Valores agregados

> **Note**
>
> El resto de los datos y recursos se cifran mediante el cifrado predeterminado con claves gestionadas por. AWS IoT SiteWise Esta clave se almacena en la cuenta de AWS IoT SiteWise .

Para obtener más información, consulte ¿Qué es AWS Key Management Service? en la Guía para AWS Key Management Service desarrolladores.

Habilitación del cifrado mediante claves administradas por el cliente

Para usar las claves administradas por el cliente AWS IoT SiteWise, debes actualizar AWS IoT SiteWise la configuración.

Para habilitar el cifrado mediante claves KMS

1. Vaya a la consola de AWS IoT SiteWise.
2. Elija Ajustes de la cuenta y, a continuación, Editar para abrir la página Editar ajustes de la cuenta.
3. En Tipo de clave de cifrado, elija Elegir una clave AWS KMS diferente. Esto habilita el cifrado con claves administradas por el cliente almacenadas en AWS KMS.

   > **Note**
   >
   > En la actualidad, solo puede utilizar el cifrado con claves administradas por el cliente para valores de propiedad de activo y valores agregados.

4. Elija su clave KMS con una de las siguientes opciones:

- Para usar una clave KMS existente: elija el alias de su clave KMS de la lista.
- Para crear una clave KMS nueva, selecciona Crear una AWS KMS clave.

> **Note**
>
> Esto abre el panel de AWS KMS . Para obtener más información sobre cómo crear una clave KMS, consulte Creación de claves en la Guía para desarrolladores de AWS Key Management Service .

5. Elija Guardar para actualizar la configuración.

SiteWise Administración de claves de Edge Gateway

SiteWise Las puertas de enlace AWS IoT Greengrass perimetrales funcionan y los dispositivos AWS IoT Greengrass principales utilizan claves públicas y privadas para autenticarse en la AWS nube y cifrar los secretos locales, como los secretos de autenticación OPC-UA. Para obtener más información, consulte Administración de claves en la Guía para desarrolladores de AWS IoT Greengrass Version 1 .

Gestión de identidades y accesos para AWS IoT SiteWise

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos. AWS IoT SiteWise La IAM es una Servicio de AWS opción que puede utilizar sin coste adicional.

Temas

- Prevención de la sustitución confusa entre servicios
- Solución de problemas AWS IoT SiteWise de identidad y acceso

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo en el que se realice. AWS IoT SiteWise

Usuario del servicio: si utiliza el AWS IoT SiteWise servicio para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más AWS IoT SiteWise funciones para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en AWS IoT SiteWise, consulte Solución de problemas AWS IoT SiteWise de identidad y acceso.

Administrador de servicios: si estás a cargo de AWS IoT SiteWise los recursos de tu empresa, probablemente tengas acceso total a ellos AWS IoT SiteWise. Su trabajo consiste en determinar a qué AWS IoT SiteWise funciones y recursos deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar la IAM AWS IoT SiteWise, consulte¿Cómo AWS IoT SiteWise funciona con IAM.

Administrador de IAM: si es un administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a AWS. Para ver ejemplos de políticas AWS IoT SiteWise basadas en la identidad que puede utilizar en IAM, consulte. AWS IoT SiteWise ejemplos de políticas basadas en la identidad

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (IAM Identity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador

habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar las solicitudes de la AWS API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Uso de la autenticación multifactor (MFA) en AWSen la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console cambiando de función. Puede asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS Single Sign-On.
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener

información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
  - Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.
- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar una AWS función a una instancia EC2 y ponerla a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

¿Cómo AWS IoT SiteWise funciona con IAM

Antes de usar AWS Identity and Access Management (IAM) para administrar el acceso AWS IoT SiteWise, debe comprender con qué funciones de IAM está disponible. AWS IoT SiteWise

Característica de IAM	¿Comple con? AWS IoT SiteWis
Políticas basadas en identidad con permisos de nivel de recursos	Sí
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política	Sí
Políticas basadas en recursos	No
Listas de control de acceso (ACL)	No
Autorización basada en etiquetas (ABAC)	Sí
Credenciales temporales	Sí
Sesiones de acceso directo (FAS)	Sí
Roles vinculados al servicio	Sí
Roles de servicio	Sí

Para obtener una visión general de cómo AWS IoT SiteWise funcionan otros AWS servicios con IAM, consulte los AWS servicios que funcionan con IAM en la Guía del usuario de IAM.

Contenido

AWS IoT SiteWise Funciones de IAM

Un rol de IAM es una entidad de la Cuenta de AWS que dispone de permisos específicos.

Uso de credenciales temporales con AWS IoT SiteWise

Puede utilizar credenciales temporales para iniciar sesión con federación, asumir un rol de IAM o asumir un rol de acceso entre cuentas. Las credenciales de seguridad temporales se obtienen llamando a operaciones de AWS STS API como AssumeRoleo GetFederationToken.

AWS IoT SiteWise admite el uso de credenciales temporales.

SiteWise Monitor permite a los usuarios federados acceder a los portales. Los usuarios del portal se autentican con sus credenciales del Centro de identidades de IAM o IAM.

> **Important**
>
> Los usuarios o roles deben tener el permiso de `iotsitewise:DescribePortal` para iniciar sesión en el portal.

Cuando un usuario inicia sesión en un portal, SiteWise Monitor genera una política de sesión que proporciona los siguientes permisos:

- Acceso de solo lectura a los activos y a los datos de los activos de AWS IoT SiteWise su cuenta a los que proporciona acceso la función de ese portal.
- Acceso a proyectos en ese portal para los que el usuario tiene acceso de administrador (propietario del proyecto) o de solo lectura (lector del proyecto).

Para obtener más información acerca de los permisos de usuario federado del portal, consulte Uso de funciones de servicio para AWS IoT SiteWise Monitor.

Sesiones de acceso directo (FAS) para AWS IoT SiteWise

Admite Forward access sessions (FAS)	Sí

Cuando utiliza un usuario o un rol de IAM para realizar acciones en AWSél, se le considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros

Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Roles vinculados al servicio

Las funciones vinculadas al servicio permiten a AWS los servicios acceder a los recursos de otros servicios para completar una acción en su nombre. Los roles vinculados a servicios aparecen en la Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

AWS IoT SiteWise admite funciones vinculadas al servicio. Para obtener más información acerca de cómo crear o administrar roles vinculados a servicios de AWS IoT SiteWise , consulte Uso de roles vinculados a servicios de AWS IoT SiteWise.

Roles de servicio

Esta característica permite que un servicio asuma un rol de servicio en su nombre. Este rol permite que el servicio obtenga acceso a los recursos de otros servicios para completar una acción en su nombre. Los roles de servicio aparecen en su Cuenta de AWS y son propiedad de la cuenta. Esto significa que un administrador de IAM puede cambiar los permisos de este rol. Sin embargo, hacerlo podría deteriorar la funcionalidad del servicio.

AWS IoT SiteWise utiliza un rol de servicio para permitir que los usuarios del portal SiteWise Monitor accedan a algunos de sus AWS IoT SiteWise recursos en su nombre. Para obtener más información, consulte Uso de funciones de servicio para AWS IoT SiteWise Monitor.

Debe disponer de los permisos necesarios para poder crear modelos de AWS IoT Events alarma en él AWS IoT SiteWise. Para obtener más información, consulte Configurar los permisos para AWS IoT Events las alarmas.

Elección de un rol de IAM en AWS IoT SiteWise

Al crear un `portal` recurso en AWS IoT SiteWise, debe elegir un rol que permita a los usuarios federados de su portal SiteWise Monitor acceder AWS IoT SiteWise en su nombre. Si ya ha creado un rol de servicio, le AWS IoT SiteWise proporciona una lista de roles entre los que puede elegir. De lo contrario, puede crear un rol con los permisos necesarios al crear un portal. Es importante elegir un rol que permita acceder a los activos y a los datos de activos. Para obtener más información, consulte Uso de funciones de servicio para AWS IoT SiteWise Monitor.

Autorización basada en etiquetas de AWS IoT SiteWise

Puede adjuntar etiquetas a AWS IoT SiteWise los recursos o pasarles etiquetas en una solicitud AWS IoT SiteWise. Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`. Para obtener más información acerca del etiquetado de recursos de AWS IoT SiteWise , consulte Etiquetar sus recursos AWS IoT SiteWise.

Para consultar un ejemplo de política basada en la identidad para limitar el acceso a un recurso en función de las etiquetas de ese recurso, consulte Visualización de los activos de AWS IoT SiteWise basados en etiquetas.

AWS IoT SiteWise políticas basadas en la identidad

Las políticas de IAM le permiten controlar quién puede hacer qué en cada lugar. AWS IoT SiteWise Puede decidir qué acciones están permitidas o no y establecer condiciones específicas para estas acciones. Por ejemplo, puede establecer reglas sobre quién puede ver o cambiar la información AWS IoT SiteWise. AWS IoT SiteWise admite acciones, recursos y claves de condición específicos. Para obtener más información acerca de los elementos que utiliza en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Acciones de políticas

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Las acciones políticas AWS IoT SiteWise utilizan el siguiente prefijo antes de la acción:`iotsitewise:`. Por ejemplo, para conceder a alguien permiso para cargar datos de propiedades de activos AWS IoT SiteWise con la operación de la `BatchPutAssetPropertyValue` API, debes incluir la `iotsitewise:BatchPutAssetPropertyValue` acción en su política. Las

declaraciones de política deben incluir un `NotAction` elemento `Action` o. AWS IoT SiteWise define su propio conjunto de acciones que describen las tareas que puede realizar con este servicio.

Para especificar varias acciones de en una única instrucción, sepárelas con comas del siguiente modo.

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

Puede utilizar caracteres comodín (*) para especificar varias acciones . Por ejemplo, para especificar todas las acciones que comiencen con la palabra `Describe`, incluya la siguiente acción.

```
"Action": "iotsitewise:Describe*"
```

Para ver una lista de AWS IoT SiteWise acciones, consulte las acciones definidas por AWS IoT SiteWise en la Guía del usuario de IAM.

BatchPutAssetPropertyValue autorización

AWS IoT SiteWise autoriza el acceso a la BatchPutAssetPropertyValueacción de una manera inusual. En la mayoría de las acciones, al permitir o denegar el acceso, esa acción devuelve un error si no se conceden los permisos. Con `BatchPutAssetPropertyValue` ella, puedes enviar varias entradas de datos a diferentes activos y propiedades de activos en una sola solicitud de API. AWS IoT SiteWise autoriza cada entrada de datos de forma independiente. Para cualquier entrada individual que no supere la autorización de la solicitud, AWS IoT SiteWise incluye un error `AccessDeniedException` en la lista de errores devuelta. AWS IoT SiteWise recibe los datos de cualquier entrada que se autorice correctamente, incluso si otra entrada de la misma solicitud no es válida.

Important

Antes de incorporar datos a un flujo de datos, haga lo siguiente:

- Autorice el `time-series` recurso si utiliza un alias de propiedad para identificar el flujo de datos.

- Autorice el `asset` recurso si utiliza un identificador de activo para identificar el activo que contiene la propiedad del activo asociada.

Recursos de políticas

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Cada instrucción de política de IAM se aplica a los recursos especificados utilizando sus ARN. Un ARN tiene la siguiente sintaxis general.

```
arn:${Partition}:${Service}:${Region}:${Account}:${ResourceType}/${ResourcePath}
```

Para obtener más información sobre el formato de los ARN, consulte Nombres de recursos de Amazon (ARN) y espacios de nombres de AWS servicios.

Por ejemplo, para especificar el activo con el ID `a1b2c3d4-5678-90ab-cdef-22222EXAMPLE` en la instrucción, utilice el siguiente ARN.

```
"Resource": "arn:aws:iotsitewise:region:123456789012:asset/a1b2c3d4-5678-90ab-
cdef-22222EXAMPLE"
```

Para especificar todos los flujos de datos que pertenecen a una cuenta específica, utilice el carácter comodín (*):

```
"Resource": "arn:aws:iotsitewise:region:123456789012:time-series/*"
```

Para especificar todos los activos que pertenecen a una cuenta específica, utilice el carácter comodín (*):

```
"Resource": "arn:aws:iotsitewise:region:123456789012:asset/*"
```

Algunas AWS IoT SiteWise acciones, como las de creación de recursos, no se pueden realizar en un recurso específico. En dichos casos, debe utilizar el carácter comodín (*).

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

Para especificar varios recursos en una única instrucción, separe los ARN con comas.

```
"Resource": [
  "resource1",
  "resource2"
]
```

Para ver una lista de los tipos de AWS IoT SiteWise recursos y sus ARN, consulte los recursos definidos por AWS IoT SiteWise en la Guía del usuario de IAM. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por AWS IoT SiteWise.

Claves de condición de política

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

> **Important**
>
> Muchas claves de condición son específicas de un recurso y algunas acciones de API utilizan varios recursos. Si escribe una instrucción de política con una clave de condición, use el elemento `Resource` de la instrucción para especificar el recurso en el que se aplica la clave de condición. Si no lo hace, la política puede impedir que los usuarios ejecuten la acción, ya que la comprobación de la condición dará un error en el caso de los recursos en los que la clave de la condición no se aplica. Si no quiere especificar un recurso o si ha escrito el elemento `Action` de la política para que contenga varias acciones de API, debe utilizar el tipo de condición `...IfExists` para asegurarse de que no se tenga en cuenta la clave de condición en el caso de los recursos que no la utilicen. Para obtener más información, consulte... IfExists condiciones de la Guía del usuario de IAM.

AWS IoT SiteWise define su propio conjunto de claves de condición y también admite el uso de algunas claves de condición globales. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

AWS IoT SiteWise claves de condición

Clave de condición	Descripción	Tipos
`iotsitewise:isAssociatedWithAssetProperty`	Si los flujos de datos están asociados a una propiedad de activo. Utilice esta clave de condición para definir permisos basados en la existencia de una propiedad de activo asociada para flujos de datos.	Cadena

Clave de condición	Descripción	Tipos
	Ejemplo de valor: `true`	
`iotsitewise:assetHierarchyPath`	Ruta de la jerarquía del activo, que es una cadena de ID de activos separados cada uno por una barra inclinada. Utilice esta clave de condición para definir permisos basados en un subconjunto de la jerarquía de todos los activos de la cuenta. Ejemplo de valor: `/a1b2c3d4-5678-90ab-cdef-222222EXAMPLE/a1b2c3d4-5678-90ab-cdef-666666EXAMPLE`	Cadena
`iotsitewise:propertyId`	ID de una propiedad de activo. Utilice esta clave de condición para definir permisos basados en una propiedad específica de un modelo de activos. Esta clave de condición se aplica a todos los activos de ese modelo. Ejemplo de valor: `a1b2c3d4-5678-90ab-cdef-333333EXAMPLE`	Cadena

Clave de condición	Descripción	Tipos
`iotsitewise:childAssetId`	ID de un activo asociado como secundario a otro activo. Utilice esta clave de condición para definir permisos basados en activos secundarios. Para definir permisos basados en activos principales, utilice la sección de activos de una instrucción de política. Ejemplo de valor: `a1b2c3d4-5678-90ab-cdef-666 66EXAMPLE`	Cadena
`iotsitewise:iam`	El ARN de una identidad de IAM al enumerar las políticas de acceso. Utilice esta clave de condición para definir permisos de política de acceso para una identidad de IAM. Ejemplo de valor: `arn:aws:iam::123456789012:user/JohnDoe`	Cadena, null
`iotsitewise:propertyAlias`	El alias que identifica una propiedad de activo o un flujo de datos. Utilice esta clave de condición para definir permisos basados en el alias.	Cadena

Clave de condición	Descripción	Tipos
`iotsitewise:user`	El ID de un usuario del Centro de identidades de IAM al enumerar las políticas de acceso. Utilice esta clave de condición para definir los permisos de la política de acceso para un usuario del Centro de identidades de IAM. Ejemplo de valor: `a1b2c3d4e5-a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE`	Cadena, null
`iotsitewise:group`	El ID de un grupo del Centro de identidades de IAM al enumerar las políticas de acceso. Utilice esta clave de condición para definir los permisos de la política de acceso para un grupo del Centro de identidades de IAM. Ejemplo de valor: `a1b2c3d4e5-a1b2c3d4-5678-90ab-cdef-bbbbbEXAMPLE`	Cadena, null

Clave de condición	Descripción	Tipos
`iotsitewise:portal`	ID de un portal en una política de acceso. Utilice esta clave de condición para definir permisos de política de acceso basados en un portal. Ejemplo de valor: `a1b2c3d4-5678-90ab-cdef-77777EXAMPLE`	Cadena, null
`iotsitewise:project`	ID de un proyecto en una política de acceso o el ID de un proyecto para un panel. Utilice esta clave de condición para definir permisos de panel o política de acceso basados en un proyecto. Ejemplo de valor: `a1b2c3d4-5678-90ab-cdef-88888EXAMPLE`	Cadena, null

Para saber con qué acciones y recursos puede utilizar una clave condicionada, consulte Acciones definidas por AWS IoT SiteWise.

Ejemplos

Para ver ejemplos de políticas AWS IoT SiteWise basadas en la identidad, consulte. AWS IoT SiteWise ejemplos de políticas basadas en la identidad

AWS IoT SiteWise ejemplos de políticas basadas en la identidad

De forma predeterminada, las entidades (usuarios y roles) no tienen permiso para crear o modificar AWS IoT SiteWise recursos. Tampoco pueden realizar tareas mediante la AWS Management

Console, AWS Command Line Interface (AWS CLI) o la AWS API. Para ajustar los permisos, un administrador AWS Identity and Access Management (IAM) debe hacer lo siguiente:

1. Cree políticas de IAM que concedan a los usuarios y roles permisos para realizar operaciones de API específicas con los recursos que necesiten.
2. Adjunta esas políticas a los usuarios o grupos que requieren esos permisos.

Para obtener más información acerca de cómo crear una política basada en identidad de IAM con estos documentos de políticas de JSON de ejemplo, consulte Creación de políticas en la pestaña JSON en la Guía del usuario de IAM.

Temas

- Prácticas recomendadas relativas a políticas
- Mediante la consola de AWS IoT SiteWise
- Permitir a los usuarios que vean sus propios permisos
- Permitir a los usuarios ingerir datos en activos de una jerarquía
- Visualización de los activos de AWS IoT SiteWise basados en etiquetas

Prácticas recomendadas relativas a políticas

Las políticas basadas en la identidad determinan si alguien puede crear AWS IoT SiteWise recursos de tu cuenta, acceder a ellos o eliminarlos. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos

como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.

- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Política de validación de Analizador de acceso de IAM en la Guía de usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Configuración del acceso a una API protegido por MFA en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Mediante la consola de AWS IoT SiteWise

Para acceder a la AWS IoT SiteWise consola, necesita un conjunto básico de permisos. Estos permisos le permiten ver y administrar los detalles de los AWS IoT SiteWise recursos de su cuenta Cuenta de AWS.

Si creas una política demasiado restrictiva, es posible que la consola no funcione como se espera para los usuarios o roles (entidades) que cuenten con esa política. Para garantizar que esas entidades puedan seguir utilizando la AWS IoT SiteWise consola, adjúnteles la política AWSIoTSiteWiseConsoleFullAccessgestionada o defina permisos equivalentes para esas entidades. Para más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

Si las entidades solo utilizan la AWS Command Line Interface (CLI) o la AWS IoT SiteWise API, y no la consola, no necesitan estos permisos mínimos. En ese caso, basta con darles acceso a las acciones específicas que necesitan para sus tareas de API.

Permitir a los usuarios que vean sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o AWS .

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

```
}
```

Permitir a los usuarios ingerir datos en activos de una jerarquía

En este ejemplo, desea conceder Cuenta de AWS acceso a un usuario para escribir datos en todas las propiedades de los activos de una jerarquía de activos específica, empezando por el activo raíz. `a1b2c3d4-5678-90ab-cdef-22222EXAMPLE` La política concede el permiso `iotsitewise:BatchPutAssetPropertyValue` al usuario. Esta política utiliza la clave de condición `iotsitewise:assetHierarchyPath` para restringir el acceso a los activos cuya ruta de jerarquía coincide con el activo o sus descendientes.

```
{
  "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/*"
          ]
        }
      }
    }
  ]
}
```

Visualización de los activos de AWS IoT SiteWise basados en etiquetas

Utilice las condiciones de su política basada en la identidad para controlar el acceso a AWS IoT SiteWise los recursos en función de las etiquetas. En este ejemplo, se muestra cómo crear una política que permita la visualización de activos. Sin embargo, los activos solo se conceden si la etiqueta del activo `0wner` tiene el valor del nombre de usuario de dicho usuario. Esta política también otorga permiso para completar esta acción en la consola.

```
{
  "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}"
        }
      }
    }
  ]
}
```

Adjunta esta política a los usuarios de tu cuenta. Si un usuario llamado `richard-roe` intenta ver un AWS IoT SiteWise activo, el activo debe estar etiquetado `0wner=richard-roe` o`owner=richard-roe`. De lo contrario, se deniega el acceso a Richard. Los nombres de las claves de las etiquetas de condición no distinguen mayúsculas de minúsculas. Por lo tanto, `0wner` coincide con `0wner` y. `owner` Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador de IAM puede crear políticas de IAM. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una. Usuario raíz de la cuenta de AWS Para obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades

del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo AWS determinar si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

AWS políticas gestionadas para AWS IoT SiteWise

Simplifique la adición de permisos a usuarios, grupos y roles mediante políticas AWS administradas en lugar de tener que escribir las políticas usted mismo. Crear políticas de IAM gestionadas por los clientes que proporcionen a su equipo permisos precisos requiere tiempo y experiencia. Para una configuración más rápida, considere la posibilidad de utilizar nuestras políticas AWS gestionadas para los casos de uso más habituales. Encuentre políticas AWS administradas en su Cuenta de AWS. Para obtener más información acerca de las políticas administradas de AWS , consulte Políticas administradas de AWS en la Guía del usuario de IAM.

AWS los servicios se encargan de actualizar y mantener las políticas AWS administradas, lo que significa que no puede modificar los permisos de estas políticas. Ocasionalmente, AWS IoT SiteWise pueden añadir permisos para adaptarse a nuevas funciones, lo que afecta a todas las identidades con la política adjunta. Estas actualizaciones son habituales con la introducción de nuevos servicios o funciones. Sin embargo, los permisos nunca se eliminan, lo que garantiza que las configuraciones permanezcan intactas.

Además, AWS admite políticas gestionadas para funciones laborales que abarcan varios servicios. Por ejemplo, la política ReadOnlyAccess AWS gestionada proporciona acceso de solo lectura a todos los AWS servicios y recursos. Cuando un servicio lanza una nueva función, AWS agrega permisos de solo lectura para nuevas operaciones y recursos. Para obtener una lista con descripciones de las políticas de funciones laborales, consulte Políticas administradas por AWS para funciones laborales en la Guía del usuario de IAM.

AWS política gestionada: AWSIoTSiteWiseReadOnlyAccess

Utilice la política `AWSIoTSiteWiseReadOnlyAccess` AWS gestionada para permitir el acceso de solo lectura a. AWS IoT SiteWise

Puede adjuntar la política `AWSIoTSiteWiseReadOnlyAccess` a las identidades de IAM.

Permisos de nivel de servicio

Esta política proporciona acceso de solo lectura a. AWS IoT SiteWise No se incluyen otros permisos de servicio en esta política.

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

AWS política gestionada: AWSServiceRoleForIoTSiteWise

El rol `AWSServiceRoleForIoTSiteWise` utiliza la política `AWSServiceRoleForIoTSiteWise` con los siguientes permisos. Esta política:

- Permite AWS IoT SiteWise implementar puertas de enlace SiteWise Edge (que se ejecutan en ellas`AWS IoT Greengrass`).
- Permite AWS IoT SiteWise realizar registros.
- Permite AWS IoT SiteWise ejecutar una consulta de búsqueda de metadatos en la AWS IoT TwinMaker base de datos.

Si la utiliza AWS IoT SiteWise con una sola cuenta de usuario, el `AWSServiceRoleForIoTSiteWise` rol crea la `AWSServiceRoleForIoTSiteWise` política en su cuenta de IAM y la adjunta a las funciones vinculadas al `AWSServiceRoleForIoTSiteWise` servicio. 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 actualizaciones de las políticas gestionadas AWS

Puede ver los detalles sobre las actualizaciones de las políticas AWS administradas desde el momento en que este servicio comenzó a realizar el seguimiento de los cambios. AWS IoT SiteWise Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial del AWS IoT SiteWise documento.

Cambio	Descripción	Fecha
AWSServiceRoleForIoTSiteWise: actualización de una política actual	AWS IoT SiteWise ahora puede ejecutar una consulta de búsqueda de metadatos en la AWS IoT TwinMaker base de datos.	6 de noviembre de 2023
AWSIoTSiteWiseReadOnlyAccess: actualización de una política actual	AWS IoT SiteWise agregó un nuevo prefijo de política, `BatchGet*` , que le permite realizar operaciones de lectura por lotes.	16 de septiembre de 2022
AWSIoTSiteWiseReadOnlyAccess: política nueva	AWS IoT SiteWise agregó una nueva política para conceder acceso de solo lectura a. AWS IoT SiteWise	24 de noviembre de 2021
AWS IoT SiteWise comenzó a rastrear los cambios	AWS IoT SiteWise comenzó a realizar un seguimiento de los cambios de sus políticas AWS gestionadas.	24 de noviembre de 2021

Uso de roles vinculados a servicios de AWS IoT SiteWise

AWS IoT SiteWise utiliza funciones AWS Identity and Access Management vinculadas al servicio (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM al que se vincula directamente. AWS IoT SiteWise Los roles vinculados al servicio están predefinidos AWS IoT SiteWise e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Las funciones vinculadas al servicio simplifican la configuración al incluir automáticamente todos AWS IoT SiteWise los permisos necesarios. AWS IoT SiteWise define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo AWS IoT SiteWise puede asumir sus funciones. Los permisos definidos incluyen la política de confianza y la política de permisos. Y esa política de permisos no se puede adjuntar a ninguna otra entidad de IAM.

Solo es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. Esto protege sus AWS IoT SiteWise recursos porque no puede eliminar inadvertidamente el permiso de acceso a los recursos.

Para obtener información sobre otros servicios que admiten roles vinculados al servicio, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Rol vinculado al servicio. Seleccione una opción Sí con un enlace para ver la documentación relativa al rol vinculado al servicio en cuestión.

Temas

- Permisos de roles vinculados a servicios de AWS IoT SiteWise
- Creación de un rol vinculado a un servicio de AWS IoT SiteWise
- Editar un rol vinculado a un servicio para AWS IoT SiteWise
- Eliminación de un rol vinculado a un servicio de AWS IoT SiteWise
- Regiones compatibles para los roles vinculados al servicio AWS IoT SiteWise
- Uso de funciones de servicio para AWS IoT SiteWise Monitor

Permisos de roles vinculados a servicios de AWS IoT SiteWise

AWS IoT SiteWise usa el rol vinculado al servicio denominado. AWSServiceRoleForIoTSiteWise AWS IoT SiteWise utiliza esta función vinculada al servicio para implementar las puertas de enlace SiteWise Edge (que se ejecutan en ellas) y realizar el AWS IoT Greengrass registro.

El rol `AWSServiceRoleForIoTSiteWise` vinculado al servicio usa la `AWSServiceRoleForIoTSiteWise` política con los siguientes permisos. Esta política:

- Permite AWS IoT SiteWise implementar puertas de enlace SiteWise Edge (que se ejecutan en ellasAWS IoT Greengrass).
- Permite AWS IoT SiteWise realizar registros.
- Permite AWS IoT SiteWise ejecutar una consulta de búsqueda de metadatos en la AWS IoT TwinMaker base de datos.

Para obtener más información sobre las acciones permitidas enAWSServiceRoleForIoTSiteWise, consulte las políticas AWS gestionadas para 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"
      ]
     }
    }
   }
  ]
}
```

Puede usar los registros para monitorear y solucionar problemas de sus puertas de enlace SiteWise Edge. Para obtener más información, consulte Supervisión de los registros de SiteWise Edge Gateway.

Para permitir que una entidad de IAM (como un usuario, grupo o rol) cree, edite o elimine un rol vinculado al servicio, primero configure los permisos. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado a un servicio de AWS IoT SiteWise

No necesita crear manualmente un rol vinculado a servicios. Al realizar las siguientes operaciones en la AWS IoT SiteWise consola, AWS IoT SiteWise crea automáticamente el rol vinculado al servicio.

- Cree una puerta de enlace Greengrass V1.
- Configure la opción de registro.
- Elegir el botón de suscripción en el banner de ejecución de consultas.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al realizar cualquier operación en la AWS IoT SiteWise consola, vuelve a AWS IoT SiteWise crear el rol vinculado al servicio.

También puede utilizar la consola o la API de IAM para crear un rol de IAM vinculado al servicio para AWS IoT SiteWise.

- Para hacerlo en la consola de IAM, cree un rol con la AWSServiceRoleForIoTSiteWisepolítica y una relación de confianza con. `iotsitewise.amazonaws.com`
- Para hacerlo mediante la API AWS CLI o la API de IAM, cree un rol con la `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise` política y una relación de confianza con. `iotsitewise.amazonaws.com`

Para obtener más información, consulte Crear un rol vinculado a un servicio en la Guía del usuario de IAM.

Si elimina este rol vinculado al servicio, puede utilizar este mismo proceso para volver a crear el rol.

Editar un rol vinculado a un servicio para AWS IoT SiteWise

AWS IoT SiteWise no permite editar el rol vinculado al AWSServiceRoleForIoTSiteWise servicio. Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. Sin embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminación de un rol vinculado a un servicio de AWS IoT SiteWise

Si una función o un servicio que requiere un rol vinculado a un servicio ya no está en uso, se recomienda eliminar el rol asociado. Esto es para evitar tener una entidad inactiva que no esté siendo monitoreada o mantenida. Sin embargo, debe limpiar los recursos de su rol vinculado al servicio antes de eliminarlo manualmente.

> **Note**
>
> Si el AWS IoT SiteWise servicio utiliza el rol cuando intentas eliminar los recursos, es posible que la eliminación no se realice correctamente. Si eso sucede, espere unos minutos e inténtelo de nuevo.

Para eliminar AWS IoT SiteWise los recursos utilizados por el AWSServiceRoleForIoTSiteWise

1. Desactivar el registro de AWS IoT SiteWise. Para más información, consulte Cambiar el nivel de registro
2. Elimine todas las puertas de enlace SiteWise Edge activas.

Cómo eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al AWSServiceRoleForIoTSiteWise servicio. Para más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Regiones compatibles para los roles vinculados al servicio AWS IoT SiteWise

AWS IoT SiteWise admite el uso de funciones vinculadas al servicio en todas las regiones en las que el servicio está disponible. Para obtener más información, consulte Puntos de conexión y cuotas de AWS IoT SiteWise.

Uso de funciones de servicio para AWS IoT SiteWise Monitor

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

Para permitir que los usuarios federados del portal SiteWise Monitor accedan a sus AWS IAM Identity Center recursos AWS IoT SiteWisey a sus recursos, debe asignar un rol de servicio a cada portal que cree. El rol de servicio debe especificar a SiteWise Monitor como entidad de confianza e incluir la política AWSIoTSiteWiseMonitorPortalAccessadministrada o definir permisos equivalentes. Esta política la mantiene AWS y define el conjunto de permisos que SiteWise Monitor utiliza para acceder a sus recursos AWS IoT SiteWise y a los del IAM Identity Center.

Al crear un portal de SiteWise Monitor, debe elegir una función que permita a los usuarios de ese portal acceder a sus recursos AWS IoT SiteWisey a los del IAM Identity Center. La AWS IoT SiteWise consola puede crear y configurar el rol por usted. Puede editar el rol en IAM más adelante. Los usuarios de su portal tendrán problemas al usar sus portales de SiteWise Monitor si quita los permisos necesarios del rol o elimina el rol.

> **Note**
>
> Los portales creados antes del 29 de abril de 2020 no requerían roles de servicio. Si creó portales antes de esta fecha, deberá asociarles roles de servicio para poder seguir usándolos. Para ello, vaya a la página Portales de la consola de AWS IoT SiteWise y elija Migrar todos los portales a fin de utilizar roles de IAM.

En las siguientes secciones se describe cómo crear y administrar el rol del servicio de SiteWise monitoreo en el AWS Management Console o el AWS Command Line Interface.

Contenido

Permisos de rol de servicio para SiteWise Monitor

Al crear un portal, AWS IoT SiteWise permite crear un rol cuyo nombre comience por AWSIoTSiteWiseMonitorServiceRole. Esta función permite a los usuarios federados de SiteWise Monitor acceder a la configuración del portal, a los activos, a los datos de activos y a los datos de configuración del IAM Identity Center.

El rol confía en el siguiente servicio para asumir el rol:

- `monitor.iotsitewise.amazonaws.com`

El rol usa la siguiente política de permisos, cuyo nombre comienza por AWSIoTSiteWiseMonitorServicePortalPolicy, para permitir a los usuarios de SiteWise Monitor realizar

acciones en los recursos de su cuenta. La política AWSIoTSiteWiseMonitorPortalAccessadministrada define permisos equivalentes.

```
{
    "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"
                    ]
                }
            }
        }
    ]
}
```

Para obtener más información sobre los permisos necesarios para las alarmas, consulte Configurar los permisos para AWS IoT Events las alarmas.

Cuando un usuario del portal inicia sesión, SiteWise Monitor crea una política de sesión basada en la intersección de la función de servicio y las políticas de acceso de ese usuario. Las políticas de acceso definen el nivel de acceso de las identidades de a sus portales y proyectos. Para obtener más información sobre los permisos y las políticas de acceso al portal, consulte Administrar sus portales de SiteWise Monitor y CreateAccessPolicy.

Administrar la función del servicio de SiteWise supervisión (consola)

Esto Consola de AWS IoT SiteWise facilita la administración de la función de servicio de SiteWise monitoreo para los portales. Al crear un portal, la consola comprueba si las funciones existentes son aptas para adjuntarlas. Si no hay ninguno disponible, la consola puede crear y configurar un rol de servicio para usted. Para obtener más información, consulte Creación de un portal.

Temas

- Búsqueda del rol de servicio de un portal (consola)
- Creación de un rol de servicio de SiteWise monitoreo (AWS IoT SiteWise consola)
- Creación de un rol de servicio de SiteWise supervisión (consola de IAM)
- Cambio del rol de servicio de un portal (consola)

Búsqueda del rol de servicio de un portal (consola)

Siga los pasos siguientes para buscar el rol de servicio asociado a un portal de SiteWise Monitor.

Para buscar el rol de servicio de un portal

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación izquierdo, elija Portales.
3. Elija el portal para el que desea buscar el rol de servicio.

   El rol asociado al portal aparece en Permisos, Rol de servicio.

Creación de un rol de servicio de SiteWise monitoreo (AWS IoT SiteWise consola)

Al crear un portal de SiteWise Monitor, puede crear un rol de servicio para su portal. Para obtener más información, consulte Creación de un portal.

También puede crear un rol de servicio para un portal existente en la AWS IoT SiteWise consola. Esto sustituye el rol de servicio existente del portal.

Para crear un rol de servicio para un portal existente

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Portales.
3. Elija el portal para el que desea crear un nuevo rol de servicio.
4. En Detalles del portal, elija Editar.
5. En Permisos, elija Crear y usar un nuevo rol de servicio de la lista.
6. Escriba un nombre para el nuevo rol.
7. Seleccione Guardar.

Creación de un rol de servicio de SiteWise supervisión (consola de IAM)

Puede crear un rol de servicio a partir de la plantilla de rol de servicio de la consola de IAM. Esta plantilla de roles incluye la política AWSIoTSiteWiseMonitorPortalAccessadministrada y especifica a SiteWise Monitor como una entidad de confianza.

Para crear un rol de servicio a partir de la plantilla de roles de servicio del portal

1. Vaya a la consola de IAM.
2. Seleccione Roles en el panel de navegación.
3. Elija Crear rol.
4. En Elige un caso de uso, elige IoT SiteWise.
5. En Seleccionar su caso de uso, elija IoT SiteWise Monitor - Portal.
6. Elija Siguiente: Permisos.
7. Elija Siguiente: Etiquetas.
8. Elija Siguiente: Revisar.
9. Introduzca un Nombre de rol para el nuevo rol de servicio.
10. Seleccione Crear rol.

Cambio del rol de servicio de un portal (consola)

Utilice el siguiente procedimiento para elegir un rol de servicio de SiteWise supervisión diferente para un portal.

Para cambiar el rol de servicio de un portal

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación, elija Portales.
3. Elija el portal para el que desea cambiar el rol de servicio.
4. En Detalles del portal, elija Editar.
5. En Permisos, elija Usar un rol existente.
6. Elija un rol existente para asociar a este portal.
7. Seleccione Guardar.

Administración de la función de servicio de SiteWise supervisión (CLI)

Puede utilizarla AWS CLI para las siguientes tareas de administración de funciones de servicio de portal:

Temas

- Búsqueda del rol de servicio de un portal (CLI)

- Creación del rol de servicio de SiteWise monitoreo (CLI)

Búsqueda del rol de servicio de un portal (CLI)

Para encontrar el rol de servicio asociado a un portal de SiteWise Monitor, ejecute el siguiente comando para ver una lista de todos los portales de la región actual.

```
aws iotsitewise list-portals
```

La operación devuelve una respuesta que contiene los resúmenes de su portal en el siguiente formato.

```
{
  "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"
    }
  ]
}
```

También puede usar la DescribePortaloperación para encontrar la función de su portal si conoce el ID de su portal.

Creación del rol de servicio de SiteWise monitoreo (CLI)

Siga los siguientes pasos para crear un nuevo rol de servicio de SiteWise monitoreo.

Para crear un rol de servicio de SiteWise monitoreo

1. Cree un rol con una política de confianza que permita a SiteWise Monitor asumir el rol. En este ejemplo se crea un rol denominado **`MySiteWiseMonitorPortalRole`** a partir de una política de confianza almacenada en una cadena 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. Copie el ARN del rol de los metadatos del rol en la salida. Al crear un portal, debe utilizar este ARN para asociar el rol al portal. Para obtener más información sobre la creación de un portal, consulte CreatePortalla referencia de la AWS IoT SiteWise API.
3. Asocie la política `AWSIoTSiteWiseMonitorPortalAccess` con el rol o asocie una política que defina permisos equivalentes.

```
aws iam attach-role-policy --role-name MySiteWiseMonitorPortalRole --policy-arn
 arn:aws:iam::aws:policy/service-role/AWSIoTSiteWiseMonitorPortalAccess
```

Para asociar un rol de servicio a un portal existente

1. Para recuperar los detalles existentes del portal, ejecute el siguiente comando. Reemplace *`portal-id`* por el ID del portal.

```
aws iotsitewise describe-portal --portal-id portal-id
```

La operación devuelve una respuesta que contiene los detalles del portal en el siguiente formato.

```
{
    "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. Para asociar un rol de servicio a un portal, ejecute el siguiente comando. Reemplace el *role-arn* con el ARN del rol de servicio y reemplace los parámetros restantes con los valores existentes del portal.

```
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 Supervise las actualizaciones de AWSIoTSiteWiseMonitorServiceRole

Puede ver los detalles sobre las actualizaciones de AWSIoTSiteWiseMonitorServiceRolefor SiteWise Monitor, empezando por el momento en que este servicio comenzó a realizar el seguimiento de los cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial del AWS IoT SiteWise documento.

Cambio	Descripción	Fecha
AWSIoTSiteWiseMonitorPortalAccess: política actualizada	AWS IoT SiteWise actualizó la política AWSIoTSiteWiseMonitorPortalAccessgestionada para la función de alarmas.	27 de mayo de 2021
AWS IoT SiteWise comenzó a rastrear los cambios	AWS IoT SiteWise comenzó a rastrear los cambios de su función de servicio.	15 de diciembre de 2020

Configurar los permisos para AWS IoT Events las alarmas

Cuando utiliza un modelo de AWS IoT Events alarma para supervisar la propiedad de un AWS IoT SiteWise activo, debe tener los siguientes permisos de IAM:

- Un rol AWS IoT Events de servicio que permite AWS IoT Events enviar datos a AWS IoT SiteWise. Para obtener más información, consulte Administración de identidades y accesos de AWS IoT Events en la Guía para desarrolladores de AWS IoT Events .
- Debe tener los siguientes permisos de AWS IoT SiteWise acción: `iotsitewise:DescribeAssetModel` `yiotsitewise:UpdateAssetModelPropertyRouting`. Estos permisos permiten AWS IoT SiteWise enviar los valores de las propiedades de los activos a los modelos de AWS IoT Events alarma.

Para obtener más información, consulte Políticas basadas en recursos en la Guía del usuario de IAM.

Permisos de acción necesarios

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones. El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política.

Antes de definir un modelo de AWS IoT Events alarma, debe conceder los siguientes permisos que permiten AWS IoT SiteWise enviar los valores de las propiedades de los activos al modelo de alarma.

- `iotsitewise:DescribeAssetModel`— Permite AWS IoT Events comprobar si existe una propiedad de un activo.
- `iotsitewise:UpdateAssetModelPropertyRouting`— Permite AWS IoT SiteWise crear automáticamente suscripciones que permiten AWS IoT SiteWise enviar datos a AWS IoT Events.

Para obtener más información sobre las acciones AWS IoT SiteWise admitidas, consulte las acciones definidas AWS IoT SiteWise en la Referencia de autorización de servicios.

Example Ejemplo 1 de política de permisos

La siguiente política permite AWS IoT SiteWise enviar los valores de las propiedades de los activos a cualquier modelo de AWS IoT Events alarma.

```
{
    "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 Ejemplo 2 de política de permisos

La siguiente política permite AWS IoT SiteWise enviar los valores de una propiedad de activo específica a un modelo de AWS IoT Events alarma específico.

```
{
    "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 Permiso (opcional)

Al actualizar o eliminar un modelo de activo, AWS IoT SiteWise puede comprobar si un modelo de alarma AWS IoT Events monitorea una propiedad de activo asociada a este modelo de activo. Esto le impide eliminar una propiedad de activo que una AWS IoT Events alarma esté utilizando actualmente. Para activar esta función AWS IoT SiteWise, debe tener el `iotevents:ListInputRoutings` permiso. Este permiso permite AWS IoT SiteWise realizar llamadas a la operación de ListInputRoutingsAPI admitida por AWS IoT Events.

> **Note**
>
> Le recomendamos encarecidamente que añada el permiso `ListInputRoutings`.

Example Ejemplo de política de permisos

La siguiente política le permite actualizar y eliminar modelos de activos y utilizar la `ListInputRoutings` API en ellos 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/*"
        }
    ]
}
```

Permisos necesarios para SiteWise Monitor

Si desea utilizar la función de alarmas en los portales de SiteWise Monitor, debe actualizar la función del servicio de SiteWise Monitor con la siguiente política:

```
{
    "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"
                    ]
                }
            }
        }
    ]
}
```

Prevención de la sustitución confusa entre servicios

El problema de la sustitución confusa es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. En AWS, la suplantación de identidad entre servicios puede provocar el confuso problema de un diputado. La suplantación entre servicios puede producirse cuando un servicio (el servicio que lleva a cabo las llamadas) llama a otro servicio (el servicio al que se llama). El servicio que lleva a cabo las llamadas se puede manipular para utilizar sus permisos a fin de actuar en función de los recursos de otro cliente de una manera en la que no debe tener permiso para acceder. Para evitarlo, AWS proporciona herramientas que le ayudan a proteger sus datos para todos los servicios con entidades principales de servicio a las que se les ha dado acceso a los recursos de su cuenta.

Se recomienda utilizar las claves de contexto de condición `aws:SourceAccount`global `aws:SourceArn`y las claves de contexto en las políticas de recursos para limitar los permisos que se AWS IoT SiteWise otorgan a otro servicio al recurso. Si el valor de `aws:SourceArn` no contiene el ID de cuenta, como un nombre de recurso de Amazon (ARN) de bucket de Amazon S3, debe utilizar ambas claves de contexto de condición global para limitar los permisos. Si utiliza claves de contexto de condición global y el valor de `aws:SourceArn` contiene el ID de cuenta, el valor de `aws:SourceAccount` y la cuenta en el valor de `aws:SourceArn` deben utilizar el mismo ID de cuenta cuando se utiliza en la misma instrucción de política.

- Utilice `aws:SourceArn` si desea que solo se asocie un recurso al acceso entre servicios.
- Utilice `aws:SourceAccount` si quiere permitir que cualquier recurso de esa cuenta se asocie al uso entre servicios.

El valor de `aws:SourceArn` debe ser el recurso AWS IoT SiteWise del cliente asociado a la `sts:AssumeRole` solicitud.

La forma más eficaz de protegerse contra el problema de la sustitución confusa es utilizar la clave de contexto de condición global de `aws:SourceArn` con el ARN completo del recurso. Si no conoce el ARN completo del recurso o si especifica varios recursos, utilice la clave de condición de contexto global `aws:SourceArn` con comodines (*) para las partes desconocidas del ARN. Por ejemplo, `arn:aws:servicename:*:123456789012:*`.

Example — Confundido: Deputy Prevention

El siguiente ejemplo muestra cómo se pueden utilizar las claves de contexto `aws:SourceArn` y de condición `aws:SourceAccount` global AWS IoT SiteWise para evitar el confuso problema de los diputados.

```
{
  "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"
      }
    }
  }
}
```

Solución de problemas AWS IoT SiteWise de identidad y acceso

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas más comunes que pueden surgir al trabajar con AWS IoT SiteWise y AWS Identity and Access Management (IAM).

Temas

No estoy autorizado a realizar ninguna acción en AWS IoT SiteWise

Si AWS Management Console le indica que no está autorizado a realizar una acción, debe ponerse en contacto con su administrador para obtener ayuda. Su administrador es la persona que le facilitó su nombre de usuario y contraseña.

El siguiente ejemplo de error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para ver los detalles de un activo, pero no dispone de los permisos `iotsitewise:DescribeAsset`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 iotsitewise:DescribeAsset on resource: a1b2c3d4-5678-90ab-cdef-22222EXAMPLE
```

En este caso, Mateo pide a su administrador que actualice sus políticas de forma que pueda obtener acceso al activo del activo con el ID `a1b2c3d4-5678-90ab-cdef-22222EXAMPLE` mediante la acción `iotsitewise:DescribeAsset`.

No tengo autorización para realizar **`iam:PassRole`**

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, las políticas deben actualizarse a fin de permitirle pasar un rol a AWS IoT SiteWise.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en AWS IoT SiteWise. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

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

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador. AWS El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis AWS IoT SiteWise recursos

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para saber si AWS IoT SiteWise es compatible con estas funciones, consulte¿Cómo AWS IoT SiteWise funciona con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.

- Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Validación de conformidad para AWS IoT SiteWise

AWS IoT SiteWise no está incluido en el ámbito de ningún programa de AWS cumplimiento.

Para obtener una lista de AWS los servicios incluidos en el ámbito de los programas de cumplimiento específicos, consulte los AWS servicios incluidos en el ámbito de aplicación por programa de cumplimiento y . Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descargar informes en AWS Artifact .

Su responsabilidad de conformidad al AWS IoT SiteWise utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en la seguridad y el cumplimiento. AWS
- Documento técnico sobre cómo diseñar una arquitectura basada en la seguridad y el cumplimiento de la HIPAA: en este documento técnico se describe cómo pueden utilizar las empresas para crear aplicaciones que cumplan con la HIPAA. AWS
- AWS Recursos de cumplimiento Recursos de de trabajo y guías puede aplicarse a su sector y ubicación.
- Evaluación de los recursos con las reglas de la Guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Este AWS servicio proporciona una visión integral del estado de su seguridad AWS que le ayuda a comprobar su conformidad con los estándares y las mejores prácticas del sector de la seguridad.
- Diez reglas de oro de seguridad para soluciones de IoT industrial: esta entrada de blog presenta diez reglas de oro que ayudan a proteger sus sistemas de control industrial (ICS), internet de las cosas industrial (IIoT) y entornos en la nube.

- Mejores prácticas de seguridad para la fabricación de OT: este documento técnico describe las mejores prácticas de seguridad para diseñar, implementar y diseñar estas cargas de trabajo de fabricación híbrida locales para la nube. AWS

Resiliencia en AWS IoT SiteWise

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. AWS Las regiones proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

AWS IoT SiteWise está totalmente gestionado y utiliza AWS servicios duraderos y de alta disponibilidad, como Amazon S3 y Amazon EC2. Para garantizar la disponibilidad en caso de que se produzca una interrupción en la zona de disponibilidad, AWS IoT SiteWise opera en varias zonas de disponibilidad.

Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte Infraestructura AWS global.

Además de la infraestructura AWS global, AWS IoT SiteWise ofrece varias funciones para ayudarlo a satisfacer sus necesidades de respaldo y resiliencia de datos:

- Puede publicar actualizaciones del valor de las propiedades AWS IoT Core mediante mensajes MQTT y, a continuación, configurar reglas para actuar en función de esos datos. Con esta función, puede realizar copias de seguridad de los datos en otros AWS servicios, como Amazon S3 y Amazon DynamoDB. Para obtener más información, consulte Interacción con otros AWS servicios y Exporte datos a Amazon S3 con notificaciones de propiedad de activos.
- Puede usar las AWS IoT SiteWise `Get*` API para recuperar y hacer copias de seguridad de los datos históricos de propiedades de los activos. Para obtener más información, consulte Consulta de los valores históricos de las propiedades de los activos.
- Puede usar las AWS IoT SiteWise `Describe*` API para recuperar las definiciones de sus recursos, como activos y modelos. Puede realizar una copia de seguridad de estas definiciones y luego utilizarlas para volver a crear los recursos. Para obtener más información, consulte la Referencia de la API de AWS IoT SiteWise .

Seguridad de la infraestructura en AWS IoT SiteWise

Como servicio gestionado, AWS IoT SiteWise está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder a AWS IoT SiteWise través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

SiteWise Las pasarelas perimetrales, que se ejecutan en AWS IoT Greengrass ella, utilizan certificados X.509 y claves criptográficas para conectarse a la nube y autenticarse en ella. AWS Para obtener más información, consulte Autenticación y autorización de dispositivos para AWS IoT Greengrass en la Guía para desarrolladores de AWS IoT Greengrass Version 1 .

Configuración y análisis de vulnerabilidades

Las flotas de IoT pueden constar de un gran número de dispositivos que tienen diversas funcionalidades, son de larga duración y están distribuidos geográficamente. Estas características hacen que la configuración de la flota sea compleja y propensa a errores. Como los dispositivos suelen tener una capacidad de procesamiento, memoria y almacenamiento limitados, no siempre son compatibles con el cifrado y otras medidas de seguridad. Además, los dispositivos a menudo usan software con vulnerabilidades conocidas. Estos factores hacen que las flotas de IoT sean un objetivo atractivo para los piratas informáticos y dificultan la protección continuada de la flota de dispositivos.

AWS IoT Device Defender aborda estos desafíos proporcionando herramientas para identificar los problemas de seguridad y las desviaciones de las mejores prácticas. Úselo AWS IoT Device

Defender para analizar, auditar y monitorear los dispositivos conectados a fin de detectar comportamientos anormales y mitigar los riesgos de seguridad. AWS IoT Device Defender puede auditar las flotas de dispositivos para garantizar que cumplen las mejores prácticas de seguridad y detectar comportamientos anormales en los dispositivos. Esto permite aplicar políticas de seguridad coherentes en toda su flota de AWS IoT dispositivos y responder rápidamente cuando los dispositivos se ven comprometidos. Para obtener más información, consulte AWS IoT Device Defender en la Guía para desarrolladores de AWS IoT .

Si utiliza las puertas de enlace SiteWise Edge para introducir datos en el servicio, es su responsabilidad configurar y mantener el entorno de su puerta de enlace SiteWise Edge. Esta responsabilidad incluye la actualización a las versiones más recientes del software del sistema, AWS IoT Greengrass el software y el conector de la AWS IoT SiteWise puerta de enlace SiteWise Edge. Para obtener más información, consulte Configurar el AWS IoT Greengrass núcleo en la Guía para AWS IoT Greengrass Version 1 desarrolladores yActualización de un conector.

Puntos de conexión de VPC

Un punto final de VPC de interfaz establece una conexión privada entre su nube privada virtual (VPC) y. AWS IoT SiteWiseAWS PrivateLinkpotencia los puntos finales de la interfaz, lo que permite el acceso privado a AWS IoT SiteWise las operaciones de la API. Puede evitar la necesidad de una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o AWS Direct Connect. Las instancias de su VPC no necesitan direcciones IP públicas para comunicar con las operaciones de la API de AWS IoT SiteWise . El tráfico entre su VPC y AWS IoT SiteWise no sale de la AWS red.

Cada punto de conexión de la interfaz está representado por una o más interfaces de redes elásticas en las subredes.

Antes de configurar un punto de enlace de VPC de interfaz para AWS IoT SiteWise, consulte las propiedades y limitaciones del punto de enlace de interfaz en la Guía del usuario de Amazon VPC.

Para obtener más información, consulte Puntos de conexión de VPC de interfaz (AWS PrivateLink) en la Guía del usuario de Amazon VPC.

Operaciones de API compatibles para puntos finales de VPC

AWS IoT SiteWise admite realizar llamadas a las siguientes operaciones de AWS IoT SiteWise API desde su VPC:

- Para todas las operaciones de la API del plano de datos, utilice el siguiente punto final: *region*Sustitúyalo por su Región de AWS

```
data.iotsitewise.region.amazonaws.com
```

  Las operaciones de la API del plano de datos incluyen lo siguiente:

  - BatchGetAssetPropertyValue
  - BatchGetAssetPropertyValueHistory
  - BatchPutAssetPropertyValue
  - GetAssetPropertyAggregates
  - GetAssetPropertyValue
  - GetAssetPropertyValueHistory
  - GetInterpolatedAssetPropertyValues

- Para las operaciones de la API del plano de control que utiliza para gestionar los modelos de activos, los activos, las pasarelas de SiteWise Edge, las etiquetas y las configuraciones de cuentas, utilice el siguiente punto final. Sustituya *region* por su Región de AWS.

```
api.iotsitewise.region.amazonaws.com
```

  Las operaciones de la API del plano de control admitidas incluyen lo siguiente:

  - 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**
>
> El punto final de la interfaz de VPC para las operaciones de la API del plano de control actualmente no admite realizar llamadas a las siguientes operaciones de la API de SiteWise Monitor:
>
> - BatchAssociateProjectAssets
> - BatchDisassociateProjectAssets
> - CreateAccessPolicy
> - CreateDashboard

- CreatePortal
- CreateProject
- DeleteAccessPolicy
- DeletePortal
- DeleteProject
- DescribeAccessPolicy
- DescribePortal
- DescribeProject
- ListAccessPolicies
- ListDashboards
- ListPortals
- ListProjects
- ListProjectAssets
- UpdateAccessPolicy
- UpdateDashboard
- UpdatePortal
- UpdateProject

Creación de un punto de conexión de VPC de interfaz para AWS IoT SiteWise

Para crear un punto de enlace de VPC para el AWS IoT SiteWise servicio, utilice la consola de Amazon VPC o (). AWS Command Line Interface AWS CLI Para más información, consulte Creación de un punto de conexión de interfaz en la Guía del usuario de Amazon VPC.

Cree un punto de enlace de VPC con uno de los siguientes nombres de servicio: AWS IoT SiteWise

- Para las operaciones de la API del plano de datos, utilice el siguiente nombre de servicio:

```
com.amazonaws.region.iotsitewise.data
```

- Para las operaciones de la API del plano de control, utilice el siguiente nombre de servicio:

```
com.amazonaws.region.iotsitewise.api
```

Acceso a AWS IoT SiteWise través de un punto final de VPC de interfaz

Al crear un punto final de interfaz, generamos nombres de host DNS específicos del punto final con los que puede comunicarse. AWS IoT SiteWise La opción de DNS privado está habilitada de forma predeterminada. Para obtener más información, consulte Uso de zonas alojadas privadas en la Guía del usuario de Amazon VPC.

Si habilitas el DNS privado para el punto final, puedes realizar solicitudes de API a AWS IoT SiteWise través de uno de los siguientes puntos finales de VPC.

- Para las operaciones de la API del plano de datos, usa el siguiente punto final: reemplaza la *región por la* tuya. Región de AWS

```
data.iotsitewise.region.amazonaws.com
```

- Para las operaciones de la API del plano de control, utilice el siguiente punto final: Sustituya *la región por la* suya Región de AWS.

```
api.iotsitewise.region.amazonaws.com
```

Si inhabilita el DNS privado para el punto final, debe hacer lo siguiente para acceder a AWS IoT SiteWise través del punto final:

1. Especifique la url del punto de conexión de VPC en las solicitudes de la API.
   - Para las operaciones de la API del plano de datos, utilice la siguiente URL del punto final. Sustituya una *región* por el ID *vpc-endpoint-id*y la región del punto final de la VPC.

```
vpc-endpoint-id.data.iotsitewise.region.vpce.amazonaws.com
```

   - Para las operaciones de la API del plano de control, utilice la siguiente URL de punto final. Sustituya una *región* por el ID *vpc-endpoint-id*y la región del punto final de la VPC.

```
vpc-endpoint-id.api.iotsitewise.region.vpce.amazonaws.com
```

2. Inhabilite la inyección de prefijos de host. Los AWS SDK AWS CLI y los SDK anteponen al punto final del servicio varios prefijos de host al llamar a cada operación de API. Esta función hace que los AWS SDK AWS CLI y los SDK generen URL que no son válidas AWS IoT SiteWise cuando se especifica un punto final de VPC.

   > **Important**
   >
   > No puedes deshabilitar la inyección de prefijos de host en el o en. AWS CLI AWS Tools for PowerShell Esto significa que si inhabilitas el DNS privado, no podrás usar estas herramientas para acceder a AWS IoT SiteWise través del punto final de la VPC. Habilita el DNS privado para usar el AWS CLI o AWS Tools for PowerShell para acceder a AWS IoT SiteWise través del punto final.

   Para obtener más información sobre cómo deshabilitar la inyección de prefijos de host en los AWS SDK, consulta las siguientes secciones de la documentación de cada 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

Para más información, consulte Acceso a un servicio a través de un punto de conexión de interfaz en la Guía del usuario de Amazon VPC.

Crear una política de puntos de conexión de VPC para AWS IoT SiteWise

Puede asociar una política de punto de conexión con su punto de conexión de VPC que controla el acceso a AWS IoT SiteWise. La política especifica la siguiente información:

- La entidad principal que puede realizar operaciones.
- Las operaciones que se pueden realizar.
- Los recursos con los que se pueden realizar las operaciones.

Para más información, consulte Control del acceso a los servicios con puntos de enlace de la VPC en la Guía del usuario de Amazon VPC.

Ejemplo: política de puntos finales de VPC para acciones AWS IoT SiteWise

El siguiente es un ejemplo de una política de puntos finales para AWS IoT SiteWise. Cuando se adjunta a un punto final, esta política otorga acceso al usuario a las AWS IoT SiteWise acciones enumeradas *iotsitewiseadmin*en Cuenta de AWS *123456789012* en el activo especificado.

```
{
    "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"
                ]
            }
        }
    ]
}
```

Mejores prácticas de seguridad para AWS IoT SiteWise

Este tema contiene las prácticas recomendadas de seguridad para AWS IoT SiteWise.

Usar credenciales de autenticación en los servidores OPC-UA

Exija las credenciales de autenticación para conectarse a sus servidores OPC-UA. Consulte la documentación de los servidores para hacerlo. A continuación, para permitir que la puerta de enlace SiteWise Edge se conecte a los servidores OPC-UA, añada los secretos de autenticación del servidor a la puerta de enlace SiteWise Edge. Para obtener más información, consulte Configuración de la autenticación de origen.

Usar modos de comunicación cifrados para los servidores OPC-UA

Elija un modo de seguridad de mensajes cifrados y no obsoleto al configurar las fuentes OPC-UA para su puerta de enlace Edge. SiteWise Esto ayuda a proteger los datos industriales a medida que se transfieren de los servidores OPC-UA a la puerta de enlace Edge. SiteWise Para obtener más información, consulte Datos en tránsito a través de la red local y Configuración de orígenes de datos.

Mantener los componentes actualizados

Si utiliza las puertas de enlace SiteWise Edge para introducir datos en el servicio, es su responsabilidad configurar y mantener el entorno de su puerta de enlace Edge. SiteWise Esta responsabilidad incluye la actualización del software del sistema de la puerta de enlace, del software de AWS IoT Greengrass y de los conectores a sus últimas versiones.

> **Note**
>
> El conector AWS IoT SiteWise Edge almacena información confidencial en su sistema de archivos. Estos secretos controlan quién puede ver los datos almacenados en caché en su puerta de enlace SiteWise Edge. Se recomienda encarecidamente activar el cifrado del disco o del sistema de archivos en el sistema en el que se ejecuta la puerta de enlace Edge. SiteWise

Cifra el sistema de archivos de tu puerta de enlace SiteWise Edge

Cifre y proteja su puerta de enlace SiteWise Edge para que sus datos industriales estén seguros a medida que se mueven a través de la puerta de enlace SiteWise Edge. Si su puerta de enlace SiteWise Edge tiene un módulo de seguridad de hardware, puede configurarlo AWS IoT Greengrass para proteger su puerta de enlace SiteWise Edge. Para obtener más información, consulte Integración de la seguridad del hardware en la Guía para desarrolladores de AWS IoT

Greengrass Version 1 . De lo contrario, consulte la documentación del sistema operativo para obtener información sobre cómo cifrar y proteger el sistema de archivos.

Acceso seguro a la configuración de su periferia

No compartas la contraseña de la aplicación de la consola perimetral ni la contraseña de la aplicación SiteWise Monitor. No coloque esta contraseña en lugares donde cualquiera pueda verla. Implemente una política de rotación de contraseñas saludable configurando una caducidad apropiada para su contraseña.

Otorgue a los usuarios de SiteWise Monitor los permisos mínimos posibles

Siga el principio de privilegio mínimo utilizando el conjunto mínimo de permisos de la política de acceso para los usuarios de su portal.

- Al crear un portal, defina un rol que permita el conjunto mínimo de activos necesarios para ese portal. Para obtener más información, consulte Uso de funciones de servicio para AWS IoT SiteWise Monitor.
- Cuando los administradores del portal y usted creen y compartan proyectos, utilice el conjunto mínimo de activos necesarios para ese proyecto.
- Cuando una identidad ya no necesite acceder a un portal o proyecto, elimínela de ese recurso. Si esa identidad ya no es aplicable a su organización, elimínela de su almacén de identidades.

La práctica recomendada de principio mínimo también se aplica a los roles de IAM. Para obtener más información, consulte Prácticas recomendadas relativas a políticas.

No exponer información confidencial

Debe evitar el registro de credenciales y otra información confidencial, como la información de identificación personal (PII). Le recomendamos que implemente las siguientes medidas de seguridad, aunque el acceso a los registros locales en una puerta de enlace de SiteWise Edge requiera privilegios de root y el acceso a CloudWatch los registros requiera permisos de IAM.

- No utilice información confidencial en nombres, descripciones o propiedades de sus activos o modelos.
- No utilices información confidencial en los nombres de las fuentes o la puerta de enlace de SiteWise Edge.

- No utilice información confidencial en nombres o descripciones de sus portales, proyectos o paneles.

Siga las prácticas recomendadas de AWS IoT Greengrass seguridad

Siga las prácticas recomendadas de AWS IoT Greengrass seguridad para su puerta de enlace SiteWise Edge. Para obtener más información, consulte Prácticas recomendadas de seguridad en la Guía para desarrolladores de AWS IoT Greengrass Version 1 .

Véase también

- Prácticas recomendadas de seguridad en la Guía para desarrolladores de AWS IoT
- Diez reglas de oro de seguridad para las soluciones de IoT industrial

Inicio de sesión y supervisión AWS IoT SiteWise

La supervisión es una parte importante del mantenimiento de la confiabilidad, la disponibilidad y el rendimiento de AWS IoT SiteWise sus demás AWS soluciones. AWS IoT SiteWise es compatible con las siguientes herramientas de supervisión para supervisar el servicio, informar cuando algo va mal y tomar medidas automáticas cuando sea necesario:

- Amazon CloudWatch monitorea tus AWS recursos y las aplicaciones en las que AWS ejecutas en tiempo real. Recopile métricas y realice un seguimiento, cree paneles personalizados y configure alarmas que le notifiquen o tomen medidas cuando una métrica específica alcance un determinado umbral. Por ejemplo, puede CloudWatch hacer un seguimiento del uso de la CPU u otras métricas de sus instancias de Amazon EC2 y lanzar automáticamente nuevas instancias cuando sea necesario. Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.
- Amazon CloudWatch Logs supervisa, almacena y accede a sus archivos de registro desde las puertas de enlace de SiteWise Edge y otras fuentes. CloudTrail CloudWatch Los registros pueden monitorear la información de los archivos de registro y notificarle cuando se alcanzan ciertos umbrales. También se pueden archivar los datos del registro en un almacenamiento de larga duración. Para obtener más información, consulta la Guía del usuario CloudWatch de Amazon Logs.
- AWS CloudTrailcaptura las llamadas a la API y los eventos relacionados realizados por su AWS cuenta o en su nombre. A continuación, CloudTrail entrega los archivos de registro a un bucket de Amazon S3 que especifique. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. Para obtener más información, consulte la Guía del usuario de AWS CloudTrail.

Temas

Supervisión con Amazon CloudWatch Logs

Configure AWS IoT SiteWise para registrar la información en CloudWatch los registros a fin de supervisar y solucionar los problemas del servicio.

Cuando utilizas la AWS IoT SiteWise consola, AWS IoT SiteWise crea un rol vinculado al servicio que permite al servicio registrar la información en tu nombre. Si no usa la AWS IoT SiteWise consola, debe crear manualmente un rol vinculado al servicio para recibir los registros. Para obtener más información, consulte Creación de un rol vinculado a un servicio de AWS IoT SiteWise.

Debe tener una política de recursos que permita colocar AWS IoT SiteWise los eventos de registro en CloudWatch las transmisiones. Para crear y actualizar una política de recursos para CloudWatch los registros, ejecute el siguiente comando. *logging-policy-name*Sustitúyalo por el nombre de la política que se va a crear.

```
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 Los registros también admiten las claves de contexto aws: SourceArn y aws: SourceAccount condition. Estas claves de contexto de condición son opcionales.

Para crear o actualizar una política de recursos que AWS IoT SiteWise permita colocar únicamente los registros asociados al AWS IoT SiteWise recurso especificado en las CloudWatch transmisiones, ejecute el comando y haga lo siguiente:

- *logging-policy-name*Sustitúyalo por el nombre de la política que se va a crear.
- Sustituya *Source-ARN* por el ARN de su AWS IoT SiteWise recurso, como un modelo o activo de activos. Para encontrar el ARN de cada tipo de AWS IoT SiteWise recurso, consulte Tipos de recursos definidos AWS IoT SiteWise en la Referencia de autorización de servicio.
- Sustituya el *ID de cuenta* por el ID de AWS cuenta asociado al recurso especificado. 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\"]}}}]}"
```

De forma predeterminada, AWS IoT SiteWise no registra la información en los CloudWatch registros. Para activar el registro, elige un nivel de registro que no sea Desactivado (`OFF`). AWS IoT SiteWise admite los siguientes niveles de registro:

- `OFF`: el registro está desactivado.
- `ERROR`: se registran los errores.
- `INFO`: se registran los errores y los mensajes informativos.

Puede configurar las puertas de enlace SiteWise Edge para que registren la información en CloudWatch Logs Through AWS IoT Greengrass. Para obtener más información, consulte Supervisión de los registros de SiteWise Edge Gateway.

También puede configurarlas AWS IoT Core para que registren información en los CloudWatch registros si está solucionando una acción de AWS IoT SiteWise regla. Para obtener más información, consulte Solución de problemas y acción de AWS IoT SiteWise regla.

Contenido

Administrar el inicio de sesión AWS IoT SiteWise

Utilice la AWS IoT SiteWise consola o AWS CLI para las siguientes tareas de configuración de registro.

Encuentra tu nivel de registro

Console

Utilice el procedimiento siguiente para buscar el nivel de registro actual en la consola de AWS IoT SiteWise .

Para encontrar su nivel de AWS IoT SiteWise registro actual

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación izquierdo, elija Logging options (Opciones de registro).

   El estado actual de registro aparece en Logging status (Estado de registro). Si el registro está activado, el nivel de registro actual aparece en Nivel de detalle.

AWS CLI

Ejecute el siguiente comando para encontrar su nivel de AWS IoT SiteWise registro actual con el AWS CLI.

```
aws iotsitewise describe-logging-options
```

La operación devuelve una respuesta que contiene el nivel de registro en el siguiente formato.

```
{
  "loggingOptions": {
    "level": "String"
  }
}
```

Cambiar el nivel de registro

Utilice el siguiente procedimiento para cambiar el nivel de registro en la AWS IoT SiteWise consola o mediante AWS CLI.

Console

Para cambiar el nivel de AWS IoT SiteWise registro

1. Vaya a la consola de AWS IoT SiteWise.
2. En el panel de navegación izquierdo, elija Logging options (Opciones de registro).
3. Elija Editar.
4. Elija el Nivel de detalle que desea activar.
5. Seleccione Guardar.

AWS CLI

Ejecute el siguiente AWS CLI comando para cambiar el nivel de AWS IoT SiteWise registro. Reemplace *logging-level* por el nivel de registro que desee.

```
aws iotsitewise put-logging-options --logging-options level=logging-level
```

Ejemplo: entradas de archivos de AWS IoT SiteWise registro

Cada entrada de AWS IoT SiteWise registro incluye información sobre el evento y los recursos relevantes para ese evento, de modo que pueda comprender y analizar los datos del registro.

En el siguiente ejemplo, se muestra una CloudWatch entrada de AWS IoT SiteWise registros que registra cuándo se crea correctamente un modelo de activos.

```
{
  "eventTime": "2020-05-05T00:10:22.902Z",
  "logLevel": "INFO",
  "eventType": "AssetModelCreationSuccess",
  "message": "Successfully created asset model.",
  "resources": {
    "assetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE"
  }
}
```

Supervisión de los registros de SiteWise Edge Gateway

Puede configurar su puerta de enlace AWS IoT SiteWise Edge para registrar la información en Amazon CloudWatch Logs o en el sistema de archivos local.

Temas

- Uso de Amazon CloudWatch Logs
- Uso de registros de servicio
- Uso de registros de eventos

Uso de Amazon CloudWatch Logs

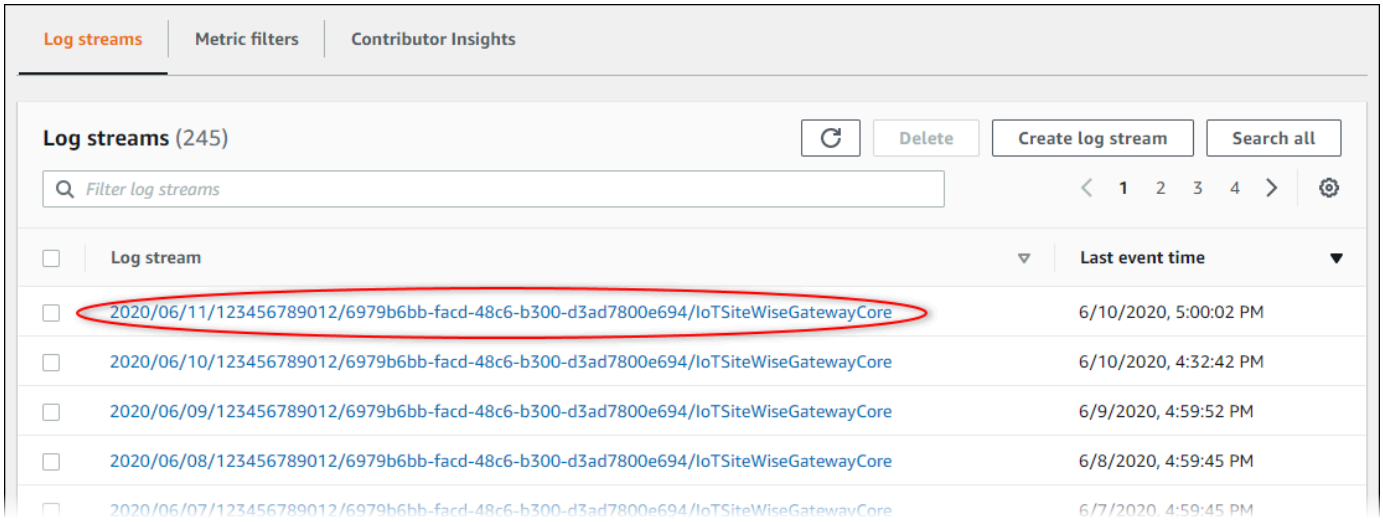
Puede configurar su puerta de enlace SiteWise Edge para enviar CloudWatch registros a Logs. Para obtener más información, consulte Habilitar el registro de CloudWatch registros en la Guía para AWS IoT Greengrass Version 2 desarrolladores.

Para configurar los CloudWatch registros y acceder a ellos (consola)

1. Vaya a la consola de CloudWatch.
2. En el panel de navegación, seleccione Grupos de registro.
3. Puede encontrar los registros de los AWS IoT SiteWise componentes en los siguientes grupos de registros:

   - `/aws/greengrass/UserComponent/region/aws.iot.SiteWiseEdgeCollectorOpcua`— Los registros del componente de la puerta de enlace SiteWise Edge que recopila datos de las fuentes OPC-UA de la puerta de enlace SiteWise Edge.
   - `/aws/greengrass/UserComponent/region/aws.iot.SiteWiseEdgePublisher`— Los registros del componente de la puerta de enlace SiteWise Edge que publica los flujos de datos OPC-UA en. AWS IoT SiteWise

   Elija el grupo de registro de la función que desea depurar.
4. Elija un flujo de registro que tenga un nombre que termine con el nombre de su AWS IoT Greengrass grupo. De forma predeterminada, CloudWatch muestra primero el flujo de registro más reciente.



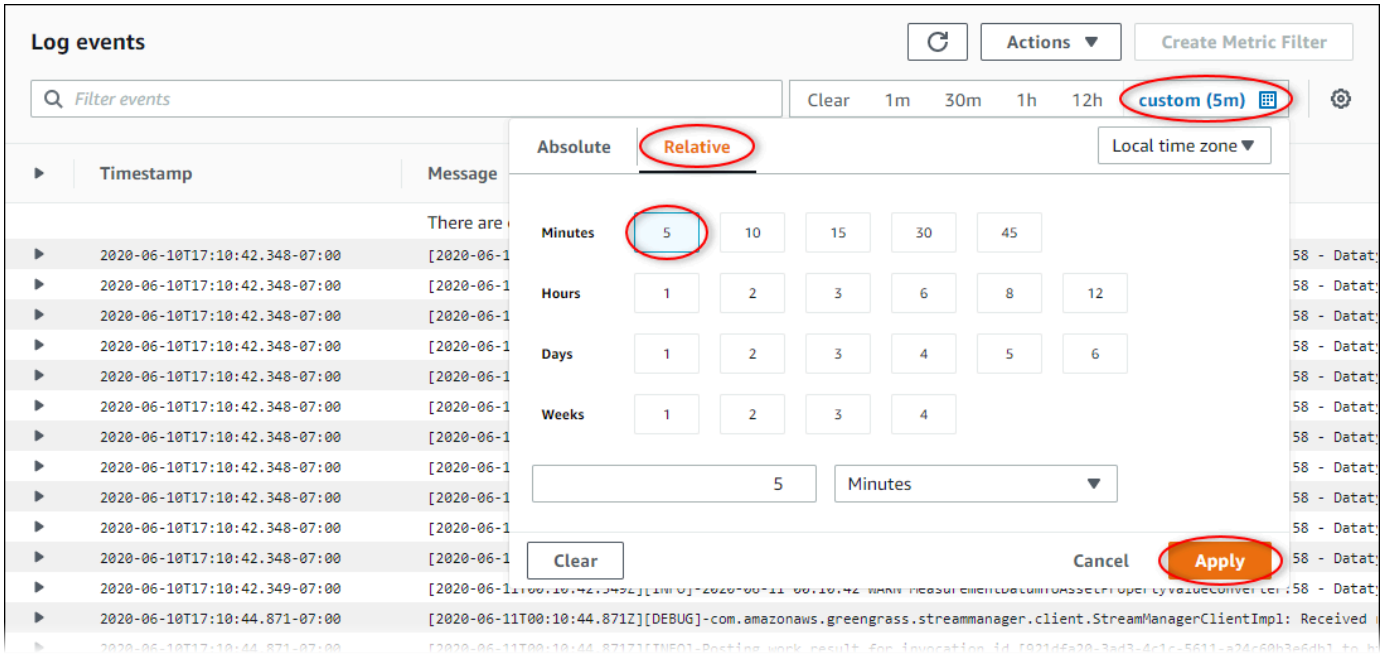
5. Para mostrar los registros de los últimos 5 minutos, haga lo siguiente:

   a. Elija custom (personalizado) en la esquina superior derecha.

   b. Elija Relative (Relativo).

   c. Elija 5 minutos.

   d. Seleccione Aplicar.



6. (Opcional) Para ver menos registros, puede seleccionar 1m (1 minuto) en la esquina superior derecha.

7. Desplácese hasta la parte inferior de las entradas de registro para ver los registros más recientes.

Uso de registros de servicio

SiteWise Los dispositivos Edge Gateway incluyen archivos de registro de servicios para ayudar a solucionar problemas. Las siguientes secciones le ayudarán a encontrar y utilizar los archivos de registro de servicio de los componentes AWS IoT SiteWise OPC-UA Collector y AWS IoT SiteWise Publisher.

AWS IoT SiteWise Archivo de registro del servicio OPC-UA Collector

El componente AWS IoT SiteWise OPC-UA Collector utiliza el siguiente archivo de registro.

Linux

```
/greengrass/v2/logs/aws.iot.SiteWiseEdgeCollectorOpcua.log
```

Windows

```
C:\greengrass\v2\logs\aws.iot.SiteWiseEdgeCollectorOpcua.log
```

Para ver los registros de este componente

- Ejecute el siguiente comando en el dispositivo principal para ver el archivo de registro de este componente en tiempo real. Sustituya */greengrass/v2* o *C:\greengrass\v2* por la ruta a la carpeta AWS IoT Greengrass raíz.

  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 Archivo de registro del servicio de Publisher

El componente AWS IoT SiteWise Publisher utiliza el siguiente archivo de registro.

Linux

```
/greengrass/v2/logs/aws.iot.SiteWiseEdgePublisher.log
```

Windows

```
C:\greengrass\v2\logs\aws.iot.SiteWiseEdgePublisher.log
```

Para ver los registros de este componente

- Ejecute el siguiente comando en el dispositivo principal para ver el archivo de registro de este componente en tiempo real. Sustituya */greengrass/v2* o *C:\greengrass\v2* por la ruta a la carpeta AWS IoT Greengrass raíz.

  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
  ```

Uso de registros de eventos

SiteWise Los dispositivos Edge Gateway incluyen archivos de registro de eventos para ayudar a solucionar problemas. Las siguientes secciones le ayudarán a encontrar y utilizar los archivos de registro de eventos de los componentes AWS IoT SiteWise OPC-UA Collector y AWS IoT SiteWise Publisher.

AWS IoT SiteWise Registros de eventos de OPC-UA Collector

El componente AWS IoT SiteWise OPC-UA Collector incluye un registro de eventos para ayudar a los clientes a identificar y solucionar problemas. El archivo de registro es independiente del archivo de registro local y se encuentra en la siguiente ubicación. Sustituya */greengrass/v2* o *C:\greengrass\v2* por la ruta de acceso a la carpeta AWS IoT Greengrass raíz.

Linux

```
/greengrass/v2/work/aws.iot.SiteWiseEdgeCollectorOpcua/logs/
IotSiteWiseOpcUaCollectorEvents.log
```

Windows

```
C:\greengrass\v2\work\aws.iot.SiteWiseEdgeCollectorOpcua\logs
\IotSiteWiseOpcUaCollectorEvents.log
```

Este registro incluye información detallada e instrucciones de solución de problemas. La información sobre la solución de problemas se proporciona junto con los diagnósticos, con una descripción de cómo solucionar el problema y, a veces, con enlaces a más información. La información de diagnóstico incluye lo siguiente:

- Nivel de gravedad
- Timestamp
- Información adicional específica del evento

Example Registro de ejemplo

```
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 Registros de eventos de Publisher

El componente AWS IoT SiteWise Publisher incluye un registro de eventos para ayudar a los clientes a identificar y solucionar problemas. El archivo de registro es independiente del archivo de registro

local y se encuentra en la siguiente ubicación. Sustituya */greengrass/v2*o *C:\greengrass\v2* por la ruta de acceso a la carpeta AWS IoT Greengrass raíz.

Linux

```
/greengrass/v2/work/aws.iot.SiteWiseEdgePublisher/logs/
IotSiteWisePublisherEvents.log
```

Windows

```
C:\greengrass\v2\work\aws.iot.SiteWiseEdgePublisher\logs
\IotSiteWisePublisherEvents.log
```

Este registro incluye información detallada e instrucciones de solución de problemas. La información sobre la solución de problemas se proporciona junto con los diagnósticos, con una descripción de cómo solucionar el problema y, a veces, con enlaces a más información. La información de diagnóstico incluye lo siguiente:

- Nivel de gravedad
- Timestamp
- Información adicional específica del evento

Example Registro de ejemplo

```
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
```

Monitorización AWS IoT SiteWise con CloudWatch métricas de Amazon

Puede monitorizar el AWS IoT SiteWise uso CloudWatch, que recopila datos sin procesar y los procesa para convertirlos en métricas legibles prácticamente en tiempo real. Estas estadísticas se mantienen durante 15 meses, de forma que pueda obtener acceso a información histórica y disponer de una mejor perspectiva sobre el desempeño de su aplicación web o servicio. También puede establecer alarmas que vigilen determinados umbrales y enviar notificaciones o realizar acciones cuando se cumplan dichos umbrales. Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.

AWS IoT SiteWise publica las métricas y dimensiones que se enumeran en las secciones siguientes en el espacio de `AWS/IoTSiteWise` nombres.

> **Tip**
>
> AWS IoT SiteWise publica las métricas en un intervalo de un minuto. Cuando visualice estas métricas en gráficos en la CloudWatch consola, le recomendamos que elija un período de 1 minuto. Esto le permite ver la resolución más alta disponible de los datos de métrica.

Temas

- AWS IoT Greengrass Version 2 métricas de pasarela
- AWS IoT Greengrass Version 1 métricas de puerta de enlace

AWS IoT Greengrass Version 2 métricas de pasarela

AWS IoT SiteWise publica las siguientes métricas de SiteWise Edge Gateway. Todas las métricas de SiteWise Edge Gateway se publican en un intervalo de un minuto.

SiteWise Métricas de Edge Gateway

Métrica	Descripción
`Gateway.CpuUsage`	El uso de la CPU de una puerta de enlace SiteWise Edge. Unidad: porcentaje Dimensión: None
`Gateway.TotalDiskSpace`	El espacio total en disco de una puerta de enlace SiteWise Edge. Unidades: bytes Dimensión: None
`Gateway.UsedDiskSpace`	El espacio en disco utilizado de una puerta de enlace SiteWise Edge. Unidades: bytes Dimensión: None
`Gateway.AvailableDiskSpace`	El espacio en disco disponible de una puerta de enlace SiteWise Edge. Unidades: bytes Dimensión: None
`Gateway.UsedPercentageDiskSpace`	El porcentaje de espacio en disco utilizado de una puerta de enlace SiteWise Edge. Unidades: bytes

Métrica	Descripción
	Dimensión: None
`Gateway.TotalMemory`	La memoria total de una puerta de enlace SiteWise Edge. Unidades: bytes Dimensión: None
`Gateway.UsedMemory`	La memoria utilizada de una puerta de enlace SiteWise Edge. Unidades: bytes Dimensión: None
`Gateway.AvailableMemory`	La memoria disponible de una puerta de enlace SiteWise Edge. Unidades: bytes Dimensión: None
`Gateway.UsedPercentageMemory`	El porcentaje de memoria utilizado de una puerta de enlace SiteWise Edge. Unidades: bytes Dimensión: None
`Gateway.CloudConnectivity`	El estado de conectividad a la nube de una puerta de enlace SiteWise Edge. Unidad: ninguna Dimensión: GatewayId

Métrica	Descripción
`Gateway.SWE.Component.RunningStatus`	El estado de funcionamiento de los componentes de una puerta de enlace SiteWise Edge. Unidad: ninguna Dimensión: GatewayId

Métricas del recopilador OPC-UA

Métrica	Descripción
`OpcUaCollector.Heartbeat`	Se generan cada minuto para cada fuente OPC-UA (`sourceName`) conectada a una puerta de enlace SiteWise Edge (). `gatewayId` Unidad: recuento (1 representa que la fuente está conectada y 0 representa que la fuente está desconectada). Dimensiones: GatewayId, SourceName
`OpcUaCollector.ActiveDataStreamCount`	El número de flujos de datos a los que se ha suscrito una puerta de enlace SiteWise Edge (`gatewayId`) para una fuente OPC-UA (). `sourceName` Unidad: recuento Dimensiones:,, GatewayId SourceName PropertyGroup
`OpcUaCollector.IncomingValuesCount`	La cantidad de puntos de datos que una puerta de enlace SiteWise Edge (`gatewayId`) recibe para una fuente OPC-UA (`sourceName`), generada cada minuto.

Métrica	Descripción
	Unidad: recuento Dimensiones: GatewayId,, SourceName PropertyGroup
`OpcUaCollector.IncomingValuesError`	El número de puntos de datos que una puerta de enlace SiteWise Edge (`gatewayId`) recibe de una fuente OPC-UA (`sourceName`) que no son valores válidos. El OpcUa recopilador no ingiere estos puntos de datos, sino que se generan cada minuto. Unidad: recuento Dimensiones: GatewayId,, SourceName PropertyGroup
`OpcUaCollector.ConversionErrors`	El número de puntos de datos que una puerta de enlace SiteWise Edge (`gatewayId`) recibió para una fuente OPC-UA (`sourceName`) y que provocaron errores de conversión al enviar los datos. AWS IoT SiteWise Collector no ingerirá estos puntos de datos. OpcUa Unidad: recuento Dimensiones: GatewayId, SourceName

AWS IoT SiteWise métricas del editor

Métrica	Descripción
`IoTSiteWisePublisher.Heartbeat`	Generadas cada minuto por el editor en la puerta de enlace de SiteWise Edge.

Métrica	Descripción
	Unidad: 1 (1 representa que el editor está en ejecución y falta el punto de datos que indica que el editor no está en ejecución). Dimensiones: GatewayId
`IoTSiteWisePublisher.PublishSuccessCount`	La cantidad de puntos de datos que una puerta de enlace SiteWise Edge (`GatewayId `) publicó correctamente en la nube y generó cada minuto. Unidad: recuento Dimensiones: GatewayId
`IoTSiteWisePublisher.PublishFailureCount`	La cantidad de puntos de datos que una puerta de enlace SiteWise Edge (`GatewayId `) no pudo publicar, generada cada minuto. Unidad: recuento Dimensiones: GatewayId
`IoTSiteWisePublisher.PublishRejectedCount`	La cantidad de puntos de datos que una puerta de enlace SiteWise Edge (`GatewayId `) rechazó desde la nube y generó cada minuto. Unidad: recuento Dimensiones: GatewayId
`IoTSiteWisePublisher.DroppedCount`	La cantidad de puntos de datos que se descartan en una puerta de enlace de SiteWise Edge (`GatewayId `) y que no se publican en la nube, generados cada minuto. Unidad: recuento Dimensiones: GatewayId

AWS IoT Greengrass Version 1 métricas de puerta de enlace

AWS IoT SiteWise publica las siguientes métricas de SiteWise Edge Gateway. Todas las métricas de SiteWise Edge Gateway se publican en un intervalo de un minuto.

> **Important**
>
> Para recibir las métricas de la puerta de enlace SiteWise Edge, debe usar al menos la versión 6 del AWS IoT SiteWise conector de la puerta de enlace SiteWise Edge. Para obtener más información, consulte Recopilador de OPC-UA de AWS IoT SiteWise en la Guía para desarrolladores de AWS IoT Greengrass Version 1 .

SiteWise Métricas de Edge Gateway

Métrica	Descripción
`Gateway.Heartbeat`	Se generan cada minuto para cada puerta de enlace SiteWise Edge (`gatewayId`) conectada. Unidad: 1 (1 representa que la puerta de enlace SiteWise Edge está activa y falta el punto de datos que representa que la puerta de enlace SiteWise Edge está desconectada de la nube). Dimensión: GatewayId
`Gateway.PublishSuccessCount`	La cantidad de puntos de datos que una puerta de enlace de SiteWise Edge (`gatewayId`) publicó correctamente. Unidad: recuento Dimensión: GatewayId
`Gateway.PublishFailureCount`	La cantidad de puntos de datos que una puerta de enlace SiteWise Edge (`gatewayId`) no pudo publicar.

Métrica	Descripción
	Esta métrica cuenta los errores que resultan de las llamadas de la puerta de enlace SiteWise Edge a la BatchPutAssetPropertyValueoperación. Para obtener más información sobre la solución de problemas de las puertas de enlace SiteWise Edge, consulteSolución de problemas de una puerta de enlace SiteWise Edge. Unidad: recuento Dimensión: GatewayId
`Gateway.ProcessFailureCount`	La cantidad de puntos de datos que una puerta de enlace SiteWise Edge (`gatewayId`) no pudo procesar. Esta métrica cuenta los errores que se producen entre la puerta de enlace SiteWise Edge y las fuentes de la puerta de enlace SiteWise Edge, incluidos los errores notificados por las fuentes. Para obtener más información sobre la solución de problemas de las puertas de enlace SiteWise Edge, consulteSolución de problemas de una puerta de enlace SiteWise Edge. Unidad: recuento Dimensión: GatewayId

Métrica	Descripción
`Gateway.PublishRejectedCount`	El número de puntos de datos de una puerta de enlace SiteWise Edge (`gatewayId `) que se rechazan. Unidad: recuento Dimensión: GatewayId

Métricas relacionadas con el OPC-UA

Métrica	Descripción
`OPCUACollector.Heartbeat`	Se genera cada minuto para cada fuente OPC-UA (`sourceName `) conectada a una puerta de enlace SiteWise Edge (`gatewayId `). Unidad: recuento (1 representa que la fuente está conectada y 0 representa que la fuente está desconectada). Dimensiones: GatewayId, SourceName
`OPCUACollector.ActiveDataStreamCount`	El número de flujos de datos a los que se ha suscrito una puerta de enlace SiteWise Edge (`gatewayId `) para una fuente OPC-UA (). `sourceName` Unidad: recuento Dimensiones:,, GatewayId SourceName PropertyGroup
`OpcUaCollector.IncomingValuesCount`	La cantidad de puntos de datos que una puerta de enlace SiteWise Edge (`gatewayId `) recibe para una fuente OPC-UA (`sourceName `), generada cada minuto.

Métrica	Descripción
	Unidad: recuento Dimensiones: GatewayId,, SourceName PropertyGroup
`OpcUaCollector.IncomingValuesError`	El número de puntos de datos que una puerta de enlace SiteWise Edge (`gatewayId`) recibió de una fuente OPC-UA (`sourceName`) que no son valores válidos. El OpcUa recopilador no ingerirá estos puntos de datos, ya que se generan cada minuto. Unidad: recuento Dimensiones: GatewayId,, SourceName PropertyGroup
`OpcUaCollector.ConversionErrors`	El número de puntos de datos que una puerta de enlace SiteWise Edge (`gatewayId`) recibió para una fuente OPC-UA (`sourceName`) y que provocaron errores de conversión al enviar los datos. AWS IoT SiteWise Collector no ingerirá estos puntos de datos. OpcUa Unidad: recuento Dimensiones: GatewayId, SourceName

Métricas relacionadas con EIP

Métrica	Descripción
`EIPCollector.Heartbeat`	Se genera cada minuto para cada fuente EIP (`sourceName`) conectada a una puerta de enlace SiteWise Edge (`gatewayId`).

Métrica	Descripción
	Unidad: 1 (1 representa que el origen está conectado y falta el punto de datos que representa que el origen está desconectado). Dimensiones: GatewayId, SourceName
`EIPCollector.IncomingValuesCount`	La cantidad de flujos de datos a los que está suscrita una puerta de enlace SiteWise Edge (`gatewayId`) para una fuente de EIP ()`sourceName` . Unidad: recuento Dimensiones:, GatewayId SourceName
`EIPCollector.ActiveDataStreamCount`	La cantidad de puntos de datos que recibió una puerta de enlace SiteWise Edge (`gatewayId`) para una fuente de EIP (`sourceName`). Unidad: recuento Dimensiones: GatewayId, SourceName

Métricas relacionadas con Modbus

Métrica	Descripción
`ModbusTCPCollector.Heartbeat`	Se genera cada minuto para cada fuente Modbus (`sourceName`) conectada a una puerta de enlace SiteWise Edge (`gatewayId`). Unidad: 1 (1 representa que el origen Modbus está conectado y falta el punto de datos que representa que el origen está desconectado). Dimensiones: GatewayId, SourceName

Métrica	Descripción
`ModbusTCPCollector.IncomingValuesCount`	La cantidad de flujos de datos a los que está suscrita una puerta de enlace SiteWise Edge (`gatewayId`) para una fuente Modbus ()`sourceName` . Unidad: recuento Dimensiones:, GatewayId SourceName
`ModbusTCPCollector.ActiveDataStreamCount`	El número de puntos de datos que recibió una puerta de enlace SiteWise Edge (`gatewayId`) para una fuente Modbus (`sourceName`). Unidad: recuento Dimensiones: GatewayId, SourceName

Registrar llamadas a la AWS IoT SiteWise API con AWS CloudTrail

AWS IoT SiteWise está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en AWS IoT SiteWise. CloudTrail captura las llamadas a la API AWS IoT SiteWise como eventos. Las llamadas capturadas incluyen llamadas desde la AWS IoT SiteWise consola y llamadas en código a las operaciones de la AWS IoT SiteWise API. Si crea una ruta, puede activar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de AWS IoT SiteWise. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por usted CloudTrail, puede determinar el destinatario de la solicitud AWS IoT SiteWise, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales.

Para obtener más información al respecto CloudTrail, consulte la Guía AWS CloudTrail del usuario.

AWS IoT SiteWise información en CloudTrail

CloudTrail se activa en su AWS cuenta al crear la cuenta. Cuando se produce una actividad de eventos admitida AWS IoT SiteWise, esa actividad se registra en un CloudTrail evento junto con

otros eventos de AWS servicio en el historial de eventos. Puedes ver, buscar y descargar los eventos recientes en tu AWS cuenta. Para obtener más información, consulta Cómo ver eventos con el historial de CloudTrail eventos.

Para tener un registro continuo de los eventos de tu AWS cuenta, incluidos los eventos de tu cuenta AWS IoT SiteWise, crea una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando crea una ruta en la consola, la ruta se aplica a todas AWS las regiones. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el elemento userIdentity de CloudTrail .

AWS IoT SiteWise eventos de datos en CloudTrail

Los eventos de datos proporcionan información sobre las operaciones de recursos realizadas en o dentro de un recurso (por ejemplo, leer o escribir en un objeto de Amazon S3). Se denominan también operaciones del plano de datos. Los eventos de datos suelen ser actividades de gran volumen. De forma predeterminada, CloudTrail no registra los eventos de datos. El historial de CloudTrail eventos no registra los eventos de datos.

Se aplican cargos adicionales a los eventos de datos. Para obtener más información sobre CloudTrail los precios, consulta AWS CloudTrail Precios.

Puede registrar eventos de datos para los tipos de AWS IoT SiteWise recursos mediante la CloudTrail consola o las operaciones de la CloudTrail API. AWS CLI La tabla de esta sección muestra los tipos de recursos disponibles para AWS IoT SiteWise.

- Para registrar eventos de datos mediante la CloudTrail consola, cree un almacén de datos de rutas o eventos para registrar eventos de datos, o actualice un banco de datos de seguimiento o evento existente para registrar eventos de datos.

  1. Elija Eventos de datos para registrar los eventos de datos.
  2. En la lista de tipos de eventos de datos, elija el tipo de recurso para el que desea registrar los eventos de datos.
  3. Elija la plantilla de selección de registros que desee utilizar. Puede registrar todos los eventos de datos del tipo de recurso, registrar todos los `readOnly` eventos, registrar todos los `writeOnly` eventos o crear una plantilla de selección de registros personalizada para filtrar `resources.`ARN los campos y. `readOnly` `eventName`

- Para registrar los eventos de datos mediante el AWS CLI, configure el `--advanced-event-selectors` parámetro para que el `eventCategory` campo sea igual al valor del tipo de recurso `Data` y el `resources.type` campo igual al valor del tipo de recurso (consulte la tabla). Puede agregar condiciones para filtrar los valores de los `resources.`ARN campos `readOnly`, `eventName` y.
  - Para configurar una ruta para registrar eventos de datos, ejecute el AWS CloudTrail put-event-selectorscomando. Para obtener más información, consulte Registrar eventos de datos para senderos con la AWS CLI.
  - Para configurar un banco de datos de eventos para registrar eventos de datos, ejecute el AWS CloudTrail create-event-data-storecomando para crear un nuevo banco de datos de eventos para registrar eventos de datos, o ejecute el AWS CloudTrail update-event-data-storecomando para actualizar un banco de datos de eventos existente. Para obtener más información, consulte Registrar eventos de datos para los almacenes de datos de eventos con AWS CLI.

En la siguiente tabla se enumeran los tipos de AWS IoT SiteWise recursos. La columna Tipo de evento de datos (consola) muestra el valor que se puede elegir en la lista de tipos de eventos de datos de la CloudTrail consola. La columna de valores resources.type muestra el `resources.type` valor que se debe especificar al configurar los selectores de eventos avanzados mediante las API

o. AWS CLI CloudTrail La CloudTrail columna API de datos en la que se ha registrado muestra las llamadas a la API registradas CloudTrail para el tipo de recurso.

Tipo de evento de datos (consola)	resources.type value	Las API de datos registradas en CloudTrail *
AWS IoT SiteWise recurso	`AWS::IoTSiteWise::Asset`	• BatchPutAssetPropertyValue • GetAssetPropertyValue • GetAssetPropertyValueHistory • GetAssetPropertyAggregates • GetInterpolatedAssetPropertyValues • BatchGetAssetPropertyValue • BatchGetAssetPropertyValueHistory • BatchGetAssetPropertyAggregates
AWS IoT SiteWise series temporales	`AWS::IoTSiteWise::TimeSeries`	• BatchPutAssetPropertyValue • GetAssetPropertyValue • GetAssetPropertyValueHistory • GetAssetPropertyAggregates • GetInterpolatedAssetPropertyValues • BatchGetAssetPropertyValue

Tipo de evento de datos (consola)	resources.type value	Las API de datos registradas en CloudTrail *
		• BatchGetAssetPropertyValueHistory • BatchGetAssetPropertyAggregates

> **Note**
>
> El tipo de recurso registrado en el evento de Cloudtrail depende del identificador utilizado en la solicitud de API. Si se especifica un identificador de activo en la solicitud, se registra el Asset resources.type y, de lo contrario, se registra el resources.type. TimeSeries

*Puede configurar selectores de eventos avanzados para filtrar los `resources.ARN` campos y registrar solo `eventName` aquellos `readOnly` eventos que sean importantes para usted. Para obtener más información acerca de estos campos, consulte AdvancedFieldSelector.

AWS IoT SiteWise eventos de gestión en CloudTrail

Los eventos de administración proporcionan información sobre las operaciones de administración que se realizan en los recursos de su AWS cuenta. Se denominan también operaciones del plano de control. De forma predeterminada, CloudTrail registra los eventos de administración.

AWS IoT SiteWise registra todas las operaciones del plano de AWS IoT SiteWise control como eventos de administración. Para obtener una lista de las operaciones del plano de AWS IoT SiteWise control en las que se AWS IoT SiteWise registra CloudTrail, consulte la referencia de la AWS IoT SiteWise API.

Ejemplo: entradas de archivos de AWS IoT SiteWise registro

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la operación solicitada, la fecha y la hora de la operación, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un seguimiento ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la `CreateAsset` operación.


```
{
  "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"
}
```

Etiquetar sus recursos AWS IoT SiteWise

El etiquetado de AWS IoT SiteWise los recursos proporciona una forma eficaz de categorizar, gestionar y recuperar los activos de la organización de forma eficiente. Al asignar etiquetas, que consisten en pares clave-valor, puede adjuntar metadatos descriptivos a sus recursos. Los metadatos de las etiquetas se pueden utilizar para agilizar las operaciones. Por ejemplo, en el escenario de un parque eólico, las etiquetas permiten etiquetar las turbinas con atributos específicos, como la ubicación, la capacidad y el estado operativo, lo que permite identificarlas y gestionarlas rápidamente AWS IoT SiteWise.

La integración de las etiquetas en las políticas AWS Identity and Access Management (IAM) mejora la seguridad y el control operativo mediante la definición de reglas de acceso condicional. Esto significa que puede especificar que solo los usuarios tengan determinadas etiquetas. Por ejemplo, solo las personas etiquetadas con un determinado rol o departamento pueden acceder a determinados recursos o modificarlos.

Usar etiquetas en AWS IoT SiteWise

Use etiquetas para clasificar sus AWS IoT SiteWise recursos por propósito, propietario, entorno o cualquier otra clasificación para su caso de uso. Cuando tenga muchos recursos del mismo tipo, podrá identificar rápidamente un recurso específico en función de las etiquetas.

Cada etiqueta se compone de una clave y un valor opcional que usted especifique. Por ejemplo, puede establecer una serie de etiquetas para sus modelos de activos a fin de realizar un seguimiento de los mismos en función de los procesos industriales a los que dan soporte. Se recomienda desarrollar un conjunto personalizado de claves de etiquetas para cada tipo de recurso que gestione. El uso de un conjunto coherente de claves de etiquetas puede facilitar la administración de los recursos.

Etiquetar con AWS Management Console

El editor de etiquetas del AWS Management Console proporciona una forma centralizada y unificada de crear y administrar las etiquetas para los recursos de todos los AWS servicios. Para obtener más información, consulte Tag Editor en la Guía del usuario de AWS Resource Groups .

Etiquetar con la API AWS IoT SiteWise

La AWS IoT SiteWise API también usa etiquetas. Antes de crear etiquetas, tenga en cuenta las restricciones de etiquetado. Para obtener más información, consulte este artículo sobre las convenciones de nomenclatura y el uso de etiquetas en la Referencia general de AWS.

- Para agregar etiquetas al crear un recurso, deberá definirlas en la propiedad `tags` del recurso.
- Para añadir etiquetas a un recurso existente o para actualizar los valores de las etiquetas, utilice la TagResourceoperación.
- Para eliminar etiquetas de un recurso, utilice la UntagResourceoperación.
- Para recuperar las etiquetas asociadas a un recurso, utilice la ListTagsForResourceoperación o describa el recurso e inspeccione su `tags` propiedad.

En la siguiente tabla, se enumeran los recursos que puedes etiquetar mediante la AWS IoT SiteWise API `Create` y sus `Describe` operaciones correspondientes.

Recursos etiquetables AWS IoT SiteWise

Recurso	Crear operación	Describir operación
Modelo de activos o modelo de componentes	CreateAssetModel	DescribeAssetModel
activo	CreateAsset	DescribeAsset
SiteWise Puerta de enlace Edge	CreateGateway	DescribeGateway
Portal	CreatePortal	DescribePortal
Proyecto	CreateProject	DescribeProject
Panel de control	CreateDashboard	DescribeDashboard
Política de acceso	CreateAccessPolicy	DescribeAccessPolicy
Serie temporal	BatchPutAssetPropertyValue	DescribeTimeSeries

Por `BatchPutAssetPropertyValue` ejemplo, puede configurar sus fuentes de datos para enviar datos industriales AWS IoT SiteWise antes de crear modelos y activos de activos. AWS IoT SiteWise crea automáticamente flujos de datos para recibir flujos de datos sin procesar de su equipo. Para obtener más información, consulte Administración de la ingesta de datos.

Utilice las siguientes operaciones para ver y administrar etiquetas para los recursos que admiten etiquetas:

- TagResource— Añade etiquetas a un recurso o actualiza el valor de una etiqueta existente.
- ListTagsForResource— Muestra las etiquetas de un recurso.
- UntagResource— Elimina las etiquetas de un recurso.

Añade o elimina etiquetas de un recurso en cualquier momento. Para actualizar el valor de una clave de etiqueta existente, añada una nueva etiqueta con la misma clave y el nuevo valor que desee al recurso. Esta acción reemplaza el valor anterior por el nuevo. Si bien es posible asignar una cadena vacía como valor de etiqueta, no se puede asignar un valor nulo.

Al eliminar un recurso, también se eliminan todas las etiquetas vinculadas a él.

Uso de etiquetas con políticas de IAM

Utilice etiquetas de recursos en sus políticas de IAM para controlar el acceso y los permisos de los usuarios. Por ejemplo, las políticas pueden permitir a los usuarios crear únicamente recursos que tengan una etiqueta específica adjunta. Las políticas también puede limitar la creación o modificación de recursos que tengan determinadas etiquetas por parte de los usuarios.

> **Note**
>
> Si utiliza etiquetas para permitir o denegar el acceso de los usuarios a los recursos, debe denegar a los usuarios la capacidad de agregar o eliminar esas etiquetas para los mismos recursos. De lo contrario, un usuario podría eludir tus restricciones y obtener acceso a un recurso modificando sus etiquetas.

Puede utilizar los siguientes valores y claves de contexto de condición en el elemento `Condition` (también llamado bloque `Condition`) de una instrucción de política.

`aws:ResourceTag/tag-key: tag-value`

Permitir o denegar acciones en recursos con etiquetas específicas.

`aws:RequestTag/tag-key: tag-value`

Exigir que se utilice (o no se utilice) una etiqueta específica al crear o modificar un recurso etiquetable.

`aws:TagKeys: [tag-key, ...]`

Exigir que se utilice (o no se utilice) un conjunto específico de claves de etiqueta al crear o modificar un recurso etiquetable.

> **Note**
>
> Las claves y valores de contexto de condición en una política de IAM se aplican solo a las acciones que tienen un recurso etiquetable como parámetro requerido. Por ejemplo, puede configurar el acceso condicional basado en etiquetas para ListAssets. No puedes activar el acceso condicional basado en etiquetas PutLoggingOptionsporque en la solicitud no se hace referencia a ningún recurso etiquetable.

Para obtener más información, consulte Controlar el acceso a AWS los recursos mediante etiquetas de recursos y la referencia a la política JSON de IAM en la Guía del usuario de IAM.

Ejemplo de políticas de IAM que utilizan etiquetas

- Visualización de los activos de AWS IoT SiteWise basados en etiquetas

Solución de problemas AWS IoT SiteWise

Utilice la información de estas secciones para solucionar y resolver problemas con AWS IoT SiteWise.

Temas

Solución de problemas de operaciones de importación y exportación masivas

Para gestionar y diagnosticar los errores producidos durante un trabajo de transferencia, consulta la AWS IoT TwinMaker GetMetadataTransferJobAPI:

1. Tras crear y ejecutar un trabajo de transferencia, llama a la GetMetadataTransferJobAPI:

```
aws iottwinmaker get-metadata-transfer-job \
--metadata-transfer-job-id your_metadata_transfer_job_id \
--region us-east-1
```

2. El estado del trabajo cambia a uno de los siguientes estados:
   - COMPLETED
   - CANCELLED
   - ERROR
3. La GetMetadataTransferJobAPI devuelve un MetadataTransferJobProgressobjeto.
4. El MetadataTransferJobProgressobjeto contiene los siguientes parámetros:
   - FailedCount: indica el recuento de activos que fallaron durante el proceso de transferencia.
   - Número omitido: indica el recuento de activos que se omitieron durante el proceso de transferencia.

- Recuento exitoso: indica el recuento de activos que se realizaron correctamente durante el proceso de transferencia.
- Recuento total: indica el recuento total de activos involucrados en el proceso de transferencia.

5. Además, la llamada a la API devuelve un elemento ReportURL, que contiene una URL prefirmada. Si tu trabajo de transferencia contiene errores que deban investigarse, puedes descargar un informe de errores completo en esta URL.

Solución de problemas de un AWS IoT SiteWise portal

Solucione los problemas habituales de sus AWS IoT SiteWise portales.

Los usuarios y administradores no pueden acceder al portal de AWS IoT SiteWise

Si los usuarios o los administradores no pueden acceder a su AWS IoT SiteWise portal, es posible que tenga permisos restringidos en las políticas adjuntas AWS Identity and Access Management (IAM) que impiden iniciar sesión correctamente.

Consulte los siguientes ejemplos de políticas de IAM que provocan errores de inicio de sesión:

> **Note**
>
> Cualquier política de IAM asociada que incluya un elemento `"Condition"` provoca un error de inicio de sesión.

Ejemplo 1: La condición aquí es una IP limitada, lo cual causa un fallo de inicio de sesión.

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

```
                "IpAddress": {
                    "aws:SourceIp": [
                        "REPLACESAMPLEIP"
                    ]
                }
            }
        }
    ]
}
```

Ejemplo 2: La condición aquí es una etiqueta incluida, lo cual causa un fallo de inicio de sesión.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iotsitewise:DescribePortal"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/project": "*"
                }
            }
        }
    ]
}
```

Al añadir usuarios o administradores al portal, evite crear políticas de IAM que restrinjan los permisos de los usuarios, como IP limitada. Las políticas adjuntas con permisos restringidos no podrán conectarse al AWS IoT SiteWise portal.

Solución de problemas de una puerta de enlace SiteWise Edge

AWS IoT SiteWise Las pasarelas Edge ejecutan un conjunto de componentes. AWS IoT Greengrass Puede configurar su puerta de enlace SiteWise Edge para registrar los eventos de los conectores en Amazon CloudWatch y en el sistema de archivos local de su puerta de enlace SiteWise Edge. A continuación, puede ver los archivos de registro asociados al conector para solucionar los problemas de su puerta de enlace SiteWise Edge.

También puede ver CloudWatch las métricas reportadas por sus puertas de enlace SiteWise Edge para solucionar problemas de conectividad o flujos de datos. Para obtener más información, consulte AWS IoT Greengrass Version 1 métricas de puerta de enlace.

Temas

- Configuración y acceso a los registros de la puerta de SiteWise enlace Edge
- Solución de problemas con la puerta de enlace SiteWise Edge
- Solución de problemas AWS IoT Greengrass

Configuración y acceso a los registros de la puerta de SiteWise enlace Edge

Para poder ver los registros de SiteWise Edge Gateway, debe configurar su puerta de enlace SiteWise Edge para que envíe los registros a Amazon CloudWatch Logs o almacene los registros en el sistema de archivos local.

- Utilice CloudWatch los registros si quiere usarlos AWS Management Console para ver los archivos de registro de su puerta de enlace SiteWise Edge. Para obtener más información, consulte Uso de Amazon CloudWatch Logs.
- Use los registros del sistema de archivos local si quiere usar la línea de comandos o el software local para ver los archivos de registro de su puerta de enlace SiteWise Edge. Para obtener más información, consulte Uso de registros de servicio.

Solución de problemas con la puerta de enlace SiteWise Edge

Utilice la siguiente información para solucionar los problemas de la puerta de enlace SiteWise Edge.

Problemas

- No se han podido implementar paquetes en las puertas de enlace de SiteWise Edge
- Las fuentes Modbus TCP no están sincronizadas
- No es posible conectarse con el administrador de flujos
- No es posible conectarse a una fuente OPC-UA
- AWS IoT SiteWise no recibe datos de los servidores OPC-UA
- No se muestran datos en el panel de control

- En aws.iot aparece el mensaje «No se pudo encontrar ni cargar la clase principal». SiteWiseEdgePublisher registra un error en /greengrass/v2/logs

No se han podido implementar paquetes en las puertas de enlace de SiteWise Edge

Si el componente AWS IoT Greengrass núcleo (`aws.greengrass.Nucleus`) está desactualizado, es posible que no pueda implementar paquetes en su puerta de enlace SiteWise Edge. Puede usar la AWS IoT Greengrass V2 consola para actualizar el componente AWS IoT Greengrass Nucleo.

Actualice el componente AWS IoT Greengrass Nucleus (consola)

1. Vaya a la consola de AWS IoT Greengrass.
2. En el panel de navegación, en AWS IoT Greengrass, seleccione Implementaciones.
3. En la lista Implementaciones, seleccione la implementación que desee revisar.
4. Seleccione Revisar.
5. En la página Especificar destino, seleccione Siguiente.
6. En la página Seleccionar componentes, en Componentes públicos, en el cuadro de búsqueda, introduzca **`aws.greengrass.Nucleus`** y, a continuación, seleccione aws.greengrass.Nucleus.
7. Seleccione Siguiente.
8. En la página Configurar componentes, seleccione Siguiente.
9. En la página Configurar opciones avanzadas, seleccione Siguiente.
10. En la página Revisar, elija Implementar.

Las fuentes Modbus TCP no están sincronizadas

Es posible que su fuente Modbus TCP no esté sincronizada si su tipo de datos de origen es ASCII, UTF8 o ISO8859 y está ejecutando una versión antigua del conector Modbus-TCP Protocol Adapter. Para actualizar el conector a la última versión, haga lo siguiente:

1. Inicie sesión en la consola de AWS IoT Greengrass V1.
2. En el panel de navegación, elija Grupos.
3. En Grupos de AWS IoT Greengrass , elija el grupo deseado.
4. En el panel de navegación, elija Conectores.
5. En la columna Actualizar, elija Disponible.
6. En la página Actualizar conector, elija la última versión y, a continuación, Actualizar.

Para obtener más información, consulte Conector Modbus-TCP Protocol Adapter en la Guía para desarrolladores de AWS IoT Greengrass Version 1 .

No es posible conectarse con el administrador de flujos

Es posible que aparezca el siguiente mensaje de registro de `swPublisher` errores si el administrador de transmisiones no está habilitado en el AWS IoT Greengrass grupo de la puerta de enlace SiteWise Edge.

```
com.amazonaws.greengrass.streammanager.client.StreamManagerClientImpl: Connect failed
```

A partir de la versión 6, el AWS IoT SiteWise conector requiere un administrador de transmisiones. Para obtener más información sobre cómo habilitar el administrador de flujos, consulte el paso 5 de Configuración de un grupo AWS IoT Greengrass.

No es posible conectarse a una fuente OPC-UA

Es posible que vea el siguiente mensaje del registro de errores de `OPCUACollector` si la versión del OpenJDK instalado no es compatible.

```
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
```

Para pasar a una versión anterior compatible de OpenJDK, siga los pasos que se indican en esta sección. En estos pasos se asume que utiliza un dispositivo con Ubuntu. Si utiliza una distribución de Linux diferente, consulte la documentación correspondiente a su dispositivo.

Para pasar a una versión anterior compatible de Amazon Corretto 8

1. Para desinstalar el OpenJDK actual, ejecute uno de los siguientes comandos.
   - ```
     sudo apt purge -y openjdk-8-jre-headless
     ```
   - ```
     sudo apt-get purge -y java-1.8.0-amazon-corretto-jdk
     ```
2. Para descargar e instalar el Amazon Corretto 8 compatible, ejecute el siguiente comando.

```
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. Para reiniciar el software AWS IoT Greengrass V1 Core, ejecute el siguiente comando.

```
sudo /greengrass/ggc/core/greengrassd restart
```

AWS IoT SiteWise no recibe datos de los servidores OPC-UA

Si tus AWS IoT SiteWise activos no reciben los datos enviados por tus servidores OPC-UA, puedes buscar en los registros de la puerta de enlace SiteWise Edge para solucionar problemas. Busque registros de `swPublisher` a nivel de información que contengan el siguiente mensaje.

```
Emitting diagnostic name=PublishError.SomeException
```

Según el tipo de registro, utiliza *`SomeException`*los siguientes tipos de excepciones y los problemas correspondientes para solucionar los problemas de tu puerta de enlace Edge: SiteWise

- ResourceNotFoundException— Sus servidores OPC-UA envían datos que no coinciden con el alias de propiedad de ningún activo. Esta excepción puede ocurrir en dos casos:
  - Sus alias de propiedad no coinciden exactamente con sus variables OPC-UA, incluido cualquier prefijo de origen que haya definido. Compruebe que los alias de propiedad y los prefijos de origen son correctos.
  - No ha asignado las variables OPC-UA a las propiedades de los activos. Para obtener más información, consulte Asignación de flujos de datos industriales a propiedades de activos.

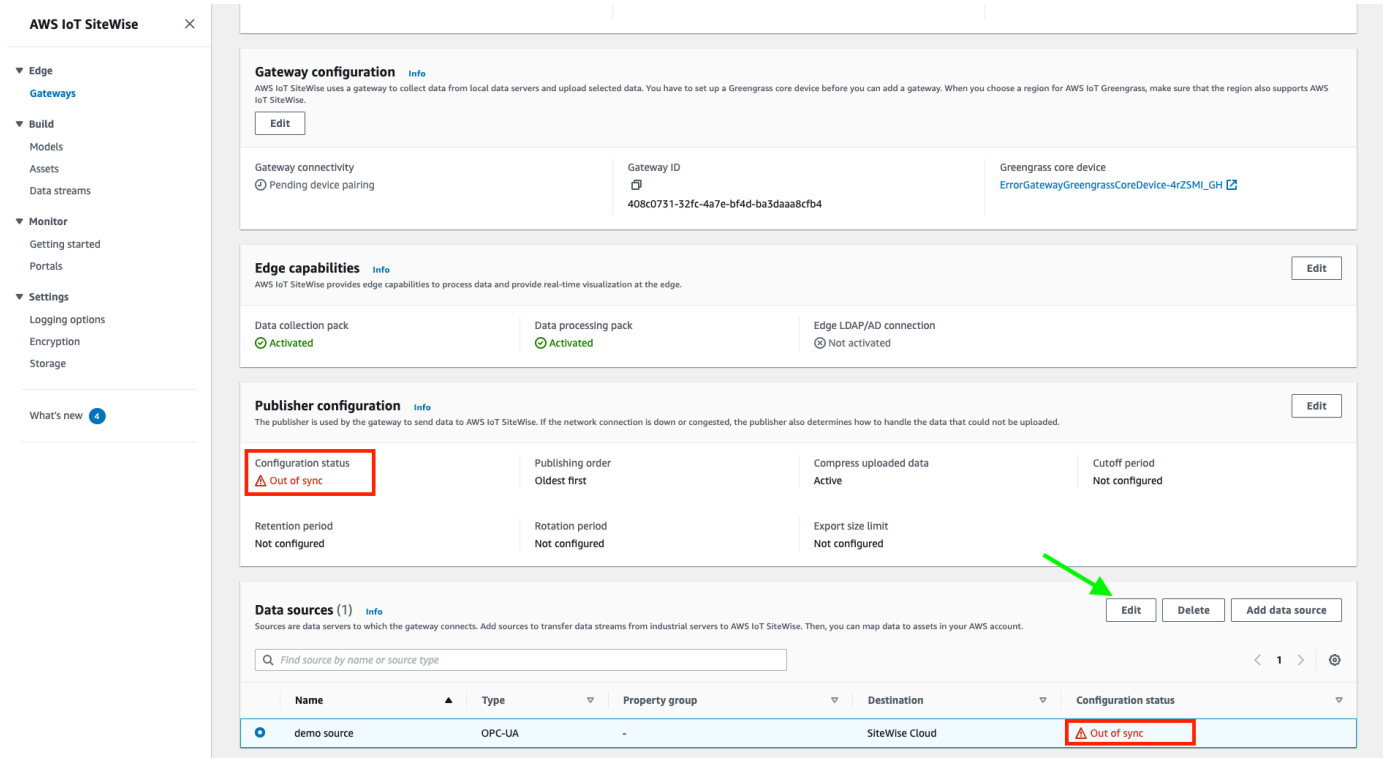
    Si ya ha mapeado todas las variables de OPC-UA que desea incluir AWS IoT SiteWise, puede filtrar las variables de OPC-UA que envía la puerta de enlace Edge. SiteWise Para obtener más información, consulte Uso de filtros de nodos OPC-UA.
- AccessDeniedException— El AWS IoT Greengrass grupo de su puerta de enlace SiteWise Edge no tiene permisos suficientes para usar la BatchPutAssetPropertyValueoperación y enviar datos a las propiedades de los activos. Para obtener más información, consulte Requisitos del conector de AWS IoT SiteWise.

- InvalidRequestException— Los tipos de datos de las variables OPC-UA no coinciden con los tipos de datos de las propiedades de los activos. Por ejemplo, si una variable de OPC-UA tiene un tipo de datos entero, la propiedad de activo correspondiente debe ser del tipo de datos entero. Una propiedad de activo de tipo doble no puede recibir valores OPC-UA enteros. Para solucionar este problema, defina nuevas propiedades con los tipos de datos correctos.
- TimestampOutOfRangeException— Su puerta de enlace SiteWise Edge envía datos que están fuera del rango que AWS IoT SiteWise acepta. AWS IoT SiteWise rechaza todos los puntos de datos con marcas de tiempo anteriores a 7 días o posteriores a 5 minutos en el futuro. Si la puerta de enlace SiteWise Edge se ha quedado sin alimentación o sin conexión a la AWS nube, es posible que tengas que borrar la memoria caché de la puerta de enlace SiteWise Edge.
- ThrottlingExceptiono bien LimitExceededException: tu solicitud superó una cuota de AWS IoT SiteWise servicio, como la tasa de puntos de datos ingeridos o la tasa de solicitudes de operaciones de la API de datos sobre propiedades de activos. Compruebe que su configuración no exceda el AWS IoT SiteWise cuotas.

No se muestran datos en el panel de control

Si no se muestran datos en su panel de control, compruebe en la consola de AWS IoT SiteWise si Configuración del publicador y Origen de datos no están sincronizados. Para solucionar este problema, utilice el siguiente método:

1. Inicie sesión en la consola de AWS IoT SiteWise.
2. En la sección Periferia, abra la sección Puertas de enlace.
3. En Origen de datos, seleccione Editar.



4. Seleccione un nuevo Nombre de origen y, a continuación, Guardar para confirmar el cambio.
5. Verifique sus cambios confirmando que el nombre del origen de datos se haya actualizado en la tabla Orígenes de datos.

Cambiar el nombre del origen de datos podría acelerar la sincronización desde la nube a la periferia y solucionar el error Asincronía.

En aws.iot aparece el mensaje «No se pudo encontrar ni cargar la clase principal». SiteWiseEdgePublisher registra un error en /greengrass/v2/logs

Si aparece este error, es posible que deba actualizar la versión java de su puerta de enlace Edge. SiteWise

- En un terminal, ejecute el comando siguiente:

```
java -version
```

  La versión de Java con la que se ejecuta su puerta de enlace SiteWise Edge aparecerá en`OpenJDK Runtime Environment`. Verá una respuesta como la siguiente:

```
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)
```

Si ejecuta la versión 11.0.20.8.1 de Java, debe actualizar el paquete IoT SiteWise Publisher a la versión 2.4.1 o posterior. Solo se ve afectada la versión 11.0.20.8.1 de Java. Los entornos con otras versiones de Java pueden seguir utilizando versiones anteriores del componente IoT SiteWise Publisher. Para obtener más información sobre la actualización de un paquete de componentes, consulte Cambiar la versión de los paquetes de componentes de SiteWise Edge Gateway.

Solución de problemas AWS IoT Greengrass

Para encontrar soluciones a muchos problemas al configurar o implementar tu puerta de enlace SiteWise Edge AWS IoT Greengrass, consulta Solución de problemas AWS IoT Greengrass en la Guía para AWS IoT Greengrass desarrolladores.

Solución de problemas y acción de AWS IoT SiteWise regla

Para solucionar problemas relacionados con AWS IoT SiteWise la acción de la regla AWS IoT Core, puede realizar uno de los siguientes procedimientos:

- Configurar Amazon CloudWatch Logs
- Configuración de una acción de error de republicación de su regla

A continuación, compare los mensajes de error con los errores de este tema para solucionar el problema.

Temas

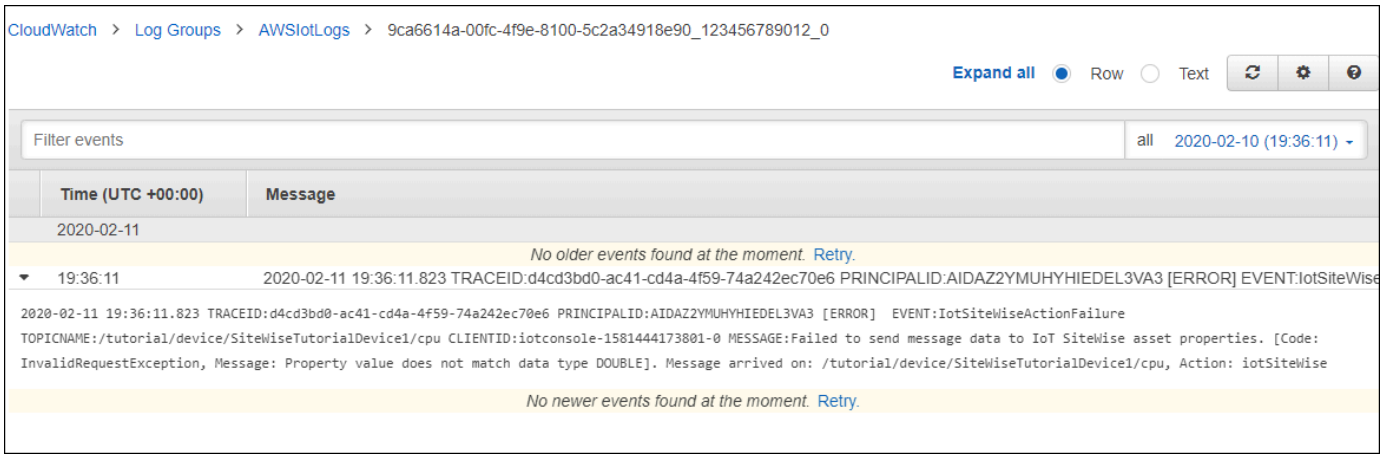
- Configuración de AWS IoT Core registros
- Configuración de una acción de error de republicar
- Solución de problemas con
- Solución de problemas de las reglas
- Solución de problemas de las reglas

Configuración de AWS IoT Core registros

Puede configurarlo AWS IoT para registrar varios niveles de información en los CloudWatch registros.

Para configurar los CloudWatch registros y acceder a ellos

1. Para configurar el registro AWS IoT Core, consulte Supervisión con CloudWatch registros en la Guía para AWS IoT desarrolladores.
2. Vaya a la consola de CloudWatch .
3. En el panel de navegación, seleccione Grupos de registro.
4. Elija el AWSIotLogsgrupo.
5. Elija una secuencia de registro reciente. De forma predeterminada, CloudWatch muestra primero el flujo de registro más reciente.
6. Elija una entrada de registro para expandir el mensaje de registro. Su entrada de registro podría parecerse a la siguiente captura de pantalla.



7. Compare los mensajes de error con los errores de este tema para solucionar el problema.

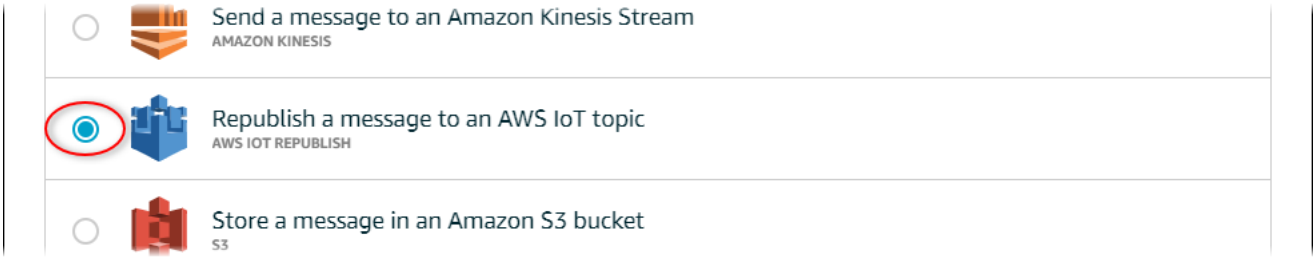
Configuración de una acción de error de republicar

Puede configurar una acción de error en la regla para controlar los mensajes de error. En este procedimiento, configure la acción de la regla Republicar como una acción de error para ver los mensajes de error en el cliente de prueba de MQTT.

> **Note**
>
> La acción de error de republicar genera solo el equivalente de los registros de nivel ERROR. Si desea registros más detallados, debe configurar CloudWatch los registros.

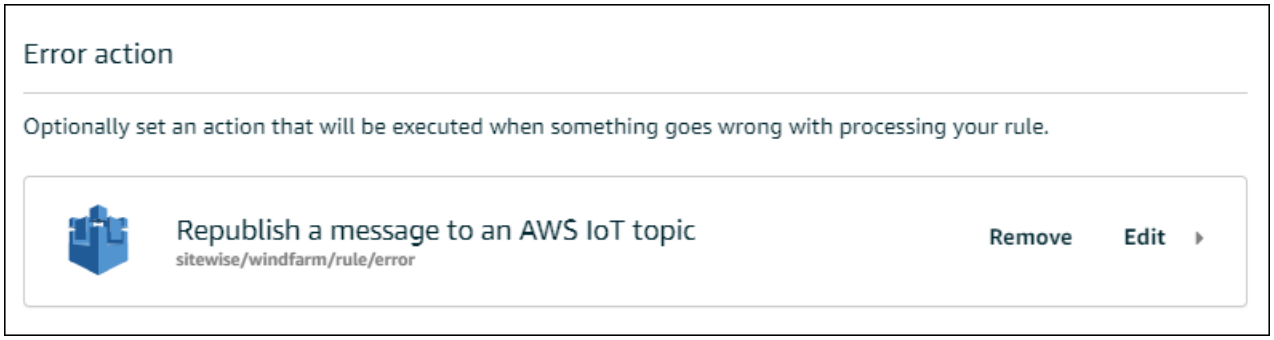
Para añadir una acción de error de republicar a una regla

1. Vaya a la consola de AWS IoT.
2. En el panel de navegación izquierdo, elija Act (Acción) y, a continuación, elija Rules (Reglas).
3. Elija su regla.
4. En Error action (Acción de error), elija Add action (Agregar acción).
5. Elige Volver a publicar un mensaje en un tema. AWS IoT



6. Seleccione Configure action (Configurar acción) en la parte inferior de la página.
7. En Tema, introduce un tema único (por ejemplo,**`sitewise/windfarm/rule/error`**). AWS IoT Core volverá a publicar los mensajes de error relacionados con este tema.
8. Elija Seleccionar para conceder AWS IoT Core acceso y realizar la acción de error.
9. Elija Select (Seleccionar) junto al rol creado para la regla.
10. Elija Update role (Actualizar rol) para añadir los permisos adicionales al rol.
11. Seleccione Agregar acción.

La acción de error de la regla debería ser similar a la siguiente captura de pantalla.



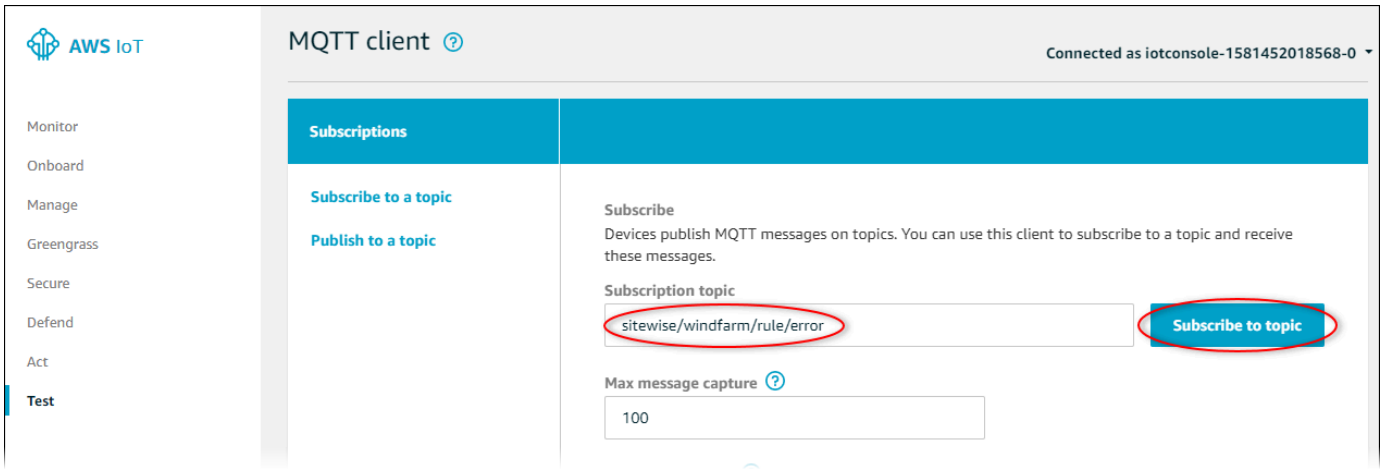
12. Selecciona la flecha hacia atrás situada en la esquina superior izquierda de la consola para volver a la página de inicio de la AWS IoT consola.

Después de configurar la acción de error de Republish (Volver a publicar), puede ver los mensajes de error en el cliente de prueba de MQTT en AWS IoT Core.

En el siguiente procedimiento, se suscribe al tema de error en el cliente de prueba de MQTT. En el cliente de prueba de MQTT, puede recibir mensajes de error de su regla para solucionar el problema.

Para suscribirse al tema de acción de error

1. Vaya a la consola de AWS IoT.
2. En la página de navegación izquierda, elija Test (Pruebas) para abrir el cliente de pruebas de MQTT.
3. En el campo Subscription topic (Tema de suscripción), escriba el tema de error que configuró anteriormente (por ejemplo, **`sitewise/windfarm/rule/error`**) y elija Subscribe to topic (Suscribirse al tema).



4. Observe si aparecen mensajes de error y, a continuación, expanda la matriz `failures` en cualquier mensaje de error.

   A continuación, compare los mensajes de error con los errores de este tema para solucionar el problema.

Solución de problemas con

Utilice la siguiente información para solucionar problemas de reglas.

Problemas

- Error: el miembro debe estar dentro de los 604800 segundos antes y 300 segundos después de la marca de tiempo actual
- Error: el valor de la propiedad no coincide con el tipo de datos <type>
- Error: Usuario: <role-arn>no está autorizado a realizar: iotsitewise: on resource BatchPutAssetPropertyValue
- Error: iot.amazonaws.com no puede funcionar: sts: on resource: AssumeRole <role-arn>
- Información: no se han enviado solicitudes. PutAssetPropertyValueEntries estaba vacío después de realizar la sustitución de plantillas.

Error: el miembro debe estar dentro de los 604800 segundos antes y 300 segundos después de la marca de tiempo actual

Su marca de tiempo es anterior a 7 días o posterior a 5 minutos, en comparación con la hora epoch de Unix. Pruebe lo siguiente:

- Verifique que la marca de tiempo esté en formato de tiempo de Unix (UTC). Si proporciona una marca temporal con una zona horaria diferente, recibirá este error.
- Comprueba que la marca de tiempo esté en segundos. AWS IoT SiteWise espera que las marcas de tiempo se dividan en tiempo en segundos (en el tiempo de época de Unix) y compensadas en nanosegundos.
- Compruebe que está cargando datos cuya fecha no sea anterior a 7 días.

Error: el valor de la propiedad no coincide con el tipo de datos <type>

Una entrada de la acción de regla tiene un tipo de datos diferente al de la propiedad del activo de destino. Por ejemplo, la propiedad del activo de destino es una `DOUBLE` y el tipo de datos seleccionado es Integer (Entero) o ha transferido el valor en `integerValue`. Pruebe lo siguiente:

- Si configura la regla desde la AWS IoT consola, compruebe que ha elegido el tipo de datos correcto para cada entrada.
- Si configuras la regla desde la API o AWS Command Line Interface (AWS CLI), comprueba que tu `value` objeto utilice el campo de tipo correcto (por ejemplo, `doubleValue` para una `DOUBLE` propiedad).

Error: Usuario: <role-arn>no está autorizado a realizar: iotsitewise: on resource BatchPutAssetPropertyValue

La regla no está autorizada a acceder a la propiedad del activo de destino o la propiedad del activo de destino no existe. Pruebe lo siguiente:

- Compruebe que su alias de propiedad es correcto y que tiene una propiedad de activo con el alias de propiedad dado. Para obtener más información, consulte Asignación de flujos de datos industriales a propiedades de activos.
- Compruebe que la regla tiene un rol y que el rol permite los permisos `iotsitewise:BatchPutAssetPropertyValue` a la propiedad del activo de destino, por ejemplo, a través de la jerarquía del activo de destino. Para obtener más información, consulte Otorgar AWS IoT el acceso requerido.

Error: iot.amazonaws.com no puede funcionar: sts: on resource: AssumeRole <role-arn>

Tu usuario no está autorizado a asumir la función que figura en tu regla en (IAM). AWS Identity and Access Management

Compruebe que su usuario tenga permiso `iam:PassRole` para asumir el rol en su regla. Para obtener más información, consulte Permisos de pase de roles en la Guía para desarrolladores de AWS IoT .

Información: no se han enviado solicitudes. PutAssetPropertyValueEntries estaba vacío después de realizar la sustitución de plantillas.

> **Note**
>
> Este mensaje es un registro de nivel `INFO`.

Su solicitud debe tener como mínimo una entrada con todos los parámetros requeridos.

Compruebe que los parámetros de la regla, incluidas las plantillas de sustitución, den como resultado valores no vacíos. Las plantillas de sustitución no pueden acceder a los valores definidos en las cláusulas `AS` de la instrucción de consulta de la regla. Para obtener más información, consulte Plantillas de sustitución en la Guía para desarrolladores de AWS IoT .

Solución de problemas de las reglas

Siga los pasos de este procedimiento para solucionar los problemas de la regla si los datos de uso de la CPU y la memoria no aparecen AWS IoT SiteWise como se esperaba. En este procedimiento, configure la acción de la regla Republicar como una acción de error para ver los mensajes de error en el cliente de prueba de MQTT. También puedes configurar el registro en los CloudWatch registros para solucionar los problemas. Para obtener más información, consulte Solución de problemas y acción de AWS IoT SiteWise regla.

Para añadir una acción de error de republicar a una regla

1. Vaya a la consola de AWS IoT.
2. En el panel de navegación de la izquierda, elija Redirección de mensajes y, a continuación, seleccione Reglas.
3. Elija la regla que creó anteriormente y elija Editar.
4. En Acción de error opcional, elija Agregar acción de error.
5. Selecciona Volver a publicar un mensaje en un AWS IoT tema.
6. En Tema, introduce la ruta del error (por ejemplo,**`sitewise/rule/tutorial/error`**). AWS IoT Core volverá a publicar los mensajes de error relacionados con este tema.
7. Elija el rol que creó anteriormente (por ejemplo, SiteWiseTutorialDeviceRuleRole).
8. Elija Actualizar.

Después de configurar la acción de error de Republish (Volver a publicar), puede ver los mensajes de error en el cliente de prueba de MQTT en AWS IoT Core.

En el siguiente procedimiento, se suscribe al tema de error en el cliente de prueba de MQTT.

Para suscribirse al tema de acción de error

1. Vaya a la consola de AWS IoT.
2. En la página de navegación izquierda, elija cliente de pruebas de MQTT para abrir el cliente de pruebas de MQTT.
3. En el campo Filtro por temas, introduzca **`sitewise/rule/tutorial/error`** y seleccione Suscribirse.

Cuando aparecen mensajes de error, vea la matriz `failures` en cualquier mensaje de error para diagnosticar problemas. Para obtener más información acerca de posibles problemas y cómo resolverlos, consulte Solución de problemas y acción de AWS IoT SiteWise regla.

Si no aparecen errores, compruebe que la regla esté habilitada y que se suscribió al mismo tema que configuró en la acción de error de Republish. Si los errores siguen sin aparecer después de hacerlo, compruebe que el script del dispositivo se esté ejecutando y actualizando correctamente la sombra del dispositivo.

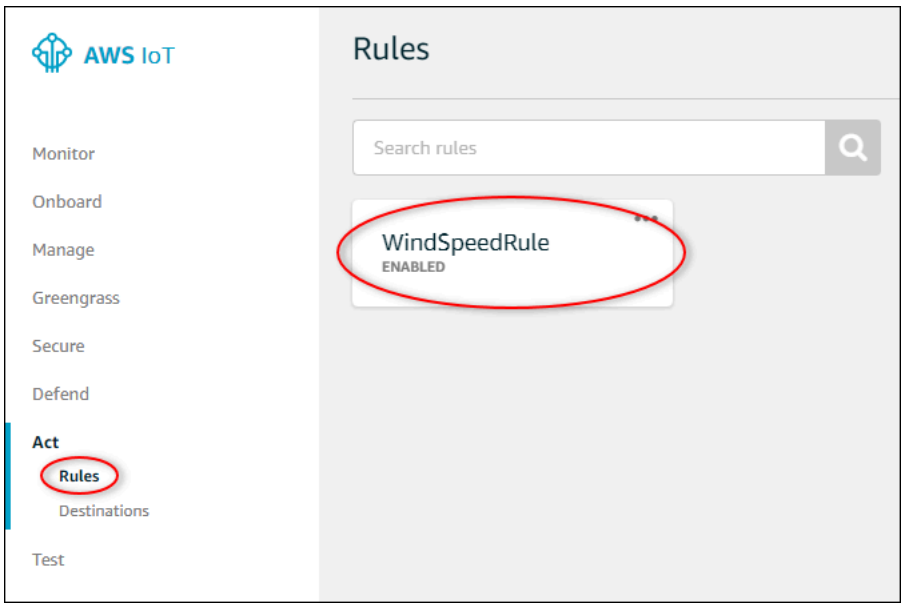
> **Note**
>
> También puedes suscribirte al tema de actualizaciones alternativas de tu dispositivo para ver la carga útil que analiza tu AWS IoT SiteWise acción. Para ello, suscríbase al siguiente tema.
>
> ```
> $aws/things/+/shadow/update/accepted
> ```

Solución de problemas de las reglas

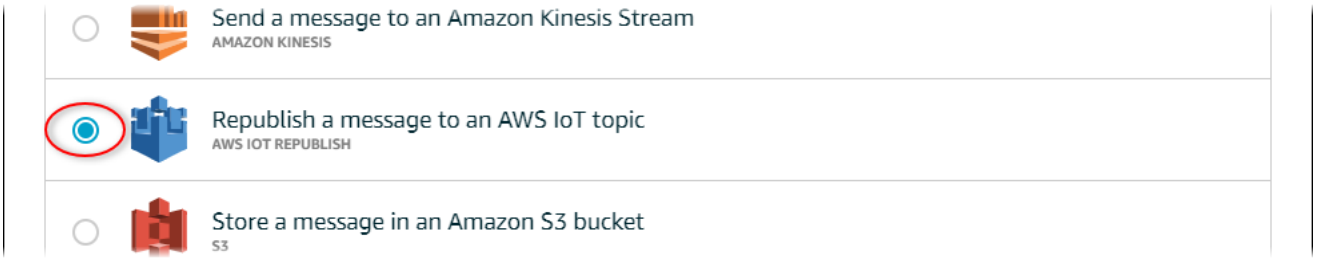
Siga los pasos de este procedimiento para solucionar problemas de la regla si los datos de activos de demostración no aparecen en la tabla de DynamoDB como se esperaba. En este procedimiento, configure la acción de la regla Republicar como una acción de error para ver los mensajes de error en el cliente de prueba de MQTT. También puede configurar el registro en CloudWatch Logs para solucionar problemas. Para obtener más información, consulte Supervisión con CloudWatch registros en la Guía para AWS IoT desarrolladores.

Para añadir una acción de error de republicar a una regla

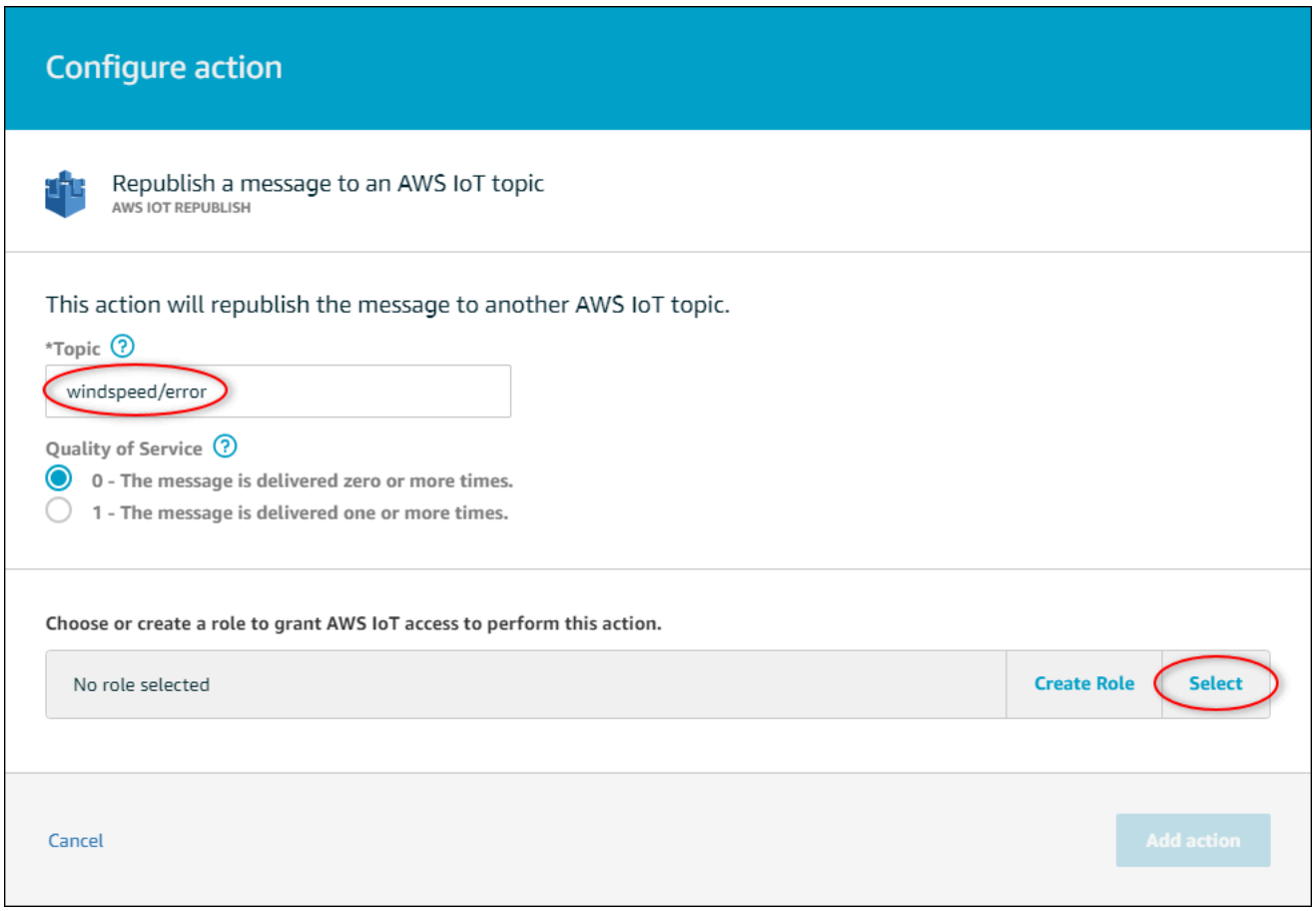
1. Vaya a la consola de AWS IoT.
2. En el panel de navegación izquierdo, elija Act (Acción) y, a continuación, elija Rules (Reglas).
3. Elija la regla que creó anteriormente.



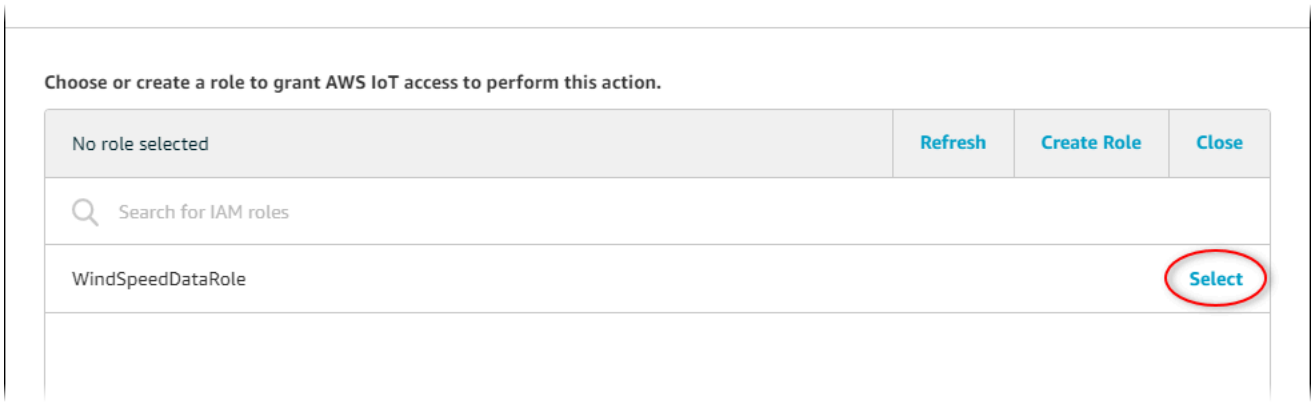
4. En Error action (Acción de error), elija Add action (Agregar acción).
5. Selecciona Volver a publicar un mensaje en un AWS IoT tema.



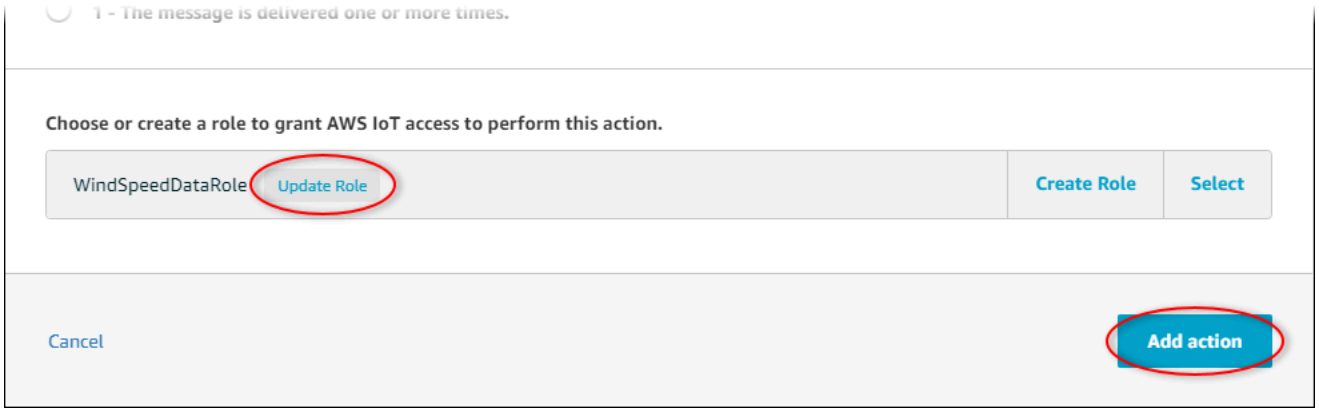
6. Seleccione Configure action (Configurar acción) en la parte inferior de la página.
7. En Tema, escriba **`windspeed/error`**. AWS IoT Core volverá a publicar los mensajes de error relacionados con este tema.



8. Elija Seleccionar para conceder acceso a AWS IoT Core y realizar la acción de error utilizando el rol que creó anteriormente.
9. Elija Select (Seleccionar) junto a su rol.



10. Elija Update role (Actualizar rol) para añadir los permisos adicionales al rol.



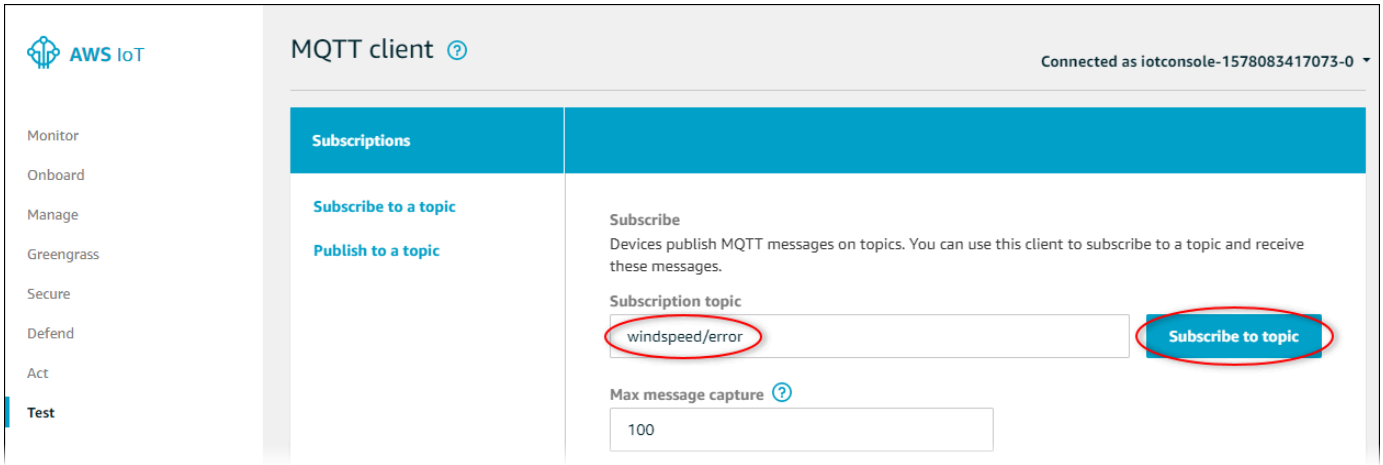
11. Elija Add action (Añadir acción) para terminar de añadir la acción de error.
12. Selecciona la flecha hacia atrás situada en la esquina superior izquierda de la consola para volver a la página de inicio de la consola AWS IoT Core.

Tras configurar la acción de error de republicación, podrá ver los mensajes de error en el cliente de prueba de MQTT de Core. AWS IoT

En el siguiente procedimiento, se suscribe al tema de error en el cliente de prueba de MQTT.

Para suscribirse al tema de acción de error

1. En la página de navegación izquierda de la consola AWS IoT Core, selecciona Probar.
2. En el campo Subscription topic (Tema de suscripción) escriba **`windspeed/error`** y elija Subscribe to topic (Suscribirse al tema).



3. Observe si aparecen mensajes de error y explore la matriz de `failures` en un mensaje de error para diagnosticar los siguientes problemas comunes:

   - Errores tipográficos en la instrucción de consulta de regla

- Permisos de rol insuficientes

Si no aparecen errores, compruebe que la regla esté habilitada y que se suscribió al mismo tema que configuró en la acción de error de Republish. Si los errores siguen sin aparecer, comprueba que los activos de demostración del parque eólico siguen existiendo y que has activado las notificaciones sobre las propiedades de la velocidad del viento. Si sus activos de demostración han caducado o han desaparecido AWS IoT SiteWise, puede crear una nueva versión de demostración y actualizar la declaración de consulta de reglas para que refleje el modelo de activos y los identificadores de propiedad actualizados.

AWS IoT SiteWise puntos finales y cuotas

En las siguientes secciones se describen los puntos finales y las cuotas de AWS IoT SiteWise.

Contenidos

AWS IoT SiteWise puntos finales

Para conectarse mediante programación AWS IoT SiteWise, utilice un punto final. Los AWS SDK y el AWS Command Line Interface (AWS CLI) utilizan automáticamente el punto final predeterminado de una región. AWS Para obtener más información sobre las regiones en las que AWS IoT SiteWise está disponible, consulta los AWS IoT SiteWise puntos finales y las cuotas en. Referencia general de AWS

AWS IoT SiteWise admite los siguientes puntos finales.

data.iotsitewise.region.amazonaws.com

Utilice este punto final para acceder a las siguientes operaciones de API del plano de datos: BatchPutAssetPropertyValueGetAssetPropertyAggregates, GetAssetPropertyValue, GetAssetPropertyValueHistoryy GetInterpolatedAssetPropertyValues. *`region`*Sustitúyala por tu AWS región.

api.iotsitewise.region.amazonaws.com

AWS IoT SiteWise ofrece este punto final consolidado para las operaciones de la API del plano de control que se utiliza para gestionar los modelos de activos, los activos, las pasarelas de SiteWise Edge, las etiquetas y las configuraciones de cuentas. Sustituya *`region`* por su región de AWS .

> **Note**
>
> - De forma predeterminada, AWS IoT SiteWise utiliza el punto final consolidado cuando realiza llamadas a las operaciones de API del plano de control compatibles.
> - Le recomendamos que utilice el punto de conexión consolidado para las operaciones de la API de plano de control admitidas.

- No puede usar el punto de conexión consolidado para acceder a las operaciones de la API SiteWise Monitor.

Las operaciones de API del plano de control compatibles incluyen AssociateAssetsCreateAssetCreateAssetModel, DeleteAsset, DeleteAssetModel,, DeleteDashboard, DescribeAsset, DescribeAssetModel, DescribeAssetProperty, DescribeDashboard, DescribeLoggingOptions, DisassociateAssets, ListAssetModels, ListAssetRelationships,, ListAssets, ListAssociatedAssets, PutLoggingOptions, UpdateAsset, UpdateAssetModel, UpdateAssetProperty, CreateGateway, DeleteGateway, DescribeGateway, DescribeGatewayCapabilityConfiguration, ListGateways, UpdateGateway, UpdateGatewayCapabilityConfiguration, DescribeStorageConfiguration, PutStorageConfiguration, DescribeDefaultEncryptionConfiguration, ListTagsForResource, PutDefaultEncryptionConfiguration, TagResource, y UntagResource.

El punto de conexión de VPC de la interfaz para las operaciones de la API de plano de control solo admite el punto de conexión consolidado. Para obtener más información, consulte Puntos de conexión de VPC .

iotsitewise.region.amazonaws.com

Utilice este punto final para acceder a las siguientes operaciones de API: DescribeStorageConfigurationPutStorageConfigurationDescribeDefaultEncryptionConfiguration, ListTagsForResource, PutDefaultEncryptionConfiguration, TagResource, y UntagResource. Sustituya *`region`* por su región de AWS .

model.iotsitewise.region.amazonaws.com

Utilice este punto final para acceder a las siguientes operaciones de API: AssociateAssetsCreateAssetCreateAssetModel, DeleteAsset, DeleteAssetModel, DeleteDashboard, DescribeAsset, DescribeAssetModel, DescribeAssetProperty, DescribeDashboard,, DescribeLoggingOptions, DisassociateAssets, ListAssetModels, ListAssetRelationships, ListAssets, ListAssociatedAssets, PutLoggingOptions, UpdateAsset , UpdateAssetModel, y UpdateAssetProperty. *`region`*Sustitúyala por tu AWS región.

edge.iotsitewise.region.amazonaws.com

Utilice este punto final para acceder a las siguientes operaciones de la API: CreateGatewayDeleteGatewayDescribeGateway, DescribeGatewayCapabilityConfiguration,

ListGateways, UpdateGateway, y UpdateGatewayCapabilityConfiguration. *region*Sustitúyala por tu AWS región.

monitor.iotsitewise.region.amazonaws.com

Utilice este punto final para acceder a las siguientes operaciones de la API: BatchAssociateProjectAssetsBatchDisassociateProjectAssetsCreateAccessPolicy, CreateDashboard, CreatePortal, CreateProject, DeleteAccessPolicy,, DeletePortal, DeleteProject, DescribeAccessPolicy, DescribePortal, DescribeProject, ListAccessPolicies, ListDashboards,, ListPortals, ListProjectAssets, ListProjects, UpdateAccessPolicy , UpdateDashboard, UpdatePortal, y UpdateProject. Sustituya *region* por su región de AWS .

AWS IoT SiteWise cuotas

En las siguientes tablas se describen las cuotas en AWS IoT SiteWise. Para obtener más información sobre cuotas y cómo solicitar aumentos de cuota, consulte service quotas de AWS en la página Referencia general de AWS. Para obtener más información sobre AWS IoT SiteWise las cuotas, consulte las cuotas de AWS IoT SiteWise servicio en Referencia general de AWS.

Cuotas de activos y modelos de activos

Recurso	Cuota	Ajustable	Notas
Número de modelos de activos por región y por AWS cuenta	1 000	Sí	
Número de activos por modelo de activos	10 000	Sí	
Número de activos secundarios por activo principal	2000	Sí	
Profundidad del árbol de jerarquía del modelo de activos	30	Sí	

Recurso	Cuota	Ajustable	Notas
Número de definiciones de jerarquía por modelo de activos	30	Sí	
Número de propiedades en el nivel raíz por modelo de activo	500	Sí	Este número máximo de `assetModelProperties` para cada modelo de activos. Este recuento no incluye `compositeModelProperties` . Esta cuota también se aplica a cualquier activo único creado a partir de este modelo de activos.

Recurso	Cuota	Ajustable	Notas
Número de propiedades por modelo de activos	5000	Sí	El número máximo de propiedades de un modelo de activos del tipo `ASSET_MODEL` o `COMPONENT_MODEL`. Este número se determina combinando las propiedades del modelo de activos raíz y cualquier modelo compuesto incluido component-model-based o en línea. Esta cuota también se aplica a cualquier activo único creado a partir de este modelo de activos.
Número de propiedades por modelo compuesto	100	Sí	El número máximo de propiedades permitido para los modelos compuestos. Además, el número máximo de propiedades permitido para un modelo de activo de este tipo `COMPONENT_MODEL`.

Recurso	Cuota	Ajustable	Notas
Profundidad del árbol de propiedades por modelo de activos	10	No	Por ejemplo, un modelo con una propiedad de transformación C que consuma una propiedad de transformación B, que a su vez consuma una propiedad de medición A tendrá una profundidad de 3.
Número de modelos de activos por árbol de jerarquía	100	Sí	

Recurso	Cuota	Ajustable	Notas
Número de propiedades directamente dependientes por modelo de activos	20	No	Esta cuota limita el número de propiedades que pueden depender directamente de una sola propiedad, tal y como se define en las expresiones de fórmulas de propiedad. El Número de propiedades dependientes para un modelo de activo debe ser mayor que el Número de propiedades directamente dependientes por modelo de activo. Debe solicitar un aumento de cuota para ambos si el límite para el Número de propiedades directamente dependientes por modelo de activo es mayor que el límite para el Número de propiedades dependientes por modelo de activo.

Recurso	Cuota	Ajustable	Notas
Número de propiedades dependientes por modelo de activos	30	No	Esta cuota limita el número de propiedades que pueden depender directa o indirectamente de una sola propiedad, tal y como se define en las expresiones de fórmulas de propiedad.
Número de modelos compuestos por modelo de activo	50	Sí	El número máximo de modelos compuestos permitido en un único modelo de activos.
Profundidad del modelo compuesto	2	Sí	La profundidad máxima del árbol del modelo compuesto por modelo de activo, incluidos los modelos en línea y component-model-based compuestos.

Recurso	Cuota	Ajustable	Notas
Número de modelos de activos únicos que utilizan el mismo modelo de componentes	20	Sí	El número máximo de modelos de activos únicos que tienen al menos un modelo component-model-based compuesto que hace referencia directamente a un modelo de activos específico del tipo COMPONENT_MODEL.
Número de variables de propiedad por expresión de fórmula de propiedad	10	No	Por ejemplo, hay dos variables de propiedad, `power` y `temp`, en la expresión `avg(power) + max(temp)` . Esto también se aplica a los resultados del cálculo de transformaciones.
Número de funciones por expresión de fórmula de propiedad	10	No	Por ejemplo, hay dos funciones, `avg` y `max`, en la expresión `avg(power) + max(temp)` .

Cuotas de datos de propiedades de activos

Recurso	Cuota	Ajustable	Notas
Velocidad de solicitudes para operaciones de la API de datos de propiedad de activos	1000 solicitudes por segundo por región y por cuenta AWS	Sí	Esta cuota se aplica a las operaciones de la API, como `GetAssetPropertyValue` y `BatchPutAssetPropertyValue`.
Número de puntos de datos por segundo por calidad de datos por propiedad de activo	10 puntos de datos	No	Esta cuota se aplica al número máximo de puntos de datos timestamp-quality-value (TQV) con la misma marca de tiempo en segundos y por calidad de datos para cada propiedad de activo. Puede almacenar hasta este número de puntos de datos de calidad buena, calidad incierta y calidad mala por cada segundo dado para cada propiedad de activo.
Número de `BatchPutAssetPropertyValue` entradas ingeridas por segundo	10 entradas por propiedad de activo	No	Esta cuota se aplica a `BatchPutAssetPropertyValue` las entradas de todas

Recurso	Cuota	Ajustable	Notas
por activo, propiedad, región y cuenta. AWS			las fuentes, incluidas las pasarelas de SiteWise Edge, AWS IoT Core las reglas y las llamadas a la API.
Tasa de puntos de datos ingeridos	5000 puntos de datos por segundo por AWS región y cuenta	Sí	Puntos de datos T imestamp-quality-v alue (TQV).
Tasa de solicitudes para `BatchGetAssetPropertyAggregates`	200	Sí	El número máximo de solicitudes `BatchGetAssetPropertyAggregates` por segundo que puede realizar en esta cuenta en la región actual.
Tasa de solicitudes para `BatchGetAssetPropertyValue`	500	Sí	El número máximo de solicitudes `BatchGetAssetPropertyValue` por segundo que puede realizar en esta cuenta en la región actual.

Recurso	Cuota	Ajustable	Notas
Tasa de solicitudes para `BatchGetAssetPropertyValueHistory`	200	Sí	El número máximo de solicitudes `BatchGetAssetPropertyValueHistory` por segundo que puede realizar en esta cuenta en la región actual.
Número de `BatchPutAssetPropertyValue` entradas ingeridas por segundo por activo, propiedad, región y cuenta. AWS	10 entradas por propiedad de activo	No	Esta cuota se aplica a `BatchPutAssetPropertyValue` las entradas de todas las fuentes, incluidas las pasarelas de SiteWise Edge, AWS IoT Core las reglas y las llamadas a la API.
Tasa de solicitudes `GetAssetPropertyAggregates` y consultas de entrada `BatchGetAssetPropertyAggregates` por propiedad de activo	50	No	El número máximo de solicitudes `GetAssetPropertyAggregates` y entradas `BatchGetAssetPropertyAggregates` totales para cada propiedad de activo por segundo en esta cuenta en la región actual.

Recurso	Cuota	Ajustable	Notas
Tasa de solicitud es `GetAssetPropertyValue` y consultas de entrada `BatchGetAssetPropertyValue` por propiedad de activo	500	No	El número máximo de solicitudes `GetAssetPropertyValue` y entradas `BatchGetAssetPropertyValue` totales para cada propiedad de activo por segundo en esta cuenta en la región actual.
Tasa de solicitud es `GetAssetPropertyValueHistory` y consultas de entrada `BatchGetAssetPropertyValueHistory` por propiedad de activo	30	No	El número máximo de solicitudes `GetAssetPropertyValueHistory` y entradas `BatchGetAssetPropertyValueHistory` totales para cada propiedad de activo por segundo en esta cuenta en la región actual.

Recurso	Cuota	Ajustable	Notas
Tasa de solicitudes de `GetInterpolatedAssetPropertyValues`	500	Sí	El número máximo de solicitudes `GetInterpolatedAssetPropertyValues` por segundo que puede realizar en esta cuenta en la región actual.
Número de resultados por solicitud `GetInterpolatedAssetPropertyValues`	10	Sí	El número máximo de resultados que devolver por solicitud `GetInterpolatedAssetPropertyValues` paginada.

Recurso	Cuota	Ajustable	Notas
Tasa de puntos de datos recuperados de `GetAssetPropertyValueHistory` y `BatchGetAssetPropertyValueHistory`	100 MB de respuesta de lectura por segundo por AWS región y cuenta.	Sí	La velocidad máxima de bytes (MB/segundo) de los puntos de datos recuperados por segundo por región y por cuenta en y. AWS `GetAssetPropertyValueHistory` y `BatchGetAssetPropertyValueHistory` La carga de respuesta evaluada para esta cuota utiliza campos marca de tiempo-calidad-valor (TQV) para cada punto de datos y redondea el tamaño en bytes de cada solicitud de la API al siguiente incremento de 4 KB. Los puntos de datos Timestamp-quality-value (TQV) recuperados por segundo varían según el tipo de datos: • Entero: hasta 5 millones de TQV por segundo

Recurso	Cuota	Ajustable	Notas
			• Doble: hasta 4 millones de TQV por segundo • Booleano: hasta 6 millones de TQV por segundo • Cadena: varía en función del tamaño del valor de cada cadena.

Cuotas para las puertas de enlace Edge SiteWise

Recurso	Cuota	Ajustable
Número de puertas de enlace SiteWise Edge por región y cuenta AWS	100	Sí
Número de fuentes OPC-UA por puerta de enlace Edge SiteWise	100	No

Cuotas para AWS IoT SiteWise Monitor

Recurso	Cuota	Ajustable
Número de portales por región y por AWS cuenta	100	Sí
Número de proyectos por portal	100	Sí
Número de paneles por proyecto	100	Sí

Recurso	Cuota	Ajustable
Número de activos raíz por proyecto	1	No
Número de visualizaciones por panel	10	Sí
Número de métricas por visualización del panel	5	Sí
Número de umbrales por visualización del panel de control	12	No

Cuotas de importación y exportación AWS IoT SiteWise masivas de metadatos

Recurso	Descripción	Cuota	Ajustable
Número de trabajos de transferencia de metadatos en cola	El número máximo de trabajos de transfere ncia de `PENDING` metadatos en la cola.	10	Sí
Tamaño del archivo de importación del trabajo de transfere ncia de metadatos	El tamaño máximo del archivo importado (en MB).	100 MB	Sí
AWS IoT SiteWise cuota de recursos para un trabajo de transferencia de metadatos	El número máximo de recursos importados o exportados en un solo trabajo. Un recurso incluye activos y modelos de activos.	5000	No

Cuotas para la importación AWS IoT SiteWise masiva de datos

Recurso	Cuota	Ajustable
Número de trabajos de importación masiva en ejecución	100	No
Tamaño del archivo CSV	10 GB	No
Tamaño del archivo de parquet sin comprimir	256 MB	No
Tamaño del `CSV` archivo para la ingesta almacenada en búfer	256 MB	No
Tamaño del grupo de hileras de parqué sin comprimir	64 MB	No
Número de medidas únicas por grupo de hileras de parquet	2000	Sí
Número de días transcurridos entre la fecha y la fecha en que se registró la ingestión en búfer	30	Sí
Tarifa de solicitud para cada región de `CreateBulkImportJobs` cada cuenta AWS	10	Sí
Solicita una tasa `ListBulkImportJobs` para cada región de cada AWS cuenta	50	Sí
Solicita una tasa `DescribeBulkImportJobs` para	50	Sí

Recurso	Cuota	Ajustable
cada región de cada AWS cuenta		

Cuotas de detección de anomalías

Las cuotas de detección de anomalías se comparten entre Amazon Lookout for Equipment AWS IoT SiteWise y Amazon Lookout for Equipment. Para obtener más información, consulta Cuotas de uso de Lookout for Equipment.

Historial de documentos de la Guía AWS IoT SiteWise del usuario

En la siguiente tabla se describe la documentación de esta versión de AWS IoT SiteWise.

- Versión de API: 2019-12-02

Cambio	Descripción	Fecha
Se agregó soporte para ejecutar SiteWise Edge en Siemens Industrial Edge	AWS IoT SiteWise ahora es compatible con la ejecución de SiteWise Edge en dispositivos Siemens Industrial Edge.	26 de noviembre de 2023
Se agregó soporte para almacenamiento en niveles cálidos	AWS IoT SiteWise ahora es compatible con el almacenam iento en caliente, un nivel de almacenamiento totalmente gestionado que facilita a los clientes el almacenamiento seguro de los datos industria les y el acceso a ellos.	15 de noviembre de 2023
Se agregó soporte para identificadores únicos definidos por el usuario	AWS IoT SiteWise ahora admite el uso de identific adores únicos definidos por el usuario para activos, modelos de activos, propiedades y jerarquías.	15 de noviembre de 2023
Se ha añadido soporte para la detección de anomalías multivariantes en activos industriales	AWS IoT SiteWise ahora admite la detección de anomalías multivariante de activos industriales mediante la integración de datos históricos y en tiempo real	15 de noviembre de 2023

	de los equipos con Amazon Lookout for Equipment.	
Se agregó soporte para la ingesta rentable y escalable de datos de series temporales en AWS IoT SiteWise	AWS IoT SiteWise ahora permite la ingesta rentable y escalable de los datos de series temporales necesarios para los casos de uso analítico s.	15 de noviembre de 2023
Se agregó soporte para la importación, exportación y actualización masivas	AWS IoT SiteWise ahora admite la importación, exportación y actualización masivas de metadatos de equipos industriales.	15 de noviembre de 2023
Se agregó soporte para los componentes del modelo de activos	AWS IoT SiteWise ahora es compatible con los component es del modelo Asset para ayudar a los clientes industria les a crear componentes reutilizables.	15 de noviembre de 2023
Se agregó soporte para la aplicación de panel de control de IoT	AWS IoT SiteWise ahora es compatible con una aplicació n de panel de código abierto en la que puede visualizar los datos operativos e interactuar con ellos.	15 de noviembre de 2023
Se actualizaron las funciones vinculadas al servicio para AWS IoT SiteWise	AWS IoT SiteWise tiene nuevas funciones vinculada s al servicio y puede ejecutar una consulta de búsqueda de metadatos en la base de datos. AWS IoT TwinMaker	6 de noviembre de 2023

Etiquetado actualizado para los recursos del flujo de datos AWS IoT SiteWise	Se añadió soporte para etiquetar los recursos del flujo de datos.	18 de agosto de 2022
Puertas de enlace SiteWise Edge actualizadas	Ahora se puede configurar el publicador para que controle qué datos deben enviarse desde la periferia a la nube y el orden en que deben enviarse a la nube.	12 de enero de 2022
Se actualizó la demostración AWS IoT SiteWise	Ahora puede utilizar la demostración para crear un portal de SiteWise monitores.	10 de enero de 2022
Se actualizó la administración del almacenamiento	Ahora puede definir un período de retención para controlar cuánto tiempo deben conservarse sus datos en el nivel de acceso frecuente.	29 de noviembre de 2021
Se añadió soporte para la administración del flujo de datos	Ahora puede incorporar datos AWS IoT SiteWise antes de crear modelos y activos de activos.	24 de noviembre de 2021
Se actualizaron las jerarquías de los modelos de activos	Ahora se puede asociar un modelo de entidad secundari a a varios modelos de activos principales.	28 de octubre de 2021
Lanzamiento regional	Lanzado AWS IoT SiteWise en AWS GovCloud (EE. UU., oeste).	29 de septiembre de 2021

Funciones de actualización	Se añadieron las siguientes características • En las métricas, puede usar expresiones anidadas en las funciones de agregación y las funciones temporales. • En las transformaciones, puede utilizar la función pretrigger() para recuperar el valor de una variable antes de actualizar la propiedad que activó el cálculo de la transformación actual.	10 de agosto de 2021
Intervalo de tiempo personalizado para las métricas	Se añadió soporte para los intervalos de tiempo personalizados y los desfases en las métricas.	3 de agosto de 2021
AWS IoT SiteWise Utilizándolo en el borde	La característica de procesamiento en la periferia está ahora disponible de forma general.	29 de julio de 2021
Exportación de datos a Amazon S3	AWS IoT SiteWise ahora puede exportar datos a Amazon S3.	27 de julio de 2021
Puntos de conexión de VPC (AWS PrivateLink)	El punto de conexión de VPC en la interfaz para las operaciones de API de plano de control ahora está disponible con carácter general.	15 de julio de 2021

Transformaciones	Las transformaciones ahora pueden introducir múltiples variables de propiedades de activos.	8 de julio de 2021
Se actualizó la función marca temporal()	En las transformaciones, ahora se puede proporcionar una variable como argumento a la función `timestamp()` .	16 de junio de 2021
Disponibilidad general de alarmas	La característica de alarmas ya está disponible con carácter general.	27 de mayo de 2021
Se lanzó la versión 2 del adaptador de protocolo Modbus-TCP	Está disponible la versión 2 del conector del adaptador de protocolo Modbus-TCP. Esta versión añadió soporte para las cadenas de origen codificadas en ASCII, UTF8 e ISO8859.	24 de mayo de 2021
Service quotas actualizadas	Se agregaron las siguiente s cuotas para la GetInterp olatedAssetPropert yValuesAPI: tasa de `GetInterpolatedAss etPropertyValues` solicitudes, cantidad de resultados por `GetInterp olatedAssetPropert yValues` solicitud y cantidad de días entre la fecha de inicio anterior y la fecha actual de`GetInterpolatedAss etPropertyValues` .	29 de abril de 2021

Se actualizaron las expresiones de fórmula	Se añadieron los siguientes operadores y funciones: • Se añadieron los siguientes operadores: `<`, `>`, `<=`, `>=`, `==`, `!=`, `!`, `and`, `or` y `not`. • Se añadió la siguiente función de comparación:`neq(x, y)`. • Se añadieron las siguientes funciones de cadena: `join()`, `format()` y `f''`.	22 de abril de 2021
Puntos de conexión de VPC (AWS PrivateLink)	Se agregó información sobre cómo establecer una conexión privada entre su nube privada virtual (VPC) y las API del plano de AWS IoT SiteWise control mediante la creación de un punto final de VPC de interfaz.	16 de marzo de 2021
Federación de IAM	Los administradores y usuarios del portal SiteWise Monitor ahora pueden iniciar sesión en los portales asignados con sus credenciales de IAM.	16 de marzo de 2021
Lanzamiento regional	Lanzado AWS IoT SiteWise en China (Pekín).	3 de febrero de 2021

Lanzamiento de la versión 10 SiteWise del conector IoT	Está disponible la versión 10 SiteWise del conector IoT. Esta versión configura `StreamManager` para mejorar el control cuando se pierda y se restablez ca la conexión de origen. Esta versión también acepta valores OPC-UA con un código `ServerTim estamp` cuando no haya un `SourceTimestamp` disponible.	22 de enero de 2021
Funciones de fecha y hora	AWS IoT SiteWise ahora es compatible con las funciones de fecha y hora.	21 de enero de 2021
Sintaxis de las funciones	Ahora puede utilizar la sintaxis uniforme de llamadas a funciones (UFCS) para AWS IoT SiteWise las funciones.	11 de enero de 2021
Integración con Grafana	Se agregó información sobre cómo visualizar los AWS IoT SiteWise datos en los paneles de Grafana.	15 de diciembre de 2020

AWS IoT SiteWise lanzamiento de funciones	Ahora puede monitorizar sus datos con alarmas, procesar datos industriales en la periferia, utilizar fuentes Modbus TCP y EtherNet/IP en su puerta de enlace SiteWise Edge, filtrar los datos entrantes con bandas muertas y mucho más. • Se añadió la sección Monitoreo de datos con alarmas que se puede utilizar para definir, configurar y responder a las alarmas en AWS IoT SiteWise. • Se añadió la sección Procesamiento en la periferia que se puede usar para configurar el procesamiento de sus datos industriales en sus dispositivos de periferia. • Se agregaron las secciones Modbus TCP y EtherNet/IP a la documentación fuente de la puerta de enlace Edge. SiteWise • Se añadió la sección destino del origen que se puede usar para personalizar el lugar al que deben enviarse los datos industriales entrantes.	15 de diciembre de 2020

	• Se agregó la sección de filtrado OPC-UA que puede usar para controlar la frecuencia y el tipo de datos que se envían a su puerta de enlace SiteWise Edge desde su servidor local industrial.	
AWS IoT SiteWise ahora es compatible con las CMK gestionadas por el cliente.	AWS IoT SiteWise ahora admite el cifrado con CMK gestionadas por el cliente.	24 de noviembre de 2020
Lanzamiento de la versión 8 SiteWise del conector IoT	Está disponible la versión 8 SiteWise del conector IoT. Esta versión mejora la estabilidad cuando el conector experimenta una conectividad de red intermitente.	19 de noviembre de 2020
Uso de cadenas y condicionales en expresiones de fórmula	Se agregó información sobre cómo encadenar y funciones condicionales en expresiones de fórmula para transformaciones y métricas.	16 de noviembre de 2020
Ingerir datos mediante el administrador de AWS IoT Greengrass flujos	Se agregó información sobre cómo ingerir grandes volúmenes de datos de IoT de fuentes de datos locales mediante un dispositivo AWS IoT Greengrass perimetral.	16 de septiembre de 2020

Puntos de conexión de VPC (AWS PrivateLink)	Se agregó información sobre cómo establecer una conexión privada entre su nube privada virtual (VPC) y las API de AWS IoT SiteWise datos mediante la creación de un punto final de VPC de interfaz.	4 de septiembre de 2020
Lanzamiento de la versión 7 SiteWise del conector IoT	Está disponible la versión 7 SiteWise del conector IoT. Esta versión corrige un problema con las métricas de SiteWise Edge Gateway.	14 de agosto de 2020
Creación de usuarios del IAM Identity Center desde la consola AWS IoT SiteWise	Se agregó información sobre cómo crear usuarios del IAM Identity Center en la AWS IoT SiteWise consola. Ahora puede crear usuarios de IAM Identity Center cuando asigne usuarios a un portal nuevo o existente. Se actualizó el tutorial Visualización y uso compartido de datos de parques eólicos para utilizar esta característica. Este cambio reduce el número de pasos del tutorial.	4 de agosto de 2020
Solución de problemas mejorada de SiteWise Edge Gateway	Se agregó información adicional sobre cómo solucionar problemas con una puerta de enlace SiteWise Edge y cómo exportar el certificado de cliente OPC-UA a una fuente.	18 de junio de 2020

Documentación de tareas de la consola	Se ha agregado documentación de tareas de la consola para Modelado de activos industriales, Consulta de datos de propiedades de activos e Interacción con otros servicios. Puede seguir estas instrucciones para completar las tareas en la consola de AWS IoT SiteWise .	11 de junio de 2020
Tutorial de análisis de datos exportados	Se agregó un tutorial que puede seguir para aprender a usar Amazon Athena para analizar los datos de activos que exportó a S3 con la plantilla de características AWS CloudFormation de exportación.	27 de mayo de 2020
Mejorado mediante el uso de expresiones de fórmula	Se agregó información detallada sobre el comportamiento de las propiedades de las AWS IoT SiteWise fórmulas y se agregó un ejemplo de cómo contar los puntos de datos filtrados.	18 de mayo de 2020

Lanzamiento de la versión 6 SiteWise del conector IoT	Está disponible la versión 6 SiteWise del conector IoT. Esta versión añade compatibilidad con las CloudWatch métricas y la detección automática de nuevas etiquetas OPC-UA. Esto significa que no es necesario reiniciar la puerta de enlace SiteWise Edge cuando cambien las etiquetas de las fuentes OPC-UA. Esta versión del conector requiere el administrador de transmisiones y el software AWS IoT Greengrass Core v1.10.0 o superior.	29 de abril de 2020

AWS IoT SiteWise versión de funciones	AWS IoT SiteWise lanzamiento de funciones. Ahora puede administrar las puertas de enlace de SiteWise Edge con la API, añadir su logotipo a los portales, ver las métricas de las puertas de enlace de SiteWise Edge y mucho más. • Se agregó la sección Exportación de datos a Amazon S3 con una AWS CloudFormation plantilla que puede usar para exportar nuevos valores de datos a un bucket de S3. • Se agregó la sección Configuración de fuentes de datos que mejora la documentación fuente de SiteWise Edge Gateway e incluye las nuevas API de SiteWise Edge Gateway. • Se agregó la sección de métricas de las puertas de enlace de SiteWise Edge, que describe las CloudWatch métricas que publican las puertas de enlace de SiteWise Edge. • Se agregó la sección Configuración de una puerta de enlace SiteWise Edge en Amazon EC2 con una AWS CloudFormation plantilla que puede usar para configurar	29 de abril de 2020

	rápidamente las dependencias de la puerta de enlace SiteWise Edge en una instancia de Amazon EC2. • Se agregó la sección de funciones de servicio del portal que describe la nueva función de permisos de SiteWise los portales Monitor. • Se ha actualizado la documentación del portal para roles de servicio del portal y logotipos del portal. • Se agregó la sección Cómo etiquetar AWS IoT SiteWise los recursos. • Se ha actualizado la sección Creación de paneles (CLI) para la nueva estructura de definición de panel. • Se ha agregado la sección Seguridad.	
Ingerir datos de AWS IoT Events	Se agregó información sobre cómo ingerir datos del AWS IoT Events momento en que ocurre un evento.	20 de abril de 2020
Tutorial sobre visualización y uso compartido de datos de parques eólicos en Monitor SiteWise	Se ha añadido un tutorial que puede seguir para aprender a utilizarlos AWS IoT SiteWise Monitor para visualizar y compartir datos de activos.	12 de marzo de 2020

AWS IoT SiteWise conceptos	Se ha añadido un glosario de AWS IoT SiteWise conceptos que puede utilizar para obtener información sobre el servicio y sus términos comunes.	5 de marzo de 2020
Se eliminaron AWS IoT Greengrass las instrucciones de instalación	Se eliminaron las instrucciones de instalación del software AWS IoT Greengrass básico de la Guía AWS IoT SiteWise del usuario. La Guía para AWS IoT Greengrass desarrolladores incluye un script de configuración del dispositivo e instrucciones para configurarlo AWS IoT Greengrass en otras plataformas, como Amazon EC2 y Docker.	14 de febrero de 2020
Se ha mejorado la ingesta de datos mediante reglas AWS IoT Core	Se ha añadido información detallada sobre cómo utilizar y solucionar los problemas de la acción de la AWS IoT SiteWise regla, que se puede utilizar para ingerir datos de los mensajes de MQTT mediante ella. AWS IoT Core	14 de febrero de 2020
Lanzamiento de la versión 5 SiteWise del conector IoT	Está disponible la versión 5 SiteWise del conector IoT. Esta versión corrige un problema de compatibilidad con la versión AWS IoT Greengrass 1.9.4 del software Core.	12 de febrero de 2020

Lanzamiento de la versión 4 SiteWise del conector IoT	Está disponible la versión 4 SiteWise del conector IoT. Esta versión corrige un problema con la reconexión del servidor OPC-UA.	7 de febrero de 2020
Activos industriales de modelado reestructurados	Se ha reestructurado la sección Actualización de activos y modelos en varios temas dentro de Modelado de activos industriales. • Estados de activos y modelos • Asignación de flujos de datos industriales a propiedades de activos • Actualización de valores de atributos • Asociación y disociación de activos • Actualizar activos y modelos • Eliminación de activos y modelos	4 de febrero de 2020
Tutorial sobre cómo ingerir datos de AWS IoT cosas	Se agregó un tutorial que puede seguir para aprender a configurar una acción de AWS IoT SiteWise regla para ingerir datos de una flota de AWS IoT cosas nueva o existente.	4 de febrero de 2020

Reestructurada: recuperación de datos de AWS IoT SiteWise	Se reestructuró la sección de recuperación de datos en dos secciones de nivel superior: Consulta de valores y agregados de propiedades de activos e Interacción con otros servicios. AWS	21 de enero de 2020
Publicación de actualizaciones de valores de propiedades en el tutorial de Amazon DynamoDB	Se ha agregado un tutorial que puede seguir para aprender a utilizar las notificaciones de valor de propiedad para almacenar datos de activos en DynamoDB.	8 de enero de 2020
Uso de expresiones de fórmula	Se ha agregado la referenci a de expresión de fórmula para organizar las constante s y las funciones disponibles para su uso en propiedades de transformación y métricas. Propiedades de activos se ha reestructurado en varios temas independientes en función de cada tipo de propiedad.	7 de enero de 2020
Uso de filtros de nodos OPC-UA	Se agregó información sobre cómo usar los filtros de nodos OPC-UA para mejorar el rendimiento de las puertas de enlace de Edge al agregar fuentes de puertas de enlace de SiteWise Edge. SiteWise	3 de enero de 2020

Actualización de un conector	Se agregó información sobre cómo actualizar una puerta de enlace SiteWise Edge cuando se publique una nueva versión del conector.	30 de diciembre de 2019
Lanzamiento de la versión 3 SiteWise del conector IoT	Está disponible la versión 3 SiteWise del conector IoT. Esta versión elimina el requisito de permisos de iot:*.	17 de diciembre de 2019
Lanzamiento de la versión 2 SiteWise del conector IoT	Está disponible la versión 2 SiteWise del conector IoT. Esta versión agrega compatibilidad para múltiples recursos de secretos de OPC-UA.	10 de diciembre de 2019
Creación de paneles de control (AWS CLI)	Se agregó información sobre cómo crear un panel al AWS IoT SiteWise Monitor usar el AWS CLI.	6 de diciembre de 2019

AWS IoT SiteWise publicada la versión 2	Vista previa publicada de la versión 2 de AWS IoT SiteWise. Ahora puede ingerir datos a través de OPC-UA, MQTT y HTTP, modelar sus datos en jerarquías de activos y visualizarlos con Monitor. SiteWise • Se ha reescrito la sección de modelado de activos en cambios en activos, modelos de activos y jerarquías de activos. • Se actualizó la sección de ingesta de datos para incluir los pasos de AWS IoT Greengrass conexión y las secciones de ingesta de datos que no son de pasarela. • Se agregó la AWS IoT SiteWise Monitorsección y una guía de aplicación independiente que muestra cómo usar la aplicación web SiteWise Monitor. • Se han agregado las secciones Consulta datos de AWS IoT SiteWise y Interacción con otros AWS servicios. • Se ha reescrito la sección de introducción para que coincida con la experiencia	2 de diciembre de 2019

	de la demostración actualizada.	
AWS IoT SiteWise publicada la versión 1	Publicada la vista previa inicial de la versión 1 de AWS IoT SiteWise.	25 de febrero de 2019

Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el Glosario de AWS en la Referencia de Glosario de AWS.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.