Manual do usuário

AWS IoT SiteWise

AWS IoT SiteWise: Manual do usuário

Table of Contents

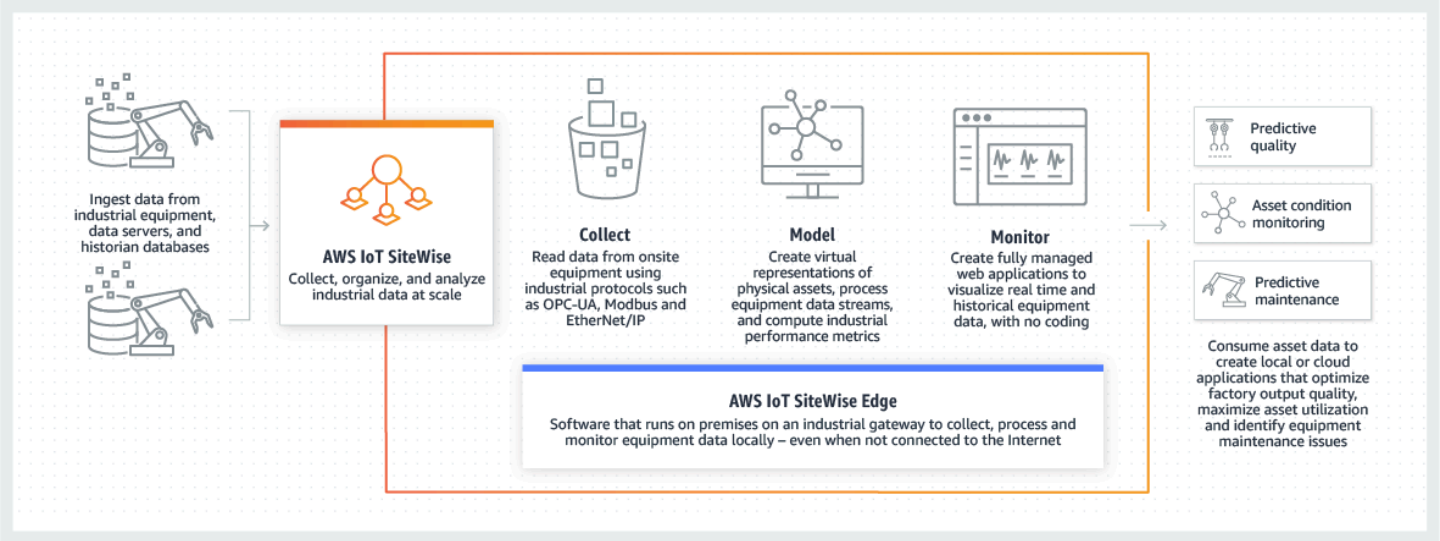
O que AWS IoT SiteWiseé

AWS IoT SiteWise é um serviço gerenciado que facilita a coleta, o armazenamento, a organização e o monitoramento de dados de equipamentos industriais em grande escala para ajudá-lo a tomar melhores decisões baseadas em dados. Você pode usar AWS IoT SiteWise para monitorar operações em várias instalações, calcular rapidamente métricas comuns de desempenho industrial e criar aplicativos que analisam dados de equipamentos industriais para evitar problemas caros com equipamentos e reduzir lacunas na produção.

AWS IoT SiteWise Monitor permite que seus usuários operacionais criem rapidamente aplicativos web para visualizar e analisar seus dados industriais em tempo real. É possível obter insights sobre suas operações industriais configurando e monitorando métricas, como tempo médio entre falhas e eficiência geral do equipamento (OEE).

AWS IoT SiteWise O Edge é um componente AWS IoT SiteWise que permite a coleta, armazenamento e processamento de dados em dispositivos locais. Isso é útil se você tiver acesso limitado à Internet ou precisar manter seus dados privados.

O diagrama a seguir mostra a arquitetura básica de AWS IoT SiteWise:



Tópicos

- Como AWS IoT SiteWise funciona
- AWS IoT SiteWise conceitos
- Casos de uso para AWS IoT SiteWise

Como AWS IoT SiteWise funciona

AWS IoT SiteWise oferece uma estrutura de modelagem de recursos que você pode usar para criar representações de seus dispositivos, processos e instalações industriais. As representações de seus equipamentos e processos são chamadas de modelos de ativos em AWS IoT SiteWise. Com os modelos de ativos, você define os dados brutos a serem consumidos e como processá-los em métricas úteis. Crie e visualize ativos e modelos para sua operação industrial no AWS IoT SiteWise console. Você também pode configurar modelos de ativos para coletar e processar dados na borda ou na AWS nuvem.

Tópicos

Ingerir dados industriais

Comece a usar AWS IoT SiteWise ingerindo dados industriais. A ingestão de seus dados é feita de várias maneiras:

- Ingestão direta de servidores locais: utilize protocolos como o OPC-UA para ler dados diretamente de dispositivos locais. Implemente o software de gateway SiteWise Edge AWS IoT Greengrass V2, compatível com, em uma ampla variedade de plataformas, como gateways industriais comuns ou servidores virtuais. Você pode conectar até 100 servidores OPC-UA a um único AWS IoT SiteWise gateway. Para ter mais informações, consulte SiteWise Requisitos do gateway Edge.

  Observe que protocolos como Modbus TCP e EtherNet/IP (EIP) são suportados por meio de nossa parceria com a no contexto de. Domatica AWS IoT Greengrass V2
- Processamento de dados Edge com pacotes: aprimore seu gateway SiteWise Edge adicionando pacotes para permitir recursos abrangentes de borda. Com o SiteWise Edge, disponível em AWS IoT Greengrass V2, o processamento de dados é executado diretamente no local antes de serem transmitidos com segurança para a AWS nuvem usando um AWS IoT Greengrass stream. Para ter mais informações, consulte Usar pacotes.

- Ingestão adaptável via Amazon S3 com operações em massa: ao trabalhar com um grande número de ativos ou modelos de ativos, use operações em massa para importar e exportar recursos em massa dos buckets do Amazon S3. Para ter mais informações, consulte Operações em massa com ativos e modelos.
- Mensagens MQTT com regras AWS IoT principais: Para dispositivos conectados ao AWS IoT Core enviando mensagens MQTT, use o mecanismo de regras AWS IoT principais para direcionar essas mensagens para AWS IoT SiteWise. Se você tiver dispositivos conectados ao AWS IoT Core enviando mensagens MQTT, use o mecanismo de regras AWS IoT principais para rotear essas mensagens para. AWS IoT SiteWise Para ter mais informações, consulte Ingestão de dados usando regras AWS IoT Core.
- Ingestão de dados acionada por eventos: use AWS IoT Events ações para configurar a SiteWise ação de IoT para enviar dados AWS IoT Events para quando os eventos ocorrerem. AWS IoT SiteWise Para ter mais informações, consulte Ingestão de dados de AWS IoT Events.
- AWS IoT SiteWise API: Seus aplicativos no Edge ou na nuvem podem enviar dados diretamente para AWS IoT SiteWise. Para ter mais informações, consulte Ingestão de dados usando a API AWS IoT SiteWise.

Modele ativos para contextualizar os dados coletados

Depois de ingerir dados, você pode usá-los para criar representações virtuais de seus ativos, processos e instalações criando modelos de suas operações físicas. Um ativo, representando um dispositivo ou processo, transmite fluxos de dados para a nuvem. AWS Os ativos também podem significar agrupamentos lógicos de dispositivos. As hierarquias são formadas pela associação de ativos para espelhar operações complexas. Essas hierarquias permitem que os ativos acessem dados dos ativos secundários associados. Os ativos são criados a partir de modelos de ativos. Os modelos de ativos são estruturas declarativas que padronizam os formatos dos ativos. Reutilize componentes de ativos para organização e manutenção de seus modelos. Para ter mais informações, consulte Modelagem de ativos industriais.

Com AWS IoT SiteWise, você pode configurar seus ativos para transformar os dados recebidos em métricas e transformações contextuais.

- Transforma o trabalho ao receber dados do equipamento.
- As métricas são calculadas em intervalos definidos por você.

As métricas e as transformações são aplicáveis tanto a ativos individuais quanto a vários ativos.AWS IoT SiteWise calcula automaticamente agregados estatísticos comumente usados, como média, soma e contagem, em vários períodos de tempo relevantes para os dados, métricas e transformações do seu equipamento.

Os ativos podem ser sincronizados usando AWS IoT TwinMaker. Para ter mais informações, consulte Integração do AWS IoT SiteWise e do AWS IoT TwinMaker.

Analise usando consultas, alarmes e previsões

Analise a data AWS IoT SiteWise coletada executando consultas e configurando alarmes. Você também pode usar o Amazon Lookout para detectar automaticamente anomalias nas métricas e identificar suas causas básicas.

- Defina alarmes específicos para alertar sua equipe quando equipamentos ou processos se desviam do desempenho ideal, garantindo a rápida identificação e resolução de problemas. Para ter mais informações, consulte Monitorar dados com alarmes.
- Use as operações da AWS IoT SiteWise API para consultar os valores atuais, valores históricos e agregados de suas propriedades de ativos em intervalos de tempo específicos. Para ter mais informações, consulte Consultar dados de AWS IoT SiteWise.
- Use a detecção de anomalias com o Amazon Lookout for Equipment para identificar e visualizar mudanças no equipamento ou nas condições operacionais. Com a detecção de anomalias, você pode determinar medidas de manutenção preventiva para suas operações. Essa integração permite que os clientes sincronizem dados entre o Amazon Lookout for Equipment AWS IoT SiteWise e o Amazon. Para ter mais informações, consulte Detecção de anomalias em equipamentos com o Amazon Lookout for Equipment.

Visualize as operações

Configure o SiteWise Monitor para criar aplicativos web para seus funcionários operacionais. Os aplicativos da web ajudam os funcionários a visualizar suas operações. Gerencie níveis variados de acesso para seus funcionários usando o IAM Identity Center ou o IAM. Configure logins e permissões exclusivos para cada funcionário para visualizar subconjuntos específicos de toda uma operação industrial. AWS IoT SiteWise fornece um guia de aplicação para que esses funcionários aprendam a usar o SiteWise Monitor.

Para obter mais informações sobre como visualizar suas operações, consulteMonitorando dados com AWS IoT SiteWise Monitor.

Armazenamento de dados

Você pode integrar o armazenamento de séries temporais ao seu data lake industrial. AWS IoT SiteWise tem três níveis de armazenamento para dados industriais:

- Um nível de armazenamento dinâmico otimizado para aplicativos em tempo real.
- Um nível de armazenamento aquecido otimizado para cargas de trabalho analíticas.
- Um nível de armazenamento a frio gerenciado pelo cliente usando o Amazon S3 para aplicativos de dados operacionais com alta tolerância à latência.

AWS IoT SiteWise ajuda você a gerenciar os custos de armazenamento mantendo os dados recentes no nível de armazenamento dinâmico. Em seguida, você define políticas de retenção de dados para mover dados históricos para armazenamento em camadas quentes ou frias. Para ter mais informações, consulte Gerenciando o armazenamento de dados.

Você também pode importar e exportar metadados de ativos. Para obter mais informações, consulte Metadados de ativos.

Integração com outros serviços da

AWS IoT SiteWise se integra a vários AWS serviços para desenvolver uma AWS IoT solução completa na AWS nuvem. Para ter mais informações, consulte Interagindo com outros serviços AWS.

AWS IoT SiteWise conceitos

A seguir estão os principais conceitos de AWS IoT SiteWise:

Agregar

Os agregados são métricas ou medições fundamentais que calculam AWS IoT SiteWise automaticamente todos os dados da série temporal. Para ter mais informações, consulte Consultando agregados de propriedades de ativos.

Ativo

Quando você insere ou ingere dados AWS IoT SiteWise de seu equipamento industrial, seus dispositivos, equipamentos e processos são exibidos como ativos. Cada ativo tem dados associados. Por exemplo, um equipamento pode ter um número de série, um local, uma marca e modelo e uma data de instalação. Também pode ter valores de séries temporais para

disponibilidade, desempenho, qualidade, temperatura, pressão e muito mais. Agrupe os ativos em hierarquias, permitindo que os ativos acessem os dados armazenados em seus ativos secundários. Para ter mais informações, consulte Modelagem de ativos industriais.

Hierarquia de ativos

Configure hierarquias de ativos para criar representações lógicas de suas operações industriais. Para fazer isso, defina uma hierarquia em um modelo de ativo e associe os ativos criados a partir desse modelo à hierarquia especificada. As métricas nos ativos principais podem combinar dados das propriedades dos ativos secundários, permitindo que você calcule métricas que oferecem informações sobre sua operação geral ou sobre uma parte específica dela. Para ter mais informações, consulte Definindo hierarquias de modelos de ativos.

Modelo de ativo

Cada ativo é feito usando um modelo de ativo. Modelos de ativos são estruturas que definem e padronizam o formato de seus ativos. Eles garantem informações consistentes em vários ativos do mesmo tipo, permitindo que você manipule dados em ativos que representam grupos de dispositivos. Em cada modelo de ativo, você pode definir atributos, entradas de séries temporais (medições), transformações de séries temporais (transformações), agregação de séries temporais (métricas) e hierarquias de ativos. Para ter mais informações, consulte Modelagem de ativos industriais.

Decida onde as propriedades do seu modelo de ativo são processadas configurando seu modelo de ativo para a borda. Utilize esse recurso para manipular e monitorar dados de ativos em seus dispositivos locais.

Propriedade de ativo

As propriedades dos ativos são as estruturas dentro de cada ativo que contêm dados industriais. Cada propriedade tem um tipo de dados e também pode ter uma unidade. Uma propriedade pode ser um atributo, uma medição, uma transformação ou uma métrica. Para ter mais informações, consulte Definir propriedades de dados.

Configure as propriedades dos ativos para computação na borda. Para obter mais informações sobre o processamento de dados na borda, consulte the section called “Habilitar o processamento de dados de borda”.

Atributo

Os atributos são propriedades de um ativo que normalmente permanecem constantes, como o fabricante do dispositivo ou a localização do dispositivo. Os atributos podem ter valores

predefinidos. Cada ativo criado a partir de um modelo de ativo inclui os valores padrão dos atributos definidos nesse modelo. Para ter mais informações, consulte Definindo dados estáticos (atributos).

Painel

Cada projeto contém um conjunto de painéis. Os painéis fornecem um conjunto de visualizações para os valores de um de ativos. Os proprietários do projeto criam os painéis e as visualizações contidas neles. Quando um proprietário de projeto está pronto para compartilhar o conjunto de painéis, o proprietário pode convidar visualizadores para o projeto e lhes conceder acesso a todos os painéis do projeto. Se você quiser um conjunto de visualizadores diferente para painéis diferentes, será necessário dividir os painéis entre projetos. Quando os espectadores visualizam os painéis, eles podem personalizar o intervalo de tempo para analisar dados específicos.

Fluxo de dados

Insira ou consuma dados industriais antes AWS IoT SiteWise mesmo de criar modelos e ativos de ativos. AWS IoT SiteWise gera automaticamente fluxos de dados para coletar fluxos de dados brutos do seu equipamento.

Apelido de fluxo de dados

Os apelidos de fluxo de dados ajudam a identificar facilmente um fluxo de dados. Por exemplo, o alias `server1-windfarm/3/turbine/7/temperature` indica valores de temperatura provenientes da turbina #7 no parque eólico #3. O termo `server1` é o nome da fonte de dados que ajuda a identificar o servidor OPC-UA e `server1-` é um prefixo anexado a todos os fluxos de dados reportados desse servidor OPC-UA.

Associação de fluxo de dados

Depois de criar modelos e ativos de ativos, associe fluxos de dados às propriedades de ativos definidas em seus ativos para estruturar seus dados. AWS IoT SiteWise pode então usar modelos de ativos e ativos para lidar com dados recebidos de seus fluxos de dados. Você também pode desassociar fluxos de dados das propriedades do ativo. Para ter mais informações, consulte Gerenciar fluxos de dados.

Fórmula

Cada propriedade de transformação e métrica vem com uma fórmula que descreve como a propriedade transforma ou agrega dados. Essas fórmulas incluem entradas de propriedades, operadores e funções oferecidas pelo. AWS IoT SiteWise Para ter mais informações, consulte Usando expressões de fórmula.

Medição

As medições são propriedades de um ativo que retratam os fluxos de dados brutos da série temporal do sensor de um dispositivo ou equipamento. Para ter mais informações, consulte Definindo fluxos de dados do equipamento (medições).

Métrica

As métricas são propriedades de um ativo que representam dados agregados de séries temporais. Cada métrica é acompanhada por uma expressão matemática (fórmula) que descreve como agregar pontos de dados e um intervalo de tempo para calcular essa agregação. As métricas geram um único ponto de dados para cada intervalo de tempo especificado. Para ter mais informações, consulte Agregando dados de propriedades e outros ativos (métricas).

Pacotes

SiteWise Os gateways Edge usam pacotes para determinar como coletar, processar e rotear dados. Atualmente, AWS IoT SiteWise suporta o pacote de coleta de dados e o pacote de processamento de dados. Para obter mais informações sobre os pacotes disponíveis para seu gateway SiteWise Edge, consultethe section called “Usar pacotes”.

Pacote de coleta de dados

Use o pacote de coleta de dados para que seu gateway SiteWise Edge possa coletar seus dados industriais e roteá-los para o AWS destino de sua escolha. Esse pacote é adicionado automaticamente ao seu gateway SiteWise Edge e não pode ser removido.

Pacote de processamento de dados

Use o pacote de processamento de dados para processar seus dados na borda e mantê-los por 30 dias para uso em aplicativos locais.

Portal

Um AWS IoT SiteWise Monitor portal é um aplicativo da web que você pode usar para visualizar e compartilhar seus AWS IoT SiteWise dados. Um portal tem um ou mais administradores e contém zero ou mais projetos.

Administrador de portal

Cada portal do SiteWise Monitor tem um ou mais administradores do portal. Os administradores de portal usam-no para criar projetos que contenham coleções de ativos e painéis. Em seguida, o administrador de portal atribui ativos e proprietários a cada projeto. Ao controlar o acesso ao projeto, os administradores do portal especificam quais ativos os proprietários e visualizadores podem ver.

Projeto

Cada portal do SiteWise Monitor contém um conjunto de projetos. Cada projeto tem uma subconjunto dos seus ativos AWS IoT SiteWise associado a ele. Os proprietários do projeto criam um ou mais painéis para fornecer uma maneira consistente de visualização dos dados associados a esses ativos. Os proprietários do projeto podem convidar visualizadores para o projeto, a fim de permitir que eles visualizem os ativos e os painéis no projeto. O projeto é a unidade básica de compartilhamento dentro do SiteWise Monitor. Os proprietários do projeto podem convidar usuários que receberam acesso ao portal pelo AWS administrador. Um usuário deve ter acesso a um portal antes que um projeto do mesmo possa ser compartilhado com esse usuário.

Proprietário de projeto

Cada projeto do SiteWise Monitor tem proprietários. Proprietários de projeto criam visualizações na forma de painéis para representar dados operacionais de forma consistente. Quando os painéis estiverem prontos para compartilhar, o proprietário de projeto pode convidar visualizadores. Os proprietários de projeto também podem atribuir outros proprietários a ele. Os proprietários do projeto podem definir limites e configurações de notificação para alarmes.

Visualizador de projeto

Cada projeto do SiteWise Monitor tem espectadores. Os visualizadores do projeto podem conectar-se ao portal para visualizar os painéis criados pelos proprietários do projeto. Em cada painel, os visualizadores do projeto podem ajustar os prazos para entender melhor os dados operacionais. Os visualizadores do projeto só podem visualizar painéis nos projetos aos quais tiverem acesso. Os visualizadores do projeto podem reconhecer e adiar os alarmes.

Apelido de propriedade

Você tem a opção de criar aliases nas propriedades do ativo, como um caminho de fluxo de dados do servidor OPC-UA (por exemplo, /company/windfarm/3/turbine/7/temperature), simplificando a identificação de uma propriedade do ativo durante a ingestão ou recuperação dos dados do ativo. Quando você usa um gateway SiteWise Edge para ingerir dados de servidores, seus aliases de propriedade devem corresponder aos caminhos dos seus fluxos de dados brutos. Para ter mais informações, consulte Mapeamento de fluxos de dados industriais para propriedades de ativos.

Notificação de propriedade

Quando você ativa as notificações de propriedade para uma propriedade de ativo, AWS IoT SiteWise publica uma mensagem MQTT AWS IoT Core sempre que a propriedade recebe

um novo valor. A carga útil da mensagem inclui detalhes sobre a atualização do valor dessa propriedade. Use notificações de valor de propriedade para criar soluções que conectam seus dados industriais AWS IoT SiteWise a outros AWS serviços. Para ter mais informações, consulte Interagindo com outros serviços AWS.

SiteWise Gateway Edge

Um gateway SiteWise Edge está situado nas instalações do cliente para coletar, manipular e direcionar dados. Um gateway SiteWise Edge se conecta às suas fontes de dados industriais por meio do protocolo OPC-UA para coletar e processar dados, enviando-os para a AWS nuvem. SiteWise Os gateways Edge também podem se conectar a fontes de dados de parceiros. SiteWise Os gateways de borda usam pacotes para coleta de dados, processamento de borda e muito mais. Para obter mais informações sobre pacotes disponíveis, consulte the section called "Usar pacotes".

Você tem a flexibilidade de criar um gateway SiteWise Edge em qualquer dispositivo ou plataforma capaz de funcionar AWS IoT Greengrass. Para ter mais informações, consulte Usando gateways SiteWise Edge.

Transformação

As transformações são propriedades de um ativo que representam dados de séries temporais transformados. Cada transformação é acompanhada por uma expressão matemática (fórmula) que especifica como converter pontos de dados de um formulário para outro. Os pontos de dados transformados mantêm uma one-to-one relação com os pontos de dados de entrada. Para ter mais informações, consulte Transformando dados (transformações).

Visualização

Em cada painel, os proprietários de projeto decidem como exibir as propriedades e alarmes dos ativos associados ao projeto. A disponibilidade pode ser representada como um gráfico de linhas, enquanto outros valores podem ser exibidos como gráficos de barras ou como indicadores-chave de desempenho (KPIs). Os alarmes são melhor exibidos como grades de status e cronogramas de status. Os proprietário do projeto personalizam cada visualização para fornecer a melhor compreensão sobre os dados desse ativo.

Casos de uso para AWS IoT SiteWise

AWS IoT SiteWise é usado em uma variedade de indústrias para muitas aplicações de coleta e análise de dados industriais.

Colete dados de forma consistente de todas as suas fontes para ajudar a resolver problemas rapidamente. AWS IoT SiteWise oferece monitoramento remoto para coletar os dados diretamente no local ou coletá-los de várias fontes em várias instalações. AWS IoT SiteWise fornece a flexibilidade necessária para soluções de dados industriais de IoT.

Fabricação

AWS IoT SiteWise pode simplificar o processo de coleta e utilização de dados de seu equipamento para identificar e minimizar ineficiências, aprimorando as operações industriais. AWS IoT SiteWise ajuda você a coletar dados de linhas e equipamentos de fabricação. Com AWS IoT SiteWise isso, você pode transferir os dados para a AWS nuvem e criar métricas de desempenho para seus equipamentos e processos específicos. Você pode usar as métricas produzidas para entender a eficácia geral de suas operações e identificar oportunidades de inovação e melhoria. Você também pode visualizar seu processo de fabricação, identificar deficiências de equipamentos e processos, lacunas na produção ou defeitos do produto.

Alimentos e bebidas

As instalações da indústria de alimentos e bebidas lidam com diferentes tipos de processamento de alimentos, como moer grãos em farinha, abate e empacotamento de carne, montagem, cozimento e congelamento de refeições congeladas. As fábricas de processamento de alimentos geralmente abrangem vários locais com operadores de instalações e equipamentos em um local centralizado para monitorar processos e equipamentos. Por exemplo, as unidades de refrigeração avaliam o manuseio e a expiração dos ingredientes. Eles monitoram a criação de resíduos em todas as instalações para garantir a eficiência operacional. Com AWS IoT SiteWise, você pode agrupar fluxos de dados de sensores de vários locais por linha de produção e instalações para que seus engenheiros de processo possam entender melhor e fazer melhorias em todas as instalações.

Energia e serviços de utilidade pública

Com AWS IoT SiteWise, você pode resolver problemas de equipamento com mais facilidade e eficiência. Você pode monitorar o desempenho dos ativos remotamente e em tempo real. Acesse dados históricos do equipamento de qualquer lugar para identificar possíveis problemas, enviar recursos precisos e prevenir e corrigir problemas com mais rapidez.

Começando com AWS IoT SiteWise

Com AWS IoT SiteWise, você pode coletar, organizar, analisar e visualizar seus dados.

AWS IoT SiteWise fornece uma demonstração que você pode usar para explorar o serviço sem configurar uma fonte de dados real. Para ter mais informações, consulte Usando a AWS IoT SiteWise demonstração.

Você pode concluir os seguintes tutoriais para explorar determinados recursos do: AWS IoT SiteWise

- Ingestão de dados de coisas AWS IoT
- Visualizando e compartilhando dados de parques eólicos no Monitor SiteWise
- Publicar atualizações de valor de propriedade no Amazon DynamoDB

Consulte os tópicos a seguir para saber mais sobre AWS IoT SiteWise:

- Ingestão de dados para AWS IoT SiteWise
- Modelagem de ativos industriais
- Habilitar o processamento de dados de borda
- Monitorando dados com AWS IoT SiteWise Monitor
- Consultar dados de AWS IoT SiteWise
- Interagindo com outros serviços AWS

Tópicos

Requisitos

Você deve ter um Conta da AWS para começar AWS IoT SiteWise. Se você não tiver uma, consulte Configurando um Conta da AWS.

Use uma região onde AWS IoT SiteWise esteja disponível. Para obter mais informações, consulte AWS IoT SiteWise Endpoints e cotas. Você pode usar o seletor de região no AWS Management Console para alternar para uma dessas regiões.

Configurando um Conta da AWS

Tópicos

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

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

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e digitar um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como uma prática recomendada de segurança, atribua o acesso administrativo para um usuário e use somente o usuário-raiz para executar tarefas que requerem o acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, digite sua senha.

   Para obter ajuda ao fazer login usando o usuário-raiz, consulte Signing in as the root user (Fazer login como usuário-raiz) no Guia do usuário do Início de Sessão da AWS .
2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilitar o IAM Identity Center.

   Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .
2. No Centro de Identidade do IAM, conceda o acesso administrativo para um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com seu usuário do Centro de Identidade do IAM, use a URL de login que foi enviada ao seu endereço de e-mail quando você criou o usuário do Centro do Usuário do IAM.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso para usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

Para obter instruções, consulte Create a permission set no Guia do usuário do AWS IAM Identity Center .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Add groups no Guia do usuário do AWS IAM Identity Center .

Usando a AWS IoT SiteWise demonstração

Você pode explorar facilmente AWS IoT SiteWise usando a AWS IoT SiteWise demonstração. AWS IoT SiteWise fornece a demonstração como um AWS CloudFormation modelo que você pode implantar para criar modelos de ativos, ativos e um portal SiteWise Monitor, além de gerar dados de amostra por até uma semana.

> **Important**
>
> Depois de criar a demonstração, você começará a ser cobrado pelos recursos que essa demonstração cria e consome.

Tópicos

Criando a AWS IoT SiteWise demonstração

Você pode criar a AWS IoT SiteWise demonstração no AWS IoT SiteWise console.

> **Note**
>
> A demonstração cria funções Lambda, uma regra de CloudWatch eventos e as funções AWS Identity and Access Management (IAM) necessárias para a demonstração. Você pode ver esses recursos em seu Conta da AWS. Recomendamos que você mantenha esses recursos até terminar a demonstração. Se você excluir os recursos, a demonstração pode parar de funcionar corretamente.

Para criar a demonstração no AWS IoT SiteWise console

1. Navegue até o AWS IoT SiteWise console e encontre a SiteWise demonstração no canto superior direito da página.
2. (Opcional) Em SiteWise demonstração, altere o campo Dias para manter ativos de demonstração para especificar por quantos dias manter a demonstração antes de excluí-la.
3. (Opcional) Para criar um portal SiteWise Monitor para monitorar dados de amostra, faça o seguinte.

   > **Note**
   >
   > Você será cobrado pelos recursos do SiteWise Monitor que essa demonstração cria e consome. Para obter mais informações, consulte SiteWise Monitor nos AWS IoT SiteWise preços.

   a. Escolha Monitorar Recursos.
   b. Escolha Permissão.
   c. Escolha um perfil do IAM existente que conceda aos seus usuários do IAM federados acesso ao portal.

      > **Important**
      >
      > Seu perfil do IAM deve incluir as seguintes permissões:

```
{
    "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 obter mais informações sobre como trabalhar com o SiteWise Monitor, consulte O que é AWS IoT SiteWise Monitor? no Guia do AWS IoT SiteWise Monitor aplicativo.

4. Escolha Criar demonstração.

   A demonstração leva cerca de 3 minutos para ser criada. Se houver falha na criação da demonstração, talvez sua conta tenha permissões insuficientes. Alterne para uma conta com permissões administrativas ou use as seguintes etapas para excluir a demonstração e tente novamente:

   a. Escolha Excluir demo.

      A demonstração leva cerca de 15 minutos para ser excluída.

   b. Se a demonstração não for excluída, abra o AWS CloudFormation console, escolha a pilha chamada SiteWiseDemoAssetsIoT e escolha Excluir no canto superior direito.

   c. Se a demonstração não for excluída novamente, siga as etapas no AWS CloudFormation console para ignorar os recursos que não foram excluídos e tente novamente.

5. Depois que a demonstração for criada com êxito, você poderá explorar os ativos e dados de demonstração no console AWS IoT SiteWise.

Excluindo a demonstração AWS IoT SiteWise

A AWS IoT SiteWise demonstração é excluída após uma semana ou o número de dias que você escolheu se criou a pilha de demonstração no AWS CloudFormation console. Você pode excluir a demonstração antes se tiver terminado de usar os recursos de demonstração. Você também pode excluir a demonstração se houver falha na criação. Use as etapas a seguir para excluir a demonstração manualmente.

Para excluir a AWS IoT SiteWise demonstração

1. Navegue até o console do AWS CloudFormation.

2. Escolha IoTSiteWiseDemoAssets na lista de Pilhas.
3. Escolha Excluir.

   Quando você exclui a pilha, todos os recursos criados para a demonstração são excluídos.
4. Na caixa de diálogo de confirmação, escolha Excluir pilha.

   A pilha leva cerca de 15 minutos para ser excluída. Se houver falha na exclusão, escolha Excluir no canto superior direito novamente. Se a demonstração não for excluída novamente, siga as etapas no AWS CloudFormation console para ignorar os recursos que não foram excluídos e tente novamente.

AWS IoT SiteWise tutoriais

Bem-vindo à página de AWS IoT SiteWise tutoriais. Essa coleção crescente de tutoriais capacita você com o conhecimento e as habilidades necessárias para navegar pelas complexidades do. AWS IoT SiteWise Esses tutoriais oferecem uma variedade diversificada de tópicos básicos para atender às suas necessidades. Ao se aprofundar nos tutoriais, descubra informações valiosas sobre vários aspectos do. AWS IoT SiteWise

Cada tutorial usa um exemplo de equipamento específico. Esses tutoriais são destinados a ambientes de teste e usam nomes de empresas, modelos, ativos, propriedades fictícios e assim por diante. O objetivo é fornecer orientação geral. Os tutoriais não se destinam ao uso direto em um ambiente de produção sem uma análise e adaptação cuidadosas para atender às necessidades exclusivas de sua organização.

Tópicos

Calculando o OEE em AWS IoT SiteWise

Esse tutorial fornece um exemplo específico de como calcular a eficácia geral do equipamento (OEE) de um processo de fabricação. Como resultado, seu cálculos ou fórmulas de OEE podem ser diferentes das mostradas aqui. Em geral, a OEE é definida como `Availability * Quality * Performance`. Para saber mais sobre como calcular a OEE, consulte Eficácia geral do equipamento na Wikipédia.

Pré-requisitos

Para concluir este tutorial, você deve configurar o consumo de dados para um dispositivo que tenha os seguintes três fluxos de dados:

- `Equipment_State` – um código numérico que representa o estado da máquina, como ocioso, com falha, interrupção planejada ou operação normal.

- `Good_Count` – um fluxo de dados em que cada ponto de dados contém o número de operações bem-sucedidas desde o último ponto de dados.
- `Bad_Count` – um fluxo de dados em que cada ponto de dados contém o número de operações mal sucedidas desde o último ponto de dados.

Para configurar o consumo de dados, consulte Ingestão de dados para AWS IoT SiteWise. Se não tiver uma operação industrial disponível, você poderá escrever um script que gere e faça upload dos dados de exemplo por meio da API do AWS IoT SiteWise .

Como calcular a OEE

Neste tutorial, você criará um modelo de ativo que calcula a OEE a partir de três fluxos de entrada de dados: `Equipment_State`, `Good_Count` e `Bad_Count`. Neste exemplo, considere uma máquina de empacotamento genérica, como uma que é usada para embalar açúcar, batatas fritas ou tinta. No AWS IoT SiteWise console, crie um modelo AWS IoT SiteWise de ativo com as seguintes medidas, transformações e métricas. Em seguida, você pode criar um ativo para representar a máquina de embalagem e observar como AWS IoT SiteWise calcula o OEE.

Defina as medições a seguir para representar os fluxos de dados brutos da máquina de empacotamento.

Medições

- `Equipment_State` – um fluxo de dados (ou medição) que fornece o estado atual da máquina de empacotamento em códigos numéricos:
  - `1024` – a máquina está ociosa.
  - `1020` – uma falha, como um erro ou atraso.
  - `1000` – uma interrupção planejada.
  - `1111` – uma operação normal.
- `Good_Count` – um fluxo de dados em que cada ponto de dados contém o número de operações bem-sucedidas desde o último ponto de dados.
- `Bad_Count` – um fluxo de dados em que cada ponto de dados contém o número de operações mal sucedidas desde o último ponto de dados.

Usando o fluxo de dados de medição `Equipment_State` e os códigos que ele contém, defina as transformações a seguir (ou medições derivadas). As transformações têm uma one-to-one relação com medições brutas.

Transformações

- `Idle = eq(Equipment_State, 1024)` – um fluxo de dados transformados que contém o estado ocioso da máquina.
- `Fault = eq(Equipment_State, 1020)` – um fluxo de dados transformados que contém o estado de falha da máquina.
- `Stop = eq(Equipment_State, 1000)` – um fluxo de dados transformados que contém o estado de interrupção planejada da máquina.
- `Running = eq(Equipment_State, 1111)` – um fluxo de dados transformados que contém o estado operacional normal da máquina.

Usando as medições brutas e as medições transformadas, defina as métricas a seguir que agregam dados da máquina em intervalos de tempo especificados. Escolha o mesmo intervalo de tempo para cada métrica ao definir as métricas nesta seção.

Metrics

- `Successes = sum(Good_Count)` – o número de pacotes preenchidos com sucesso durante o intervalo de tempo especificado.
- `Failures = sum(Bad_Count)` – o número de pacotes preenchidos sem sucesso durante o intervalo de tempo especificado.
- `Idle_Time = statetime(Idle)` – o tempo total de ociosidade da máquina (em segundos) por intervalo de tempo especificado.
- `Fault_Time = statetime(Fault)` – o tempo total de falha da máquina (em segundos) por intervalo de tempo especificado.
- `Stop_Time = statetime(Stop)` – o tempo total de interrupção planejada da máquina (em segundos) por intervalo de tempo especificado.
- `Run_Time = statetime(Running)` – o tempo total de execução sem problemas da máquina (em segundos) por intervalo de tempo especificado.
- `Down_Time = Idle_Time + Fault_Time + Stop_Time` – o tempo de inatividade total da máquina (em segundos) durante o intervalo de tempo especificado, calculado como a soma dos estados da máquina diferentes de `Run_Time`.

- `Availability = Run_Time / (Run_Time + Down_Time)` – o tempo de atividade da máquina ou a porcentagem de tempo programado que a máquina está disponível para operar durante o intervalo de tempo especificado.
- `Quality = Successes / (Successes + Failures)` – a porcentagem de pacotes preenchidos com êxito da máquina durante o intervalo de tempo especificado.
- `Performance = ((Successes + Failures) / Run_Time) / Ideal_Run_Rate` – o desempenho da máquina durante o intervalo de tempo especificado como uma porcentagem da taxa de execução ideal (em segundos) para o processo.

  Por exemplo, a `Ideal_Run_Rate` pode ser 60 pacotes por minuto (1 pacote por segundo). Se a `Ideal_Run_Rate` for por minuto ou por hora, você precisará dividi-la pelo fator de conversão de unidade apropriado porque `Run_Time` está em segundos.
- `OEE = Availability * Quality * Performance` – a eficácia geral do equipamento da máquina durante o intervalo de tempo especificado Esta fórmula calcula OEE como uma fração de 1.

Ingestão de dados de coisas AWS IoT

Saiba como ingerir dados AWS IoT SiteWise de uma frota de AWS IoT coisas usando sombras de dispositivos neste tutorial. As sombras do dispositivo são objetos JSON que armazenam informações sobre o estado atual de um AWS IoT dispositivo. Para obter mais informações, consulte Device shadow service no AWS IoT Developer Guide

Depois de concluir este tutorial, você pode configurar uma operação AWS IoT SiteWise com base em AWS IoT coisas. Ao usar AWS IoT coisas, você pode integrar sua operação com outros recursos úteis do AWS IoT. Por exemplo, você pode configurar AWS IoT recursos para realizar as seguintes tarefas:

- Configure regras adicionais para transmitir dados para o AWS IoT EventsAmazon DynamoDB e outros. Serviços da AWS Para ter mais informações, consulte Regras no Guia do desenvolvedor do AWS IoT .
- Indexe, pesquise e agregue os dados do seu dispositivo com o serviço de indexação de AWS IoT frotas. Para obter mais informações, consulte Serviço de indexação de frota no AWS IoT Guia do desenvolvedor.
- Audite e proteja seus dispositivos com AWS IoT Device Defender. Para obter mais informações, consulte AWS IoT Device Defender no AWS IoT Guia do desenvolvedor.

Neste tutorial, você aprende como ingerir dados das sombras AWS IoT dos dispositivos das coisas até os ativos em. AWS IoT SiteWise Para fazer isso, você cria uma ou mais AWS IoT coisas e executa um script que atualiza a sombra do dispositivo de cada coisa com dados de uso da CPU e da memória. Use os dados de uso de CPU e memória neste tutorial para imitar dados de sensor realistas. Em seguida, você cria uma regra com uma AWS IoT SiteWise ação que envia esses dados para um ativo AWS IoT SiteWise sempre que a sombra do dispositivo de uma coisa é atualizada. Para ter mais informações, consulte Ingestão de dados usando regras AWS IoT Core.

Tópicos

Pré-requisitos

Para concluir este tutorial, você precisará do seguinte:

- Um Conta da AWS. Se você não tiver uma, consulte Configurando um Conta da AWS.
- Um computador de desenvolvimento executando WindowsmacOS,Linux,, ou Unix para acessar AWS Management Console o. Para obter mais informações, consulte Conceitos básicos sobre o AWS Management Console.
- Um usuário AWS Identity and Access Management (IAM) com permissões de administrador.
- Python3 instalado no seu computador de desenvolvimento ou instalado no dispositivo que você deseja registrar como uma AWS IoT coisa.

Etapa 1: criar uma AWS IoT política

Neste procedimento, crie uma AWS IoT política que permita que suas AWS IoT coisas acessem os recursos usados neste tutorial.

Para criar uma AWS IoT política

1. Faça login no AWS Management Console.
2. Analise as AWS regiões em AWS IoT SiteWise que há suporte. Mude para uma dessas regiões compatíveis, se necessário.
3. Navegue até o console do AWS IoT. Se um botão Connect device for exibido, escolha-o.
4. No painel de navegação à esquerda, selecione Proteção e em seguida escolha Políticas.
5. Escolha Criar.
6. Insira um nome para a AWS IoT política (por exemplo,**`SiteWiseTutorialDevicePolicy`**).
7. Em Documento de política, escolha JSON para inserir a seguinte política no formato JSON. Substitua *`region`* e *`account-id`* por sua região e seu ID da conta, como **`us-east-1`** e **`123456789012`**.

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

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

Essa política permite que seus AWS IoT dispositivos estabeleçam conexões e se comuniquem com sombras de dispositivos usando mensagens MQTT. Para obter mais informações sobre mensagens MQTT, consulte O que é MQTT? . Para interagir com as sombras do dispositivo, suas AWS IoT coisas publicam e recebem mensagens MQTT sobre tópicos que começam com. `$aws/things/thing-name/shadow/` Essa política incorpora uma variável de política conhecida como`${iot:Connection.Thing.ThingName}`. Essa variável substitui o nome da coisa conectada em cada tópico. A `iot:Connect` declaração define limitações sobre quais dispositivos podem estabelecer conexões, garantindo que a variável de política thing só possa substituir nomes começando com`SiteWiseTutorialDevice`.

Para obter mais informações, consulte Thing policy variables in the AWS IoT Developer Guide.

> **Note**
>
> Essa política se aplica a coisas cujos nomes começam com `SiteWiseTutorialDevice`. Para usar um nome diferente para as coisas, é necessário atualizar a política de acordo.

8. Escolha Create (Criar).

Etapa 2: Criando e configurando uma coisa do AWS IoT

Neste procedimento, você cria e configura qualquer AWS IoT coisa. Você pode designar seu computador de desenvolvimento como uma AWS IoT coisa. À medida que você progride, lembre-se de que os princípios que você está aprendendo aqui podem ser aplicados a projetos reais. Você tem a flexibilidade de criar e configurar AWS IoT coisas em qualquer dispositivo capaz de executar um AWS IoT SDK, incluindo AWS IoT Greengrass FreeRTOS. Para obter mais informações, consulte AWS IoT SDKs no AWS IoT Developer Guide.

Para criar e configurar qualquer AWS IoT coisa

1. Abra uma linha de comando e execute o comando a seguir a fim de criar um diretório para este tutorial.

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

2. Execute o comando a seguir a fim de criar um diretório para os certificados da coisa.

```
mkdir device1
```

Se você estiver criando coisas adicionais, incremente o número no nome do diretório de acordo para manter o controle de quais certificados pertencem a qual coisa.

3. Navegue até o console do AWS IoT.
4. No painel de navegação esquerdo, escolha Todos os dispositivos na seção Gerenciar. Então, selecione Things (Coisas).
5. Se uma caixa de diálogo You don't have any things yet (Você ainda não tem coisas), selecione Create a thing (Criar uma coisa). De outro modo, selecione Criar coisas.
6. Na página Criar coisas, escolha Criar uma única coisa e em seguida escolha Próximo.
7. Na página Especificar propriedades do item, insira um nome para o item AWS IoT (por exemplo,**`SiteWiseTutorialDevice1`**) e escolha Avançar. Se você estiver criando coisas adicionais, incremente o número no nome da coisa de acordo.

> **Important**
>
> O nome da coisa deve corresponder ao nome usado na política que você criou na Etapa 1: Criação de uma AWS IoT política. Caso contrário, seu dispositivo não conseguirá se conectar AWS IoT a.

8. Na página Configurar certificado do dispositivo - opcional, selecione Gerar automaticamente um novo certificado (recomendado) e escolha Avançar. Os certificados AWS IoT permitem identificar seus dispositivos com segurança.
9. Na página Anexar políticas ao certificado - opcional, selecione a política que você criou na Etapa 1: Criando uma AWS IoT política e escolha Criar coisa.
10. Na caixa de diálogo Baixar certificados e chaves, faça o seguinte:

    a. Selecione os links de Download (Fazer download) para fazer download do certificado, da chave pública de da chave privada da coisa. Salve todos os três arquivos no diretório criado para os certificados da coisa (por exemplo, `iot-sitewise-rule-tutorial/device1`).

    > **Important**
    >
    > Essa é a única vez que você pode fazer download do certificado e das chaves da coisa. Eles são necessário para que o dispositivo possa se conectar ao AWS IoT.

   b. Escolha o link de Download para baixar um certificado CA raiz. Salve o certificado CA em `iot-sitewise-rule-tutorial`. Recomendamos fazer download do Amazon Root CA 1.

11. Selecione Done (Concluído).

Agora você registrou AWS IoT alguma coisa no seu computador. Execute uma das próximas etapas a seguir:

- Continue com a Etapa 3: Criar um modelo de ativo de dispositivo sem criar AWS IoT coisas adicionais. É possível concluir este tutorial com somente uma coisa.
- Reputa as etapas nesta seção em outro computador ou dispositivo para criar mais coisas do AWS IoT . Para este tutorial, recomendamos que você siga esta opção para poder ingerir dados de uso de CPU e memória exclusivos de vários dispositivos.
- Reputa as etapas desta seção no mesmo dispositivo (o computador) para criar mais coisas do AWS IoT . Cada AWS IoT coisa recebe dados de uso de CPU e memória semelhantes do seu computador, então use essa abordagem para demonstrar a ingestão de dados não exclusivos de vários dispositivos.

Etapa 3: Criando um modelo de ativo de dispositivo

Neste procedimento, você cria um modelo de ativo AWS IoT SiteWise para representar seus dispositivos que transmitem dados de uso de CPU e memória. Para processar dados em ativos que representam grupos de dispositivos, os modelos de ativos impõem informações consistentes em vários ativos do mesmo tipo. Para ter mais informações, consulte Modelagem de ativos industriais.

Como criar um modelo de ativo que representa um dispositivo

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação à esquerda, selecione Modelos.
3. Escolha Criar modelo.
4. Em Detalhes do modelo, insira um nome para seu modelo. Por exemplo, **`SiteWise Tutorial Device Model`**.
5. Em Measurement definitions (Definições de medição), faça o seguinte:

   a. Em Nome, insira **`CPU Usage`**.

   b. Em Unidade, insira **`%`**.

c. Deixe o Data type (Tipo de dados) como Double (Duplo).

As propriedades de medição representam os fluxos de dados brutos de um dispositivo. Para ter mais informações, consulte Definindo fluxos de dados do equipamento (medições).

6. Selecione Adicionar medição para adicionar uma segunda propriedade de medição.
7. Na segunda linha, em Measurement definitions (Definições da medição), faça o seguinte:

   a. Em Nome, insira **`Memory Usage`**.

   b. Em Unidade, insira **`%`**.

   c. Deixe o Data type (Tipo de dados) como Double (Duplo).
8. Em Metric definitions (Definições de métrica), faça o seguinte:

   a. Em Nome, insira **`Average CPU Usage`**.

   b. Em Formula (Fórmula), insira **`avg(CPU Usage)`**. Selecione CPU Usage na lista de preenchimento automático quando ela for exibida.

   c. Em Time interval (Intervalo de tempo), insira **`5 minutes`**.

   As propriedades da métrica definem cálculos de agregação que processam todos os pontos de dados de entrada em um intervalo e produzem um único ponto de dados por intervalo. Esta propriedade da métrica calcula o uso médio da CPU de cada dispositivo a cada cinco minutos. Para ter mais informações, consulte Agregando dados de propriedades e outros ativos (métricas).
9. Selecione Adicionar métrica para adicionar uma segunda propriedade de métrica.
10. Na segunda linha, em Metric definitions (Definições de métrica), faça o seguinte:

    a. Em Nome, insira **`Average Memory Usage`**.

    b. Em Formula (Fórmula), insira **`avg(Memory Usage)`**. Selecione Memory Usage na lista de preenchimento automático quando ela for exibida.

    c. Em Time interval (Intervalo de tempo), insira **`5 minutes`**.

    Esta propriedade da métrica calcula o uso médio da memória de cada dispositivo a cada cinco minutos.
11. (Opcional) Adicione outras métricas que você esteja interessado em calcular de acordo com o dispositivo. Algumas funções interessantes incluem `min` e `max`. Para ter mais informações,

consulte Usando expressões de fórmula. Na In Etapa 4:, Criando um modelo de ativo de frota de dispositivo, você pode criar um ativo pai que pode calcular métricas usando dados de toda a sua frota de dispositivos.

12. Escolha Criar modelo.

Etapa 4: Criar um modelo de ativo de frota de dispositivos

Neste procedimento, você cria um modelo de ativo AWS IoT SiteWise para simbolizar sua coleção de dispositivos. Nesse modelo de ativos, você estabelece uma estrutura que permite vincular vários ativos de dispositivos a um ativo abrangente da frota. Depois disso, você descreve as métricas no modelo de ativos da frota para consolidar os dados de todos os ativos de dispositivos conectados. Essa abordagem fornece informações abrangentes sobre o desempenho coletivo de toda a sua frota.

Como criar um modelo de ativo que representa uma frota de dispositivos

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação à esquerda, selecione Modelos.
3. Escolha Criar modelo.
4. Em Detalhes do modelo, insira um nome para seu modelo. Por exemplo, **`SiteWise Tutorial Device Fleet Model`**.
5. Em Hierarchy definitions (Definições de hierarquia), faça o seguinte:

   a. Em Hierarchy name (Nome da hierarquia), insira **`Device`**.

   b. Em Hierarchy model (Modelo da hierarquia), escolha o modelo de ativo do dispositivo (**`SiteWise Tutorial Device Model`**).

   Uma hierarquia define uma relação entre um modelo de ativo pai (frota) e um modelo de ativo filho (dispositivo). Os ativos pai podem acessar os dados de propriedade dos ativos filhos. Ao criar ativos posteriormente, é necessário associar ativos filhos a ativos pai de acordo com uma definição de hierarquia no modelo de ativo pai. Para ter mais informações, consulte Definindo hierarquias de modelos de ativos.
6. Em Metric definitions (Definições de métrica), faça o seguinte:

   a. Em Nome, insira **`Average CPU Usage`**.

   b. Em Formula (Fórmula), insira **`avg(Device | Average CPU Usage)`**. Quando a lista de preenchimento automático for exibida, selecione Device para escolher uma hierarquia

e selecione Average CPU Usage para escolher a métrica do ativo do dispositivo criado anteriormente.

c. Em Time interval (Intervalo de tempo), insira **`5 minutes`**.

Essa propriedade da métrica calcula o uso médio da CPU de todos os ativos de dispositivo associados a um ativo de frota por meio da hierarquia **`Device`**.

7. Selecione Adicionar métrica para adicionar uma segunda propriedade de métrica.
8. Na segunda linha, em Metric definitions (Definições de métrica), faça o seguinte:

   a. Em Nome, insira **`Average Memory Usage`**.

   b. Em Formula (Fórmula), insira **`avg(Device | Average Memory Usage)`**. Quando a lista de preenchimento automático for exibida, selecione Device para escolher uma hierarquia e selecione Average Memory Usage para escolher a métrica do ativo do dispositivo criado anteriormente.

   c. Em Time interval (Intervalo de tempo), insira **`5 minutes`**.

   Essa propriedade da métrica calcula o uso médio da memória de todos os ativos de dispositivo associados a um ativo de frota por meio da hierarquia **`Device`**.
9. (Opcional) Adicione outras métricas que você esteja interessado em calcular em toda a frota de dispositivos.
10. Escolha Criar modelo.

Etapa 5: Criar e configurar um ativo de dispositivo

Neste procedimento, você gera um ativo de dispositivo baseado em seu modelo de ativo de dispositivo. Depois, defina aliases de propriedade para cada propriedade de medição. Um alias de propriedade é uma string exclusiva que identifica uma propriedade do ativo. Posteriormente, você pode identificar uma propriedade para upload de dados usando os aliases em vez do ID do ativo e do ID da propriedade. Para ter mais informações, consulte Mapeamento de fluxos de dados industriais para propriedades de ativos.

Como criar um ativo de dispositivo e definir aliases de propriedade

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação à esquerda, escolha Ativos.

3. Escolha Criar ativo.
4. Em Informações do modelo, escolha o modelo de ativo do seu dispositivo, **`SiteWise Tutorial Device Model`**.
5. Em Informações do ativo, insira um nome para seu ativo. Por exemplo, **`SiteWise Tutorial Device 1`**.
6. Escolha Criar ativo.
7. No novo ativo de dispositivo, selecione Editar.
8. Em CPU Usage, insira **`/tutorial/device/SiteWiseTutorialDevice1/cpu`** como o alias da propriedade. Você inclui o nome da AWS IoT coisa no alias da propriedade para poder ingerir dados de todos os seus dispositivos usando uma única AWS IoT regra.
9. Em Memory Usage, insira **`/tutorial/device/SiteWiseTutorialDevice1/memory`** como o alias da propriedade.
10. Selecione Salvar.

Se você criou várias AWS IoT coisas anteriormente, repita as etapas de 3 a 10 para cada dispositivo e incremente o número no nome do ativo e nos aliases da propriedade de acordo. Por exemplo, o nome de ativo do segundo dispositivo deve ser **`SiteWise Tutorial Device 2`** e os aliases de suas propriedades devem ser **`/tutorial/device/SiteWiseTutorialDevice2/cpu`** e **`/tutorial/device/SiteWiseTutorialDevice2/memory`**.

Etapa 6: Criar e configurar um ativo de frota de dispositivos

Neste procedimento, você forma um ativo de frota de dispositivos derivado do seu modelo de ativos de frota de dispositivos. Em seguida, você vincula seus ativos individuais do dispositivo ao ativo da frota. Essa associação permite que as propriedades métricas do ativo da frota compilem e analisem dados de vários dispositivos. Esses dados fornecem uma visão consolidada do desempenho coletivo de toda a frota.

Como criar um ativo de frota de dispositivos e associar ativos de dispositivo

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação à esquerda, escolha Ativos.
3. Escolha Criar ativo.
4. Em Modelo de informação, escolha o modelo de ativo da frota do dispositivo, **`SiteWise Tutorial Device Fleet Model`**.

5. Em Informações do ativo, insira um nome para seu ativo. Por exemplo, **`SiteWise Tutorial Device Fleet 1`**.
6. Escolha Criar ativo.
7. No novo ativo de frota de dispositivos, selecione Editar.
8. Em Ativos associados a esse ativo, escolha Adicionar ativo associado e faça o seguinte:
   a. Em Hierarchy (Hierarquia), selecione Device. Essa hierarquia identifica a relação hierárquica entre o dispositivo e os ativos da frota de dispositivos. Você definiu essa hierarquia no modelo de ativo de frota de dispositivos anteriormente neste tutorial.
   b. Em Asset (Ativo), selecione o ativo do dispositivo, SiteWise Tutorial Device 1.
9. (Opcional) Se você criou vários ativos de dispositivo anteriormente, repita as etapas de 8 a 10 para cada ativo de dispositivo criado.
10. Selecione Salvar.

    Agora você deve ver os ativos do dispositivo organizados como uma hierarquia.

Etapa 7: criar uma regra no AWS IoT Core para enviar dados aos ativos do dispositivo

Neste procedimento, você estabelece uma regra em AWS IoT Core. A regra foi criada para interpretar as mensagens de notificação das sombras do dispositivo e transmitir os dados para os ativos do seu dispositivo em AWS IoT SiteWise.Cada vez que a sombra do seu dispositivo é atualizada, AWS IoT envia uma mensagem MQTT. É possível criar uma regra que seja executada quando as sombras do dispositivo são alteradas com base na mensagem MQTT. Nesse caso, o objetivo é lidar com a mensagem de atualização, extrair os valores da propriedade e transmiti-los aos ativos do seu dispositivo em AWS IoT SiteWise.

Para criar uma regra com uma AWS IoT SiteWise ação

1. Navegue até o console do AWS IoT.
2. No painel de navegação à esquerda, escolha Roteamento de mensagens e Regras.
3. Selecione Criar regra.
4. Insira um nome e uma descrição para a sua regra e selecione Avançar.
5. Insira a instrução a seguir e escolha Executar.

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

Essa instrução de consulta de regra funciona, pois o serviço de sombra do dispositivo publica atualizações de sombra em `$aws/things/thingName/shadow/update/accepted`. Para obter mais informações sobre sombras de dispositivos, consulte Device shadow service no AWS IoT Developer Guide.

Na cláusula `WHERE`, essa instrução de consulta de regra usa a função `topic(3)` para obter o nome da coisa do terceiro segmento do tópico. Depois, a instrução exclui os dispositivos com nomes que não correspondem aos dos dispositivos do tutorial. Para obter mais informações sobre AWS IoT SQL, consulte a referência de AWS IoT SQL no Guia do AWS IoT desenvolvedor.

6. Em Ações de regra, escolha Enviar dados de mensagem para propriedades do ativo em AWS IoT SiteWise e faça o seguinte:

   a. Selecione By property alias (Por alias da propriedade).

   b. Em Property alias (Alias da propriedade), insira **`/tutorial/device/${topic(3)}/cpu`**.

      A `${...}` sintaxe é um modelo de substituição. AWS IoT avalia o conteúdo dentro das chaves. Esse modelo de substituição extrai o nome da coisa do tópico para criar um alias exclusivo para cada coisa. Para obter mais informações, consulte Modelos de substituição no Guia do desenvolvedor do AWS IoT .

      > **Note**
      >
      > Como uma expressão em um modelo de substituição é avaliado separadamente da instrução `SELECT`, não é possível usar um modelo de substituição para fazer referência a um alias criado usando uma cláusula `AS`. Você pode fazer referência somente às informações presentes na carga original, além das funções e dos operadores compatíveis.

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

   Os IDs de entrada identificam exclusivamente cada tentativa de entrada de valor. Se uma entrada retornar um erro, será possível encontrar o ID da entrada na saída do erro a fim de solucionar o problema. O modelo de substituição nesse ID de entrada combina o nome da coisa e o time stamp informado do dispositivo. Por exemplo, o ID da entrada resultante poderia ser `SiteWiseTutorialDevice1-cpu-1579808494`.

d. Em Time in seconds (Tempo em segundos), insira **`${floor(state.reported.timestamp)}`**.

   Esse modelo de substituição calcula o tempo em segundos do time stamp informado do dispositivo. Neste tutorial, os dispositivos informam o time stamp em segundos em horário Unix epoch como um número de ponto flutuante.

e. Em Offset in nanos - opcional, insira **`${floor((state.reported.timestamp % 1) * 1E9)}`**.

   Esse modelo de substituição calcula o deslocamento em nanossegundos do tempo em segundos convertendo a parte decimal do time stamp informado do dispositivo.

   > **Note**
   >
   > AWS IoT SiteWise requer que seus dados tenham um carimbo de data/hora atual na época do Unix. Se os dispositivos não informarem a hora com precisão, você poderá obter a hora atual no mecanismo de regras do AWS IoT com time stamp(). Essa função informa o tempo em milissegundos, portanto, é necessário atualizar os parâmetros de tempo da ação de regra para os seguintes valores:
   >
   > - Em Time in seconds (Tempo em segundos), insira **`${floor(timestamp() / 1E3)}`**.
   > - Em Offset in nanos (Deslocamento em nanossegundos), insira **`${(timestamp() % 1E3) * 1E6}`**.

f. Em Data type (Tipo de dados), selecione Double (Duplo).

   Esse tipo de dados deve corresponder ao tipo de dados da propriedade de ativo definida no modelo de ativo.

g. Em Valor, informe **`${state.reported.cpu}`**. Em modelos de substituição, use o operador **`.`** para recuperar um valor de dentro de uma estrutura JSON.

h. Selecione Add entry (Adicionar entrada) para adicionar uma nova entrada à propriedade de uso de memória e conclua as seguintes etapas novamente para essa propriedade:

   i. Selecione By property alias (Por alias da propriedade).

   ii. Em Property alias (Alias da propriedade), insira **`/tutorial/device/${topic(3)}/memory`**.

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

   iv. Em Time in seconds (Tempo em segundos), insira **`${floor(state.reported.timestamp)}`**.

   v. Em Offset in nanos - opcional, insira **`${floor((state.reported.timestamp % 1) * 1E9)}`**.

   vi. Em Data type (Tipo de dados), selecione Double (Duplo).

   vii. Em Valor, informe **`${state.reported.memory}`**.

i. Em Perfil do IAM,selecione Create new role para criar um perfil do IAM para essa ação de regra. Essa função permite enviar dados AWS IoT para propriedades em seu ativo de frota de dispositivos e sua hierarquia de ativos.

j. Forneça um nome de função e escolha Create role.

7. (Opcional) Configure uma ação de erro que pode ser usada para solucionar problemas da regra. Para ter mais informações, consulte Solucionar problemas de uma regra.

8. Escolha Próximo.

9. Revise as configurações do grupo de regras e selecione Criar para criar a regra.

Etapa 8: executar o script do cliente do dispositivo

Neste tutorial, você não está usando um dispositivo real para relatar dados. Em vez disso, você executa um script para atualizar AWS IoT a sombra do dispositivo com o uso da CPU e da memória para imitar dados reais do sensor. Para executar o script, você deve primeiro instalar Python os pacotes necessários. Neste procedimento, você instala os Python pacotes necessários e, em seguida, executa o script do cliente do dispositivo.

Como configurar e executar o script do cliente do dispositivo

1. Navegue até o console do AWS IoT.
2. Na parte inferior do painel de navegação à esquerda, selecione Settings (Configurações).
3. Salve o endpoint personalizado para uso com o script do cliente do dispositivo. Use esse endpoint para interagir com as sombras da coisa. Esse endpoint é exclusivo da conta na região atual.

   O endpoint personalizado deve ser semelhante ao exemplo a seguir.

   ```
   identifier.iot.region.amazonaws.com
   ```
4. Abra uma linha de comando e execute o comando a seguir para navegar até o diretório do tutorial criado anteriormente.

   ```
   cd iot-sitewise-rule-tutorial
   ```
5. Execute o comando a seguir para instalar o AWS IoT Device SDK for Python.

   ```
   pip3 install AWSIoTPythonSDK
   ```

   Para obter mais informações, consulte AWS IoT Device SDK for Python no Guia do desenvolvedor do AWS IoT .
6. Execute o comando a seguir para instalar o psutil, um processo entre plataformas e uma biblioteca de utilitários do sistema.

   ```
   pip3 install psutil
   ```

   Para obter mais informações, consulte psutil no Python Package Index.
7. Crie um arquivo chamado `thing_performance.py` no `iot-sitewise-rule-tutorial` diretório e copie o código Python a seguir no arquivo.

   ```
   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. Execute `thing_performance.py` na linha de comando com os seguintes parâmetros:

   - `-n`, `--thingName` – o nome da coisa, como **`SiteWiseTutorialDevice1`**.

- `-e`, `--endpoint` — Seu AWS IoT endpoint personalizado que você salvou anteriormente neste procedimento.
- `-r`, `--rootCA` — O caminho para seu certificado CA AWS IoT raiz.
- `-c`, `--cert` — O caminho para o certificado de sua AWS IoT coisa.
- `-k`, `--key` — O caminho para sua AWS IoT chave privada de certificado.
- `-d`, `--requestDelay` – (opcional) o tempo, em segundos, para esperar entre cada atualização de sombra do dispositivo. O padrão é de 1 segundo.
- `-v`, `--enableLogging` – (opcional) se esse parâmetro estiver presente, o script imprimirá mensagens de depuração do AWS IoT Device SDK for Python.

O comando deve ser semelhante ao exemplo a seguir.

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

Se você estiver executando o script para outras AWS IoT coisas, atualize o nome do item e o diretório do certificado adequadamente.

9. Tente abrir e fechar programas no dispositivo para ver como os usos da CPU e da memória mudam. O script imprime cada leitura de uso de CPU e de memória. Se o script fizer upload de dados para o serviço de sombra do dispositivo com êxito, a saída do script deverá ser semelhante ao exemplo a seguir.

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

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

10. Siga estas etapas para verificar se o script está atualizando a sombra do dispositivo:

    a. Navegue até o console do AWS IoT.

    b. No painel de navegação à esquerda, selecione Todos os dispositivos e Coisas.

c. Escolha sua coisa, SiteWiseTutorialDevice.

d. Escolha a guia Sombras do dispositivo, escolha Sombra clássica e verifique se o estado da sombra se parece com o exemplo a seguir.

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

Se o estado de sombra da sua coisa estiver vazio ou não se parecer com o exemplo anterior, verifique se o script está sendo executado e conectado com êxito AWS IoT. Se o tempo limite do script persistir ao se conectar AWS IoT, verifique se sua política de coisas está configurada de acordo com este tutorial.

11. Siga estas etapas para verificar se a ação da regra está enviando dados para o AWS IoT SiteWise:

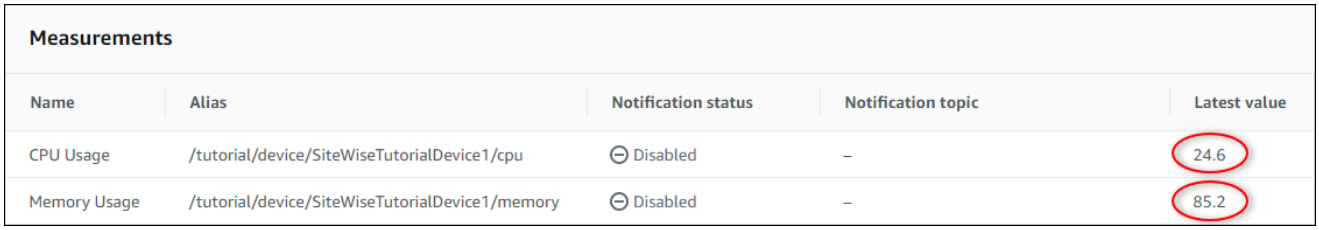
a. Navegue até o console do AWS IoT SiteWise.

b. No painel de navegação à esquerda, escolha Ativos.

c. Selecione a seta ao lado do ativo de frota de dispositivos (SiteWise Tutorial Device Fleet 1 1) para expandir sua hierarquia de ativos e selecione o ativo de dispositivo (SiteWise Tutorial Device 1).

d. Selecione Measurements (Medidas).

e. Verifique se as células de Latest value (Valor mais recente) têm valores para as propriedades CPU Usage e Memory Usage.



f. Se as propriedades CPU Usage e Memory Usage não tiverem os valores mais recentes, atualize a página. Se os valores não forem exibidos em alguns minutos, consulte Solucionar problemas de uma regra.

12. Você concluiu este tutorial. Se quiser explorar visualizações dos dados em tempo real, você poderá configurar um portal no AWS IoT SiteWise Monitor. Para ter mais informações, consulte Monitorando dados com AWS IoT SiteWise Monitor. De outro modo, pressione CTRL+C no prompt de comando para interromper o script do cliente do dispositivo. É improvável que o programa Python envie mensagens suficientes para gerar cobranças, mas é uma melhor prática interromper o programa ao concluir.

Etapa 9: limpar recursos após o tutorial

Depois de concluir o tutorial sobre a ingestão de dados de AWS IoT coisas, limpe seus recursos para evitar cobranças adicionais.

Para excluir ativos hierárquicos no AWS IoT SiteWise

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação à esquerda, escolha Ativos.
3. Ao excluir ativos em AWS IoT SiteWise, você deve primeiro desassociá-los.

   Conclua as seguintes etapas para desassociar os ativos do dispositivo do ativo da frota de dispositivos:

   a. Escolha o seu ativo de frota de dispositivos (SiteWise Tutorial Device Fleet 1).
   b. Selecione a opção Editar.
   c. Em Assets associated to this asset (Ativos associados a este ativo), selecione Disassociate (Desassociar) para cada ativo de dispositivo associado a esse ativo da frota de dispositivos.
   d. Selecione Salvar.

      Agora os ativos do dispositivo não estarão mais organizados como uma hierarquia.
4. Escolha o ativo do dispositivo (SiteWise Tutorial Device 1).
5. Escolha Delete.
6. Na caixa de diálogo de confirmação, insira **`Delete`** e selecione Delete (Excluir).
7. Repita as etapas de 4 a 6 para cada ativo de dispositivo e para o ativo da frota de dispositivos (SiteWise Tutorial Device Fleet 1).

Para excluir modelos hierárquicos de ativos no AWS IoT SiteWise

1. Navegue até o console do AWS IoT SiteWise.
2. Caso ainda não tenha feito isso, exclua o dispositivo e os ativos da frota de dispositivos. Para obter mais informações, consulte o procedimento anterior. Não é possível excluir um modelo se você tem ativos que foram criados usando esse modelo.
3. No painel de navegação à esquerda, selecione Modelos.
4. Escolha o seu modelo de ativos da frota de dispositivos (SiteWise Tutorial Device Fleet Model).

   Ao excluir modelos de ativos hierárquicos, comece excluindo primeiro o modelo de ativo principal.
5. Escolha Delete.
6. Na caixa de diálogo de confirmação, insira **`Delete`** e selecione Delete (Excluir).
7. Repita as etapas de 4 a 6 para o modelo de ativo do dispositivo (SiteWise Tutorial Device Model).

Para desativar ou excluir uma regra no AWS IoT Core

1. Navegue até o console do AWS IoT.
2. No painel de navegação à esquerda, escolha Roteamento de mensagens e Regras.
3. Selecione sua regra e escolha Excluir.
4. Na caixa de diálogo de confirmação, insira o nome da regra e selecione Delete.

Visualizando e compartilhando dados de parques eólicos no Monitor SiteWise

Este tutorial explica como usar AWS IoT SiteWise Monitor para visualizar e compartilhar dados industriais por meio de aplicativos web gerenciados, conhecidos como portais. Cada portal abrange projetos, oferecendo a flexibilidade de escolher quais dados podem ser acessados em cada projeto. Em seguida, especifique as pessoas em sua organização que podem acessar cada portal. Seus usuários acessam portais usando AWS IAM Identity Center contas, para que você possa usar seu repositório de identidades existente ou uma loja gerenciada por AWS.

Você e seus usuários com permissão suficiente podem criar painéis em cada projeto para visualizar os dados industriais de maneiras significativas. Assim, seus usuários podem visualizar esses painéis

para obter informações sobre os dados rapidamente e monitorar a operação. Você pode configurar permissões administrativas ou somente leitura para cada projeto e cada usuário na empresa. Para ter mais informações, consulte Monitorando dados com AWS IoT SiteWise Monitor.

Ao longo do tutorial, você aprimora a AWS IoT SiteWise demonstração, fornecendo um conjunto de dados de amostra para um parque eólico. Você configura um portal no SiteWise Monitor, cria um projeto e painéis para visualizar os dados do parque eólico. O tutorial também aborda a criação de usuários adicionais, juntamente com a atribuição de permissões para possuir ou visualizar o projeto e seus painéis associados.

> **Note**
>
> Ao usar o SiteWise Monitor, você é cobrado por usuário que entra em um portal (por mês). Neste tutorial, você criará três usuários, mas só precisará fazer login com um deles. Depois de concluir este tutorial, você será cobrado por um usuário. Para obter mais informações, consulte Preços do AWS IoT SiteWise.

Tópicos

Pré-requisitos

Para concluir este tutorial, você precisará do seguinte:

- Um Conta da AWS. Se você não tiver uma, consulte Configurando um Conta da AWS.
- Um computador de desenvolvimento executando WindowsmacOS,Linux,, ou Unix para acessar AWS Management Console o. Para obter mais informações, consulte Conceitos básicos sobre o AWS Management Console.

- Um usuário AWS Identity and Access Management (IAM) com permissões de administrador.
- Uma demonstração em funcionamento de um parque AWS IoT SiteWise eólico. Quando você configura a demonstração, ela define modelos e ativos AWS IoT SiteWise e transmite dados para eles para representar um parque eólico. Para ter mais informações, consulte Usando a AWS IoT SiteWise demonstração.
- Se você ativou o IAM Identity Center em sua conta, faça login na sua conta AWS Organizations de gerenciamento. Para obter mais informações, consulte Terminologia e conceitos do AWS Organizations. Se você não habilitou o Centro de identidade do IAM, você o habilitará neste tutorial e definirá sua conta como a conta de gerenciamento.

  Se você não conseguir entrar na sua conta AWS Organizations de gerenciamento, poderá concluir parcialmente o tutorial, desde que tenha um usuário do IAM Identity Center na sua organização. Nesse caso, você pode criar o portal e os painéis, mas não pode criar novos usuários do Centro de identidade do IAM para atribuir aos projetos.

Etapa 1: Criar um portal no SiteWise Monitor

Neste procedimento, você cria um portal no AWS IoT SiteWise Monitor. Cada portal é um aplicativo web gerenciado no qual você e seus usuários podem entrar com AWS IAM Identity Center contas. Com o IAM Identity Center, você pode usar o repositório de identidade existente da sua empresa ou criar um gerenciado por AWS. Os funcionários da sua empresa podem se inscrever sem criar uma conta separada Contas da AWS.

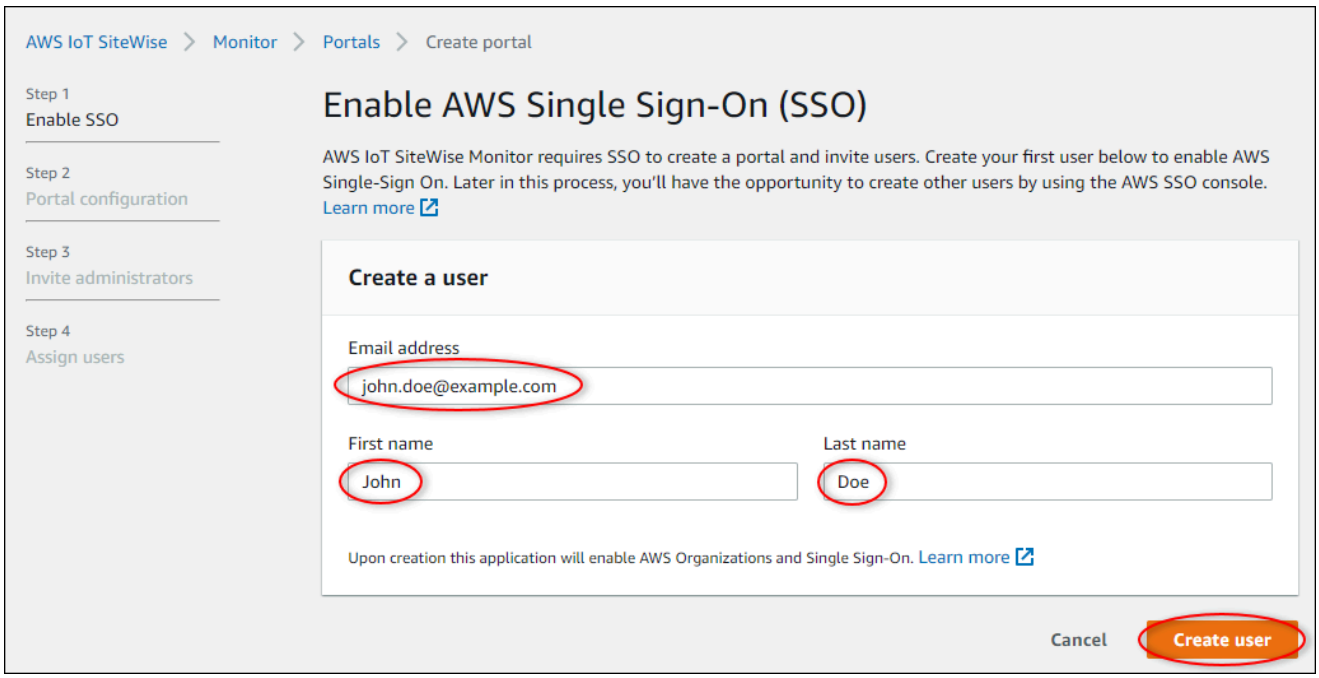
Como criar um portal

1. Faça login no AWS IoT SiteWise console.
2. Analise os AWS IoT SiteWise endpoints e as cotas em que AWS IoT SiteWise há suporte e troque de região, se necessário. Você deve executar a AWS IoT SiteWise demonstração na mesma região.
3. No painel de navegação à esquerda, escolha Portais.
4. Escolha Criar portal.
5. Se você já habilitou o Centro de identidade do IAM, pule para a etapa 6. Caso contrário, execute as etapas a seguir para habilitar o Centro de identidade do IAM:

   a. Na página Habilitar AWS IAM Identity Center (SSO), insira seu endereço de e-mail, nome e sobrenome para criar um usuário do IAM Identity Center para você mesmo ser o

administrador do portal. Use um endereço de e-mail que você possa acessar para receber um e-mail de definição de senha para seu novo usuário do Centro de identidade do IAM.

Em um portal, o administrador do portal cria projetos e atribui usuários a projetos. É possível criar mais usuários posteriormente.



b. Selecione Criar usuário.

6. Na página Configuração do portal, conclua as seguintes etapas:

   a. Insira um nome para o portal, como **`WindFarmPortal`**.

   b. (Opcional) Insira uma descrição para o portal. Se você tiver vários portais, use descrições significativas para controlar o que cada portal contém.

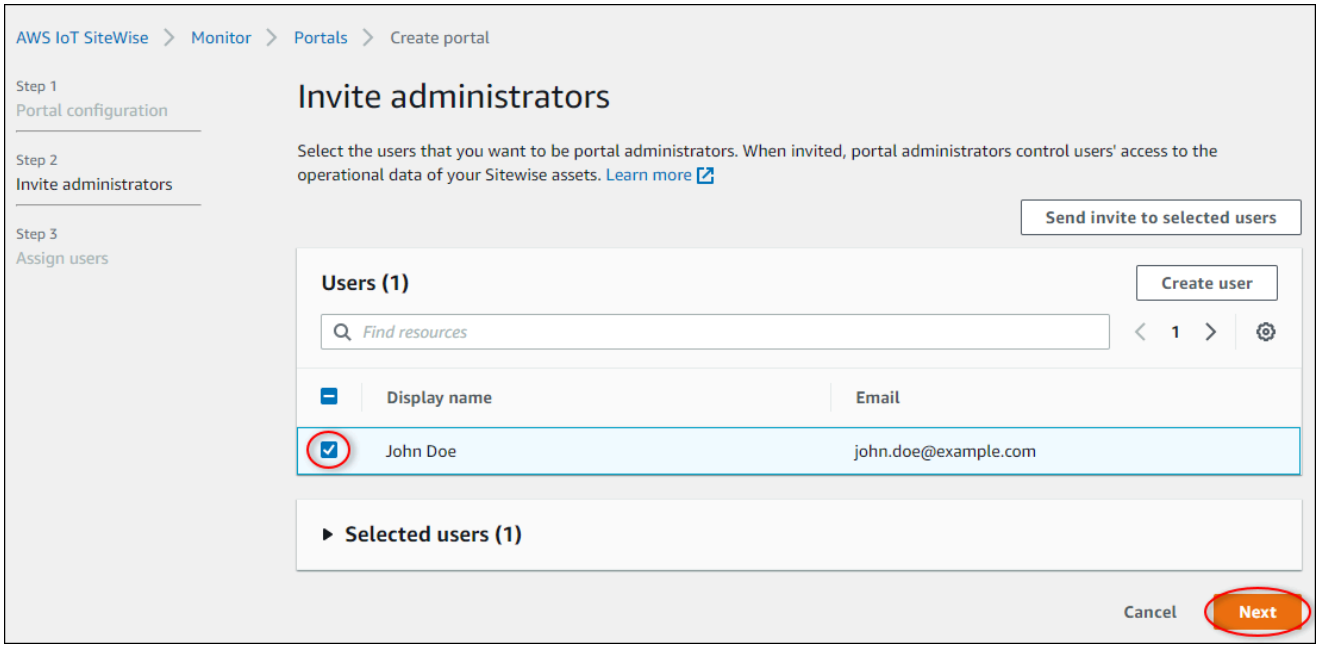
   c. (Opcional) Faça upload de uma imagem para exibir no portal.

   d. Insira um endereço de e-mail que os usuários do portal possam contatar quando tiverem um problema com o portal e precisarem da ajuda do AWS administrador da sua empresa para resolvê-lo.

   e. Escolha Criar portal.

7. Na página Convidar administradores, você pode atribuir usuários do Centro de identidade do IAM ao portal como administradores. Os administradores do portal gerenciam permissões e projetos em um portal. Nesta página, faça o seguinte:

   a. Selecione um usuário para ser o administrador do portal. Se você ativou o Centro de identidade do IAM no início deste tutorial, selecione o usuário que você criou.



b. (Opcional) Escolha Enviar convite para os usuários selecionados. Seu cliente de e-mail será aberto e um convite aparecerá no corpo da mensagem. É possível personalizar o e-mail antes de enviá-lo para os administradores do portal. Também é possível enviar o e-mail para os administradores do portal mais tarde. Se você estiver testando o SiteWise Monitor pela primeira vez e for o administrador do portal, não precisará enviar um e-mail para si mesmo.

c. Escolha Próximo.

8. Na página Atribuir usuários, você pode atribuir usuários do Centro de identidade do IAM ao portal. Posteriormente, os administradores do portal atribuem esses usuários como proprietários ou visualizadores do projeto. Os proprietários do projeto podem criar painéis nos projetos. Os visualizadores do projeto têm acesso somente para leitura aos projetos atribuídos a eles. Nesta página, você pode criar usuários do Centro de identidade do IAM para adicionar ao portal.

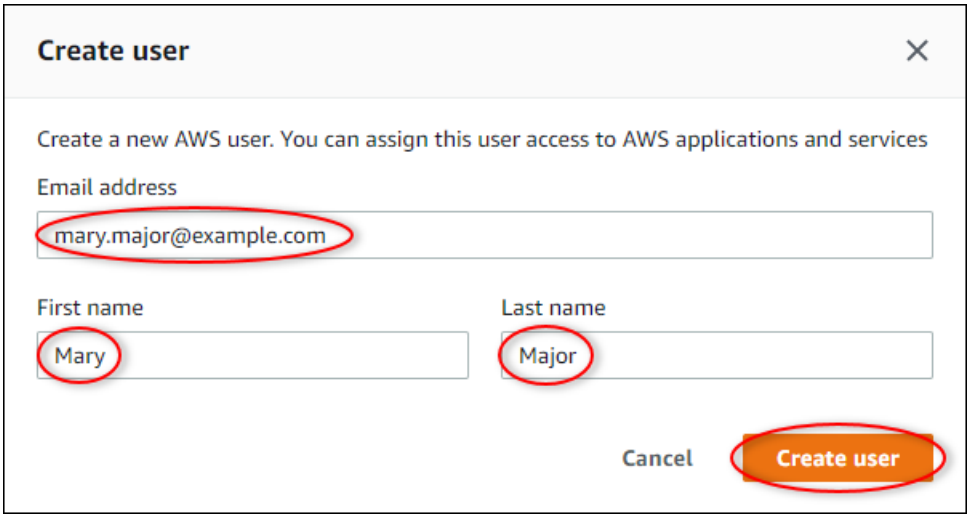
> **Note**
>
> Se você não estiver conectado à sua conta AWS Organizations de gerenciamento, não poderá criar usuários do IAM Identity Center. Escolha Atribuir usuários para criar o portal sem usuários do portal e, então, pule esta etapa.

Nesta página, faça o seguinte:

a. Realize duas vezes as etapas a seguir para criar dois usuários do Centro de identidade do IAM:

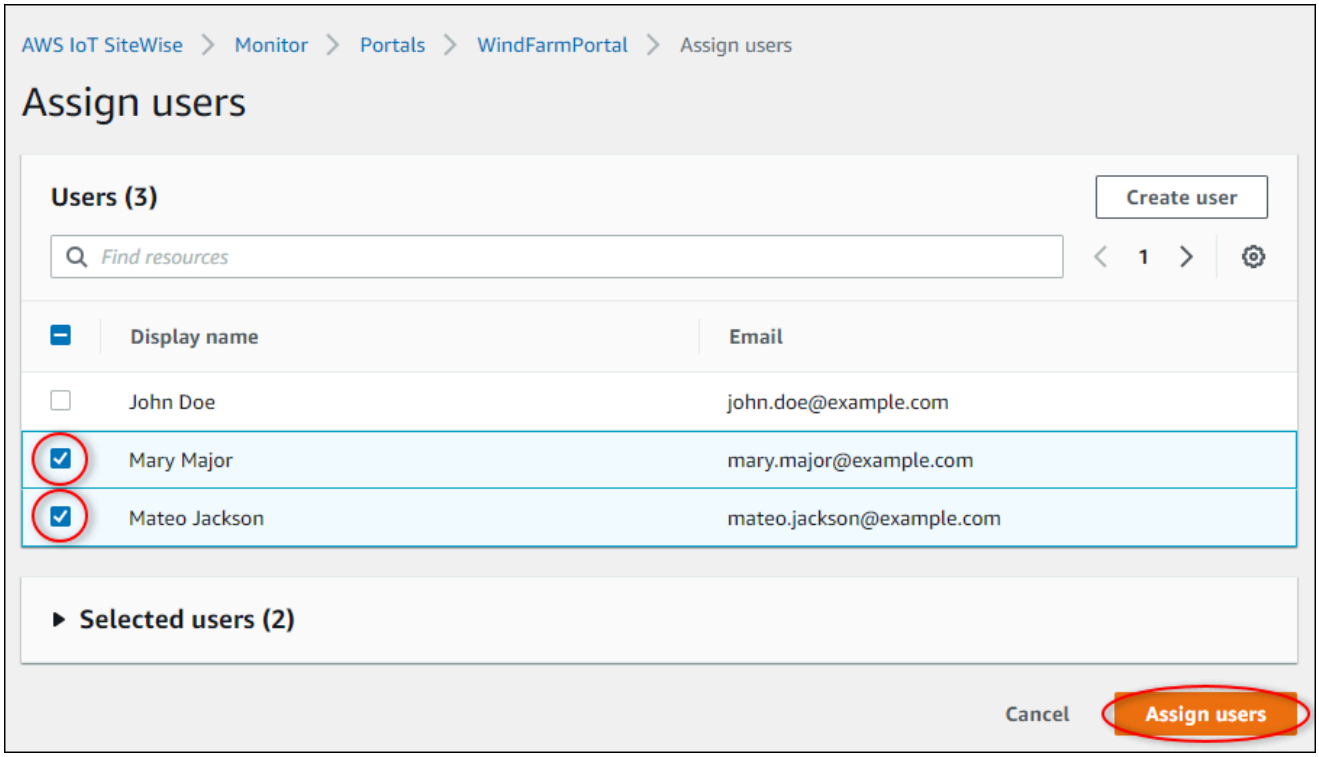
   i. Escolha Criar usuário para abrir uma caixa de diálogo onde você insere detalhes do novo usuário.

   ii. Insira o Endereço de e-mail, Nome e Sobrenome do novo usuário. O Centro de identidade do IAM envia ao usuário um e-mail para que ele defina sua senha. Se você quiser fazer login no portal como esses usuários, escolha um endereço de e-mail que você possa acessar. Cada endereço de e-mail deve ser exclusivo. Seus usuários fazem login no portal usando seus endereços de e-mail como nome de usuário.



   iii. Selecione Criar usuário.

b. Selecione os dois usuários do Centro de Identidade do IAM que você criou na etapa anterior.



c. Escolha Atribuir usuários para adicionar esses usuários ao portal.

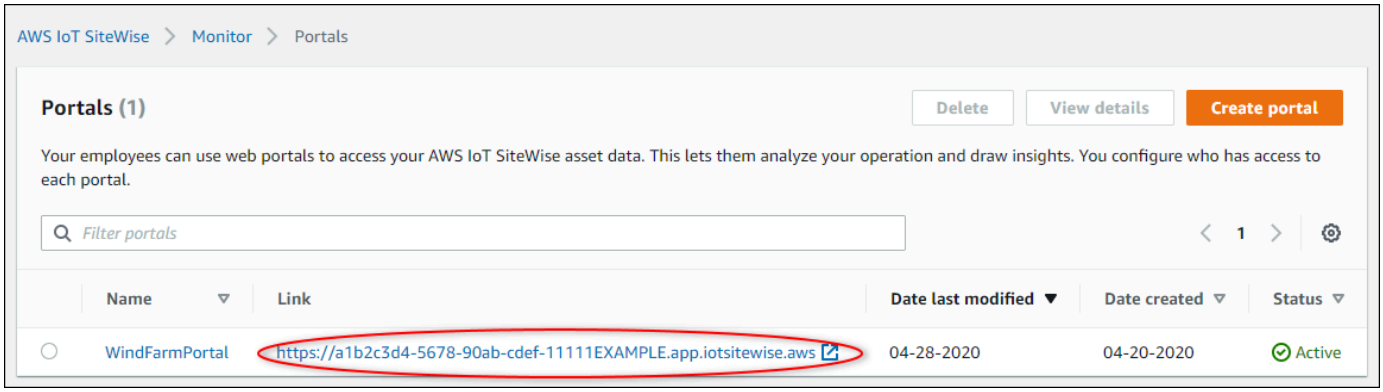
A página de portais é aberta com seu novo portal listado.

Etapa 2: Entrar em um portal

Neste procedimento, você entra no seu novo portal utilizando o AWS IAM Identity Center usuário que você adicionou no portal.

Como fazer login em um portal

1. Na página Portais, escolha o Link do seu novo portal para abri-lo em uma nova guia.



2. Se você criou seu primeiro usuário do Centro de Identidade do IAM anteriormente no tutorial, use as seguintes etapas para criar uma senha para seu usuário:

   a. Procure o e-mail com a linha de assunto Invitation to join AWS IAM Identity Center.

   b. Abra esse e-mail de convite e escolha Accept invitation.

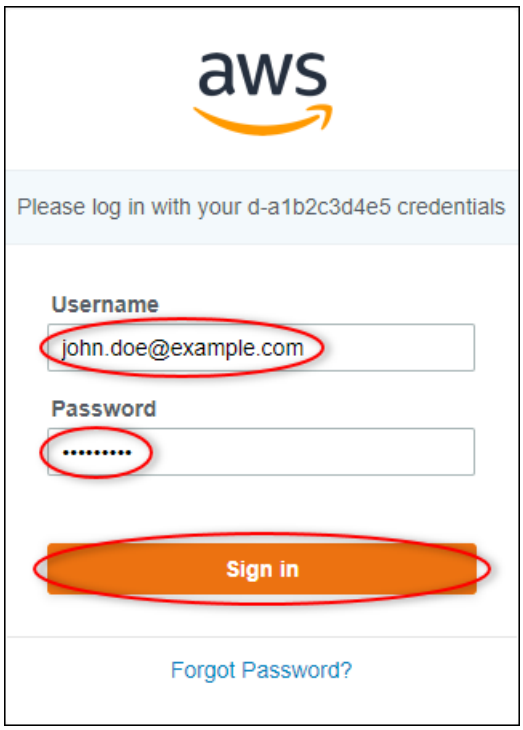
   c. Na nova janela, defina uma senha para o usuário do Centro de Identidade do IAM.

   Se quiser fazer login mais tarde no portal como o segundo e o terceiro usuários do Centro de identidade do IAM que você criou anteriormente, você também pode realizar essas etapas para definir senhas para esses usuários.

   > **Note**
   >
   > Caso não tenha recebido um e-mail, você pode gerar uma senha para seu usuário no console do Centro de Identidade do IAM. Para obter mais informações, consulte Redefinir uma senha no Guia do usuário do AWS IAM Identity Center .

3. Entre no seu Centro de identidade do IAM Username e Password. Se você criou o Centro de identidade do IAM anteriormente neste tutorial, seu Username é o endereço de e-mail do usuário administrador do portal que você criou.

   Todos os usuários do portal, incluindo o administrador do portal, devem fazer login com suas credenciais de usuário do Centro de identidade do IAM. Essas credenciais normalmente não são as mesmas que as usadas para entrar no AWS Management Console.



4. Selecione Sign in.

   O portal é aberto.

Etapa 3: criar um projeto de parque eólico

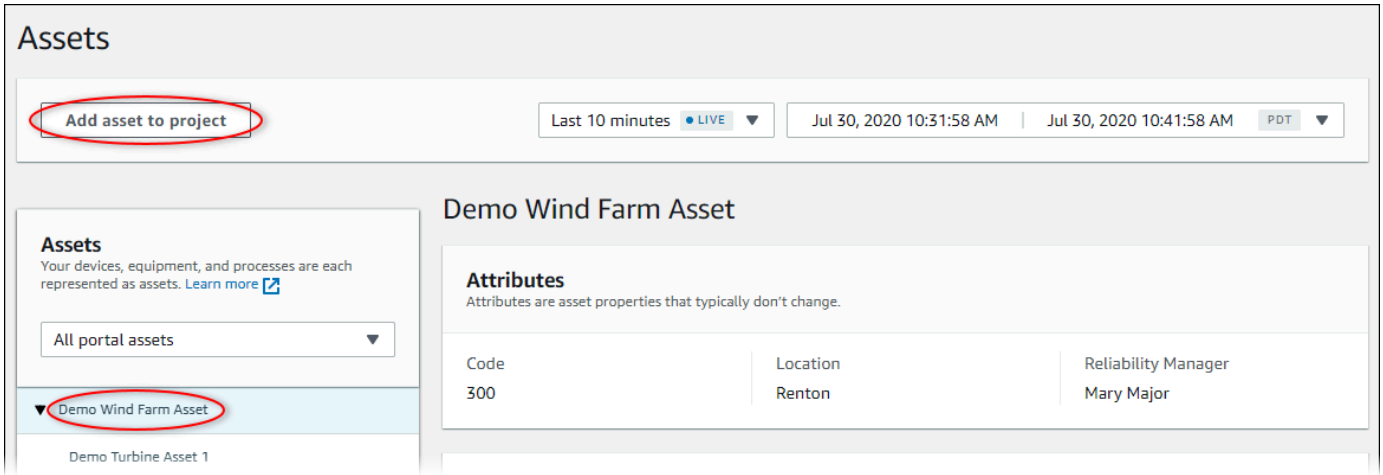
Neste procedimento, você cria um projeto em seu portal. Projetos são recursos que definem um conjunto de permissões, ativos e painéis, que você pode configurar para visualizar dados de ativos nesse projeto. Com projetos, você define quem tem acesso a quais subconjuntos da operação e como os dados desses subconjuntos são visualizados. É possível atribuir usuários do portal como proprietários ou visualizadores de cada projeto. Os proprietários do projeto podem criar painéis para visualizar e compartilhar o projeto com outros usuários. Os visualizadores do projeto podem visualizar painéis, mas não editá-los. Para obter mais informações sobre funções no SiteWise Monitor, consulteSiteWise Monitore as funções.

Como criar um projeto de parque de energia eólica

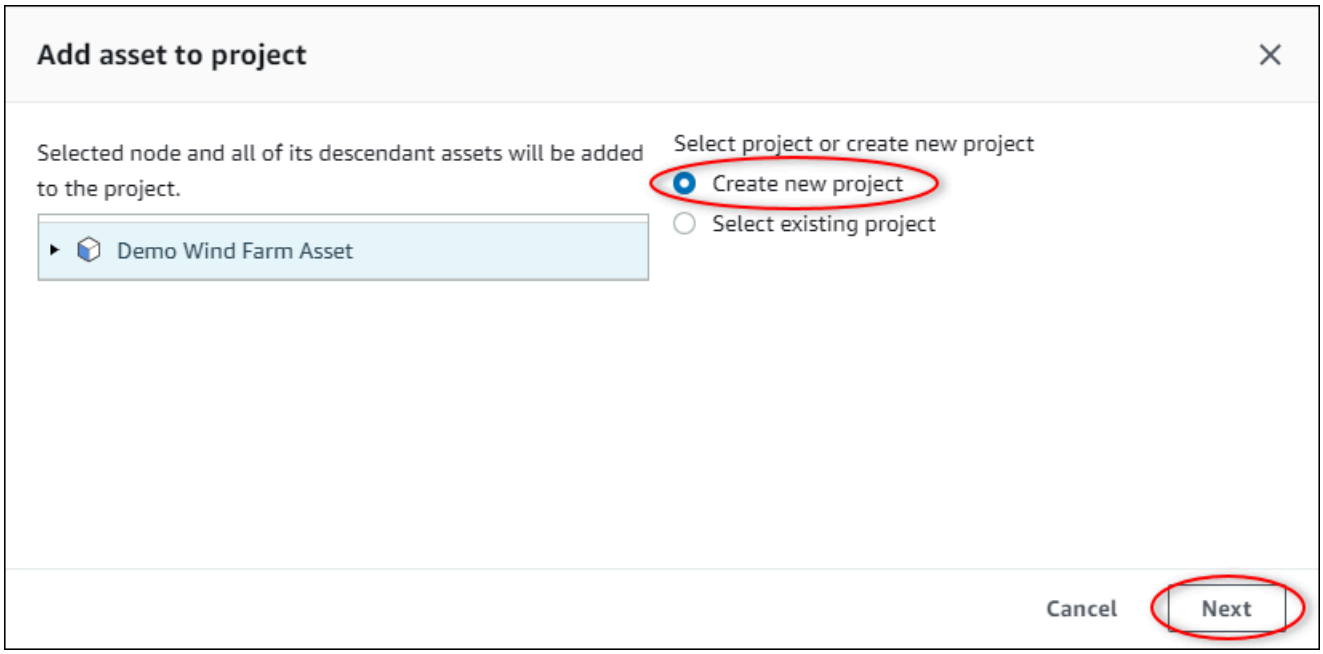
1. No painel de navegação à esquerda do portal, escolha a guia Ativos. Na página de Ativos, você pode explorar todos os ativos disponíveis no portal e adicionar ativos aos projetos.

2. No navegador de ativos, escolha Demo Wind Farm Asset. Ao escolher um ativo, você pode explorar os dados reais e históricos desse ativo. Você também pode pressionar Shift para selecionar vários ativos e comparar seus dados side-by-side.

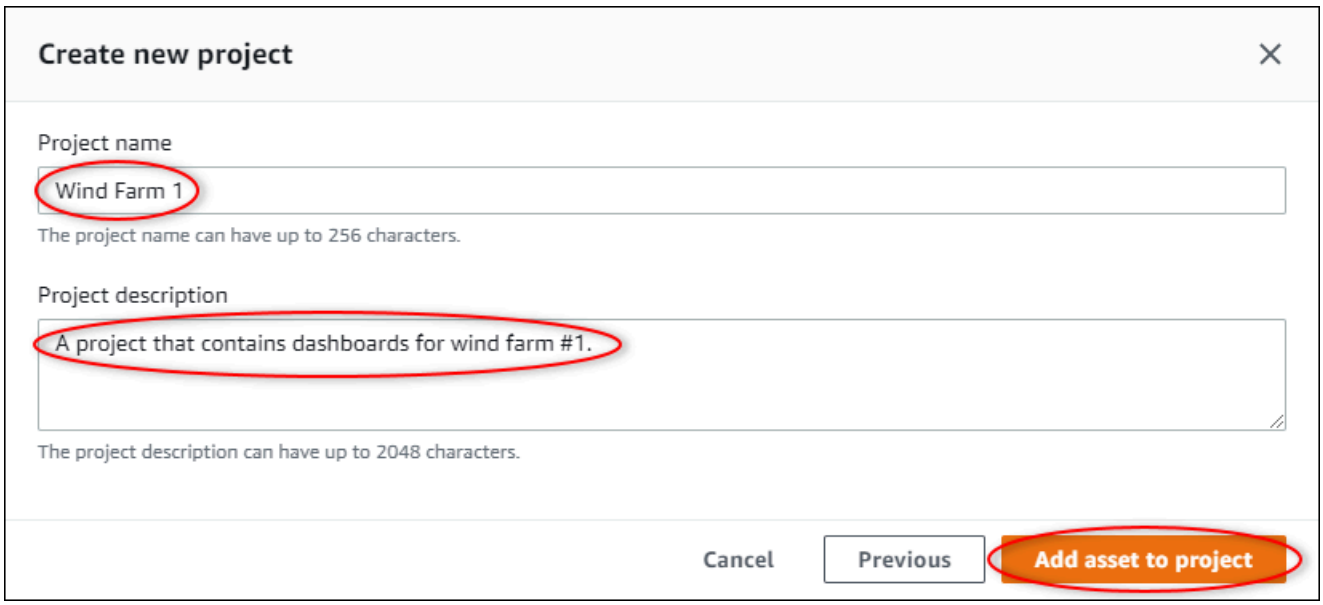
3. Escolha Adicionar ativo ao projeto no canto superior esquerdo. Os projetos contêm painéis que os usuários do portal podem visualizar para explorar os dados. Cada projeto tem acesso a um subconjunto de seus ativos em AWS IoT SiteWise. Quando você adiciona um ativo a um projeto, todos os usuários com acesso a esse projeto também podem acessar os dados desse ativo e seus filhos.



4. Na caixa de diálogo Adicionar ativo ao projeto, selecione Criar novo projeto, e então Avançar.



5. Na caixa de diálogo Criar novo projeto, insira um Nome de projeto e uma Descrição do projeto para o projeto e escolha Adicionar ativo ao projeto.



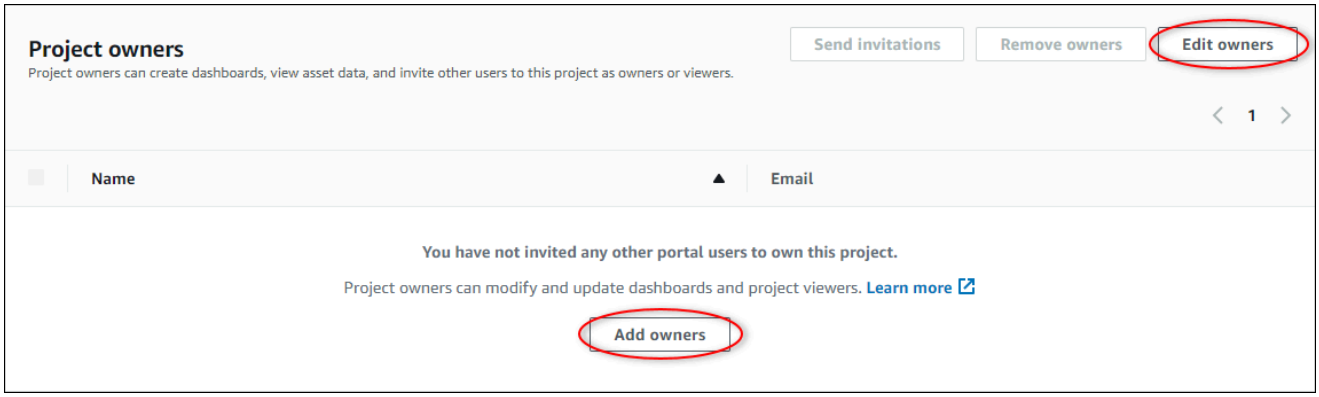
A página do seu novo projeto é aberta.

6. Na página do projeto, você pode adicionar usuários do portal como proprietários ou visualizadores do projeto.

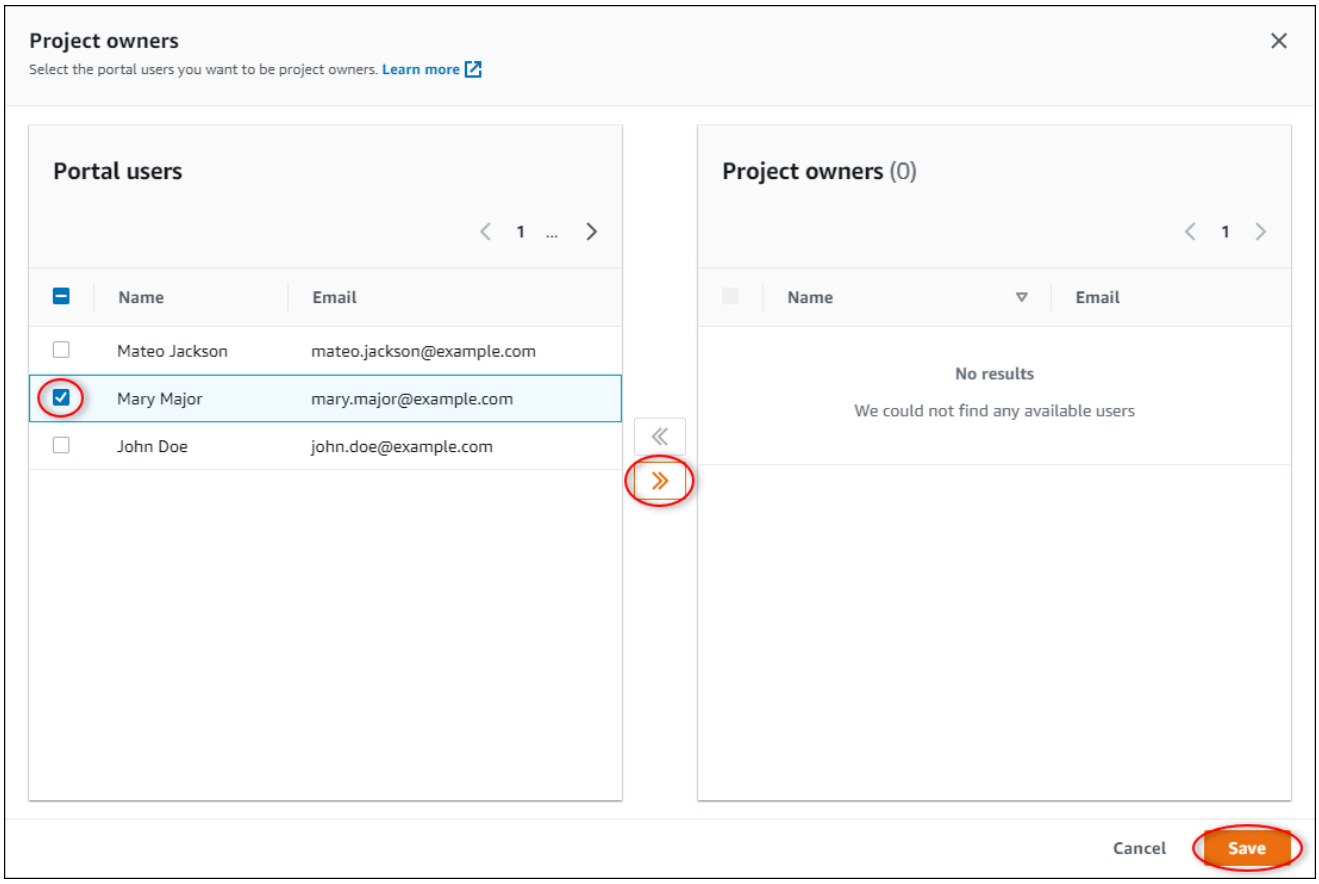
> **Note**
>
> Se você não estiver conectado à sua conta AWS Organizations de gerenciamento, talvez você não tenha usuários do portal para atribuir a este projeto, então você pode pular esta etapa.

Nesta página, faça o seguinte:

a. Em Proprietários do projeto, escolha Adicionar proprietários ou Editar usuários.



b. Escolha o usuário a ser adicionado como proprietário do projeto (por exemplo, Mary Major) e selecione o ícone **>>** .



c. Escolha Salvar.

Seu usuário do Centro de identidade do IAM Mary Major pode fazer login neste portal para editar os painéis neste projeto e compartilhar esse projeto com outros usuários do portal.

d. Em Visualizadores do projeto, escolha Adicionar visualizadores ou Editar usuários.

e. Escolha o usuário a ser adicionado como visualizador do projeto (por exemplo, Mateo Jackson) e selecione o ícone **>>** .

f. Escolha Salvar.

Seu outro usuário do Centro de identidade do IAM Mateo Jackson pode fazer login neste portal para visualizar, mas não editar, os painéis no projeto do parque de energia eólica.

Etapa 4: criar um painel para visualizar os dados do parque eólico

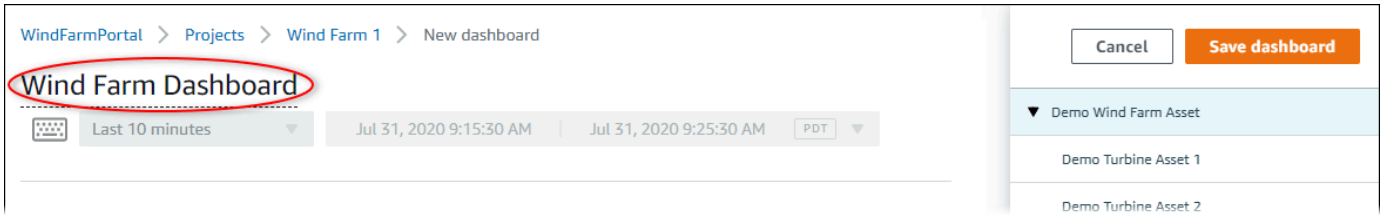
Neste procedimento, você cria painéis para visualizar os dados de demonstração do parque de energia eólica. Os painéis contêm visualizações personalizáveis dos dados de ativos do seu projeto. Cada visualização pode ter um tipo diferente, como gráfico de linhas, gráfico de barras ou exibição de indicadores-chave de desempenho (KPI). Você pode escolher o tipo de visualização que funciona melhor para seus dados. Os proprietários do projeto podem editar painéis, enquanto os visualizadores do projeto só podem visualizar os painéis para obter informações.

Como criar um painel com visualizações

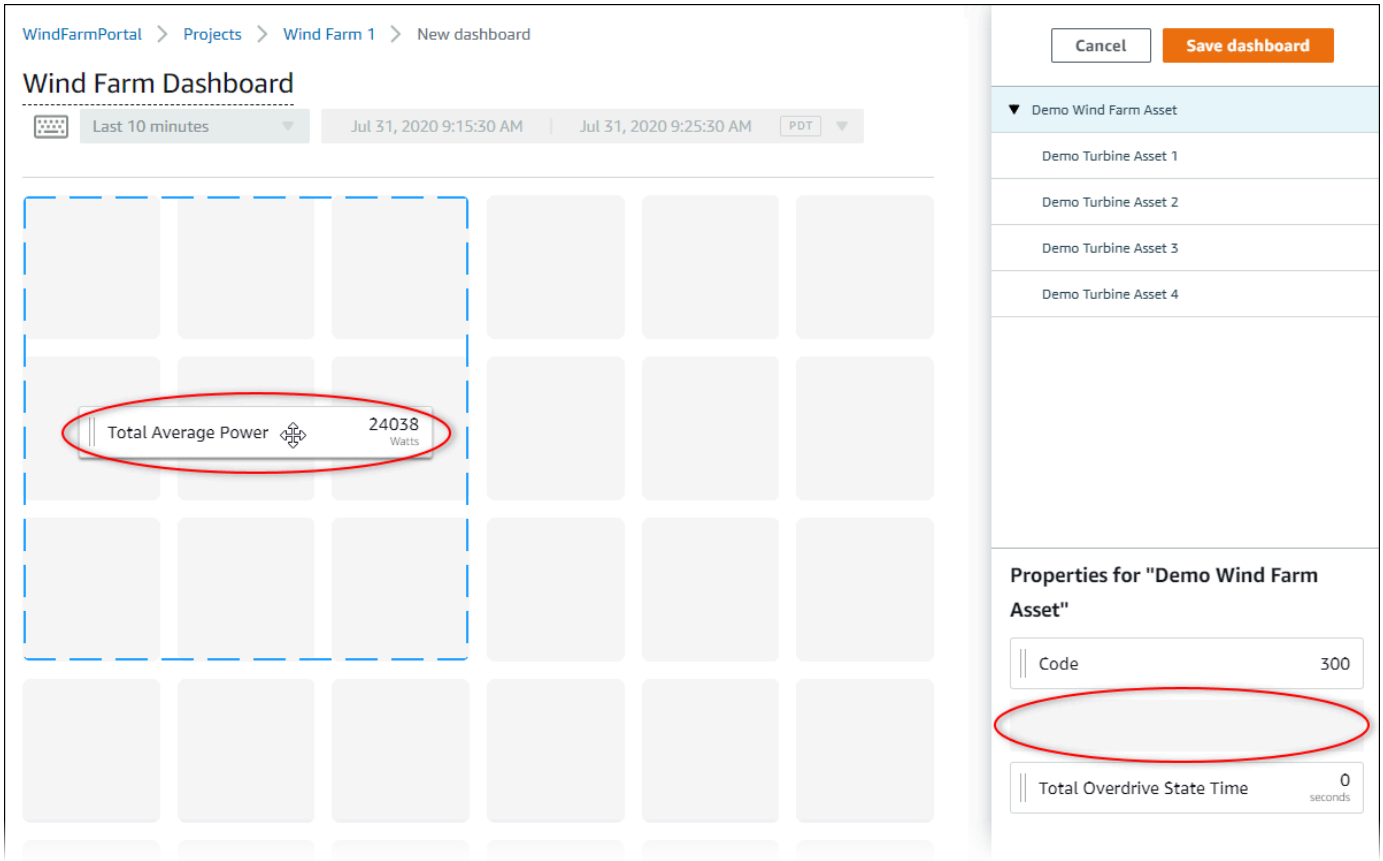
1. Na página do seu novo projeto, escolha Criar painel para criar um painel e abrir sua página de edição.

   Na página de edição de um painel, você pode arrastar as propriedades do ativo da hierarquia de ativos para o painel a fim de criar visualizações. Então, você pode editar o título, os títulos das legendas, o tipo, o tamanho e o local de cada visualização no painel.

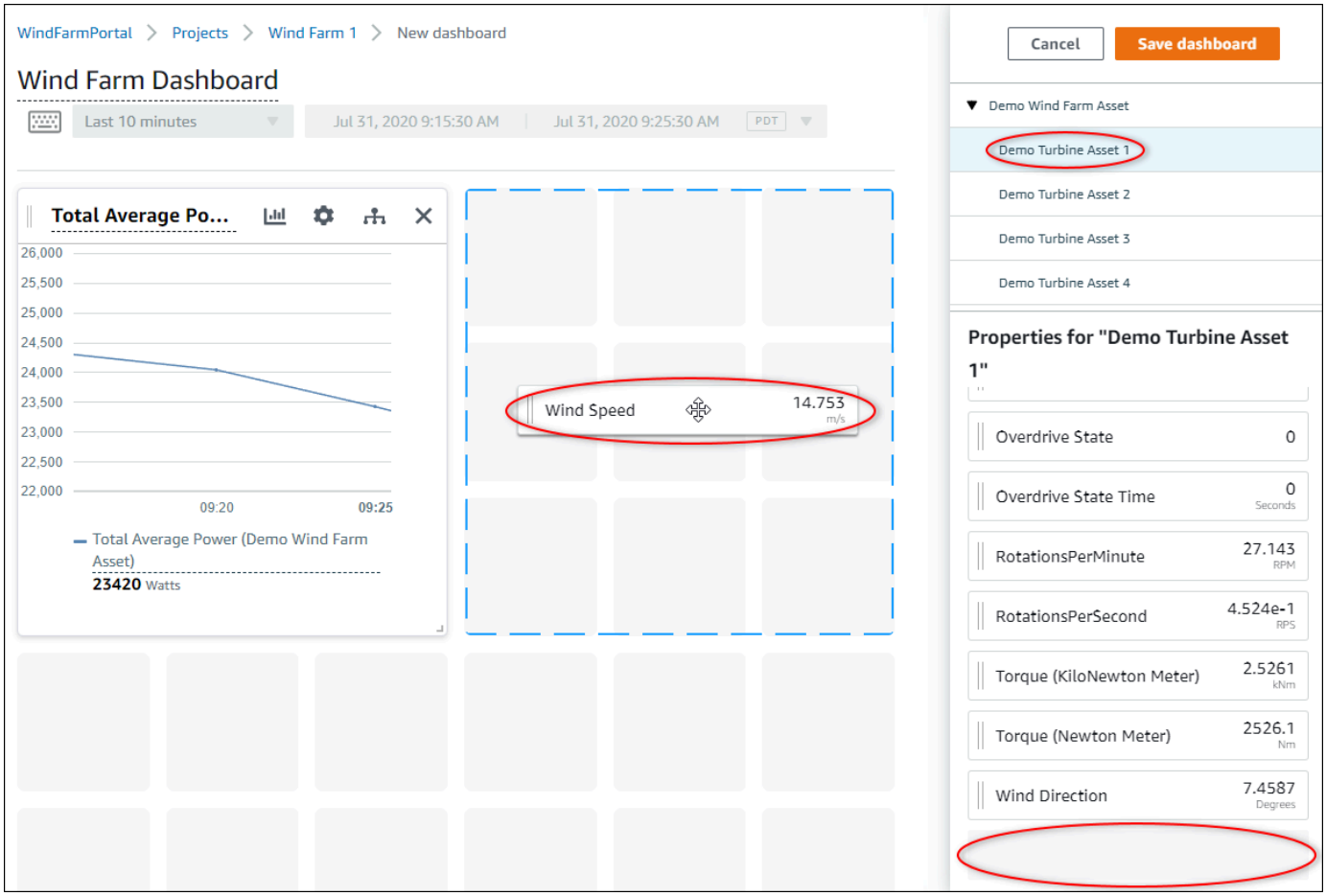
2. Insira um nome para seu painel.



3. Arraste Total Average Power do Demo Wind Farm Asset para o painel para criar uma visualização.

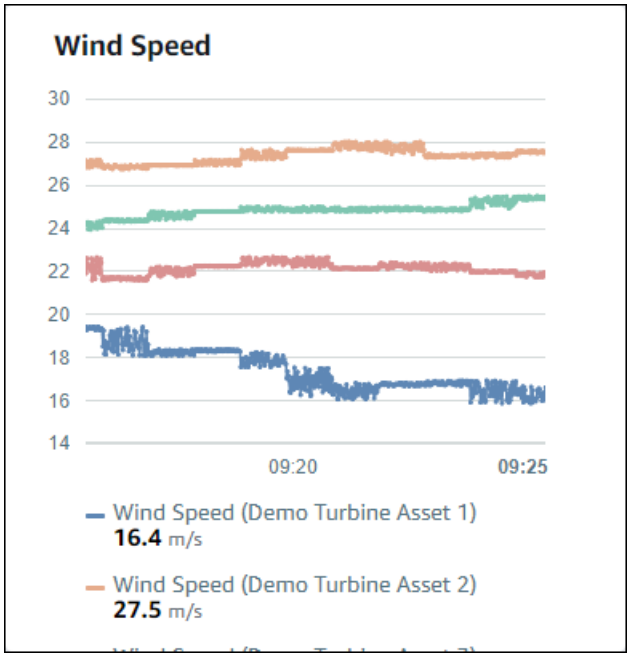


4. Escolha Demo Turbine Asset 1 mostrar as propriedades desse ativo e, em seguida, arraste Wind Speed até o painel para criar uma visualização da velocidade do vento.

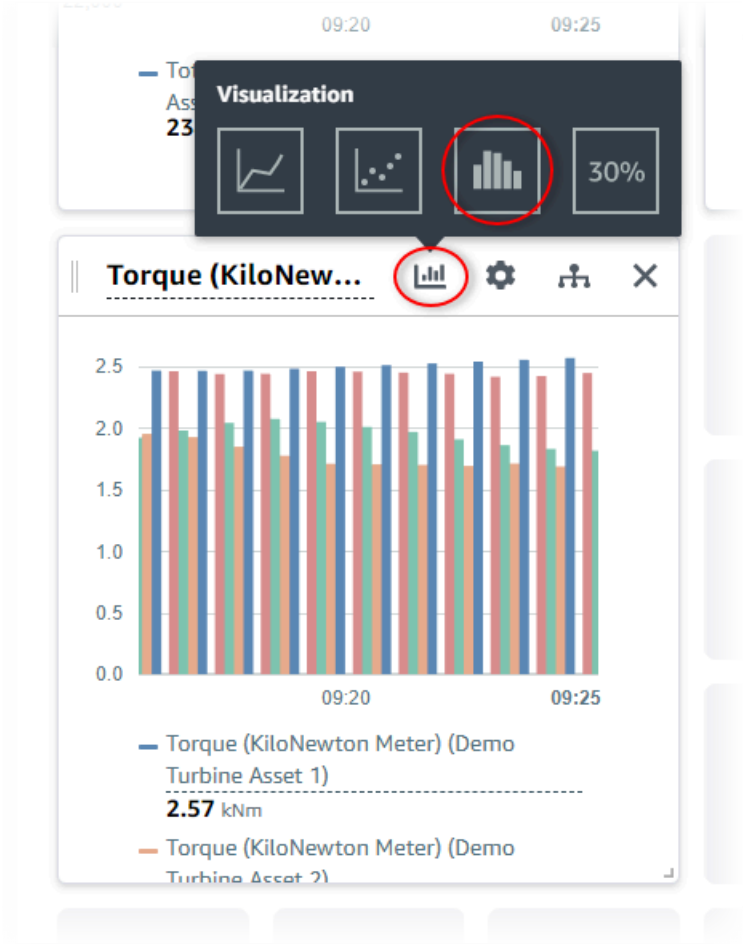


5. Adicione Wind Speed à nova visualização da velocidade do vento para cada Demo Turbine Asset 2, 3, e 4 (nessa ordem).

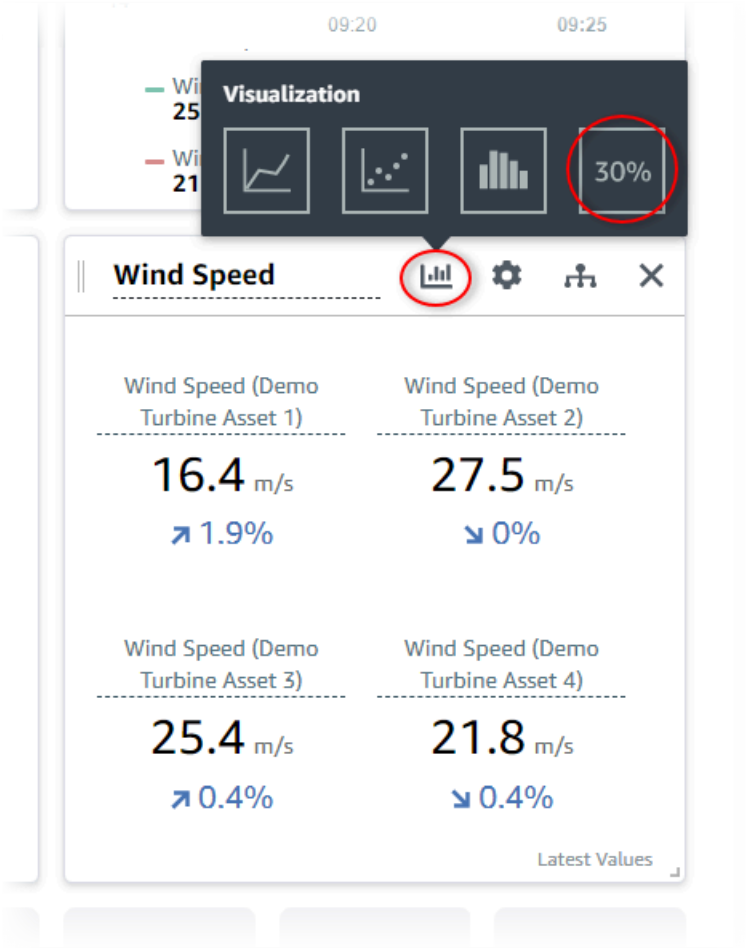
   Sua visualização de Wind Speed deve ser semelhante à imagem a seguir.



6. Repita as etapas 4 e 5 para as propriedades de Torque (KiloNewton Meter) das turbinas eólicas a fim de criar uma visualização do torque da turbina eólica.
7. Escolha o ícone de tipo de visualização para a visualização Torque (KiloNewton Meter) e selecione o ícone de gráfico de barras.

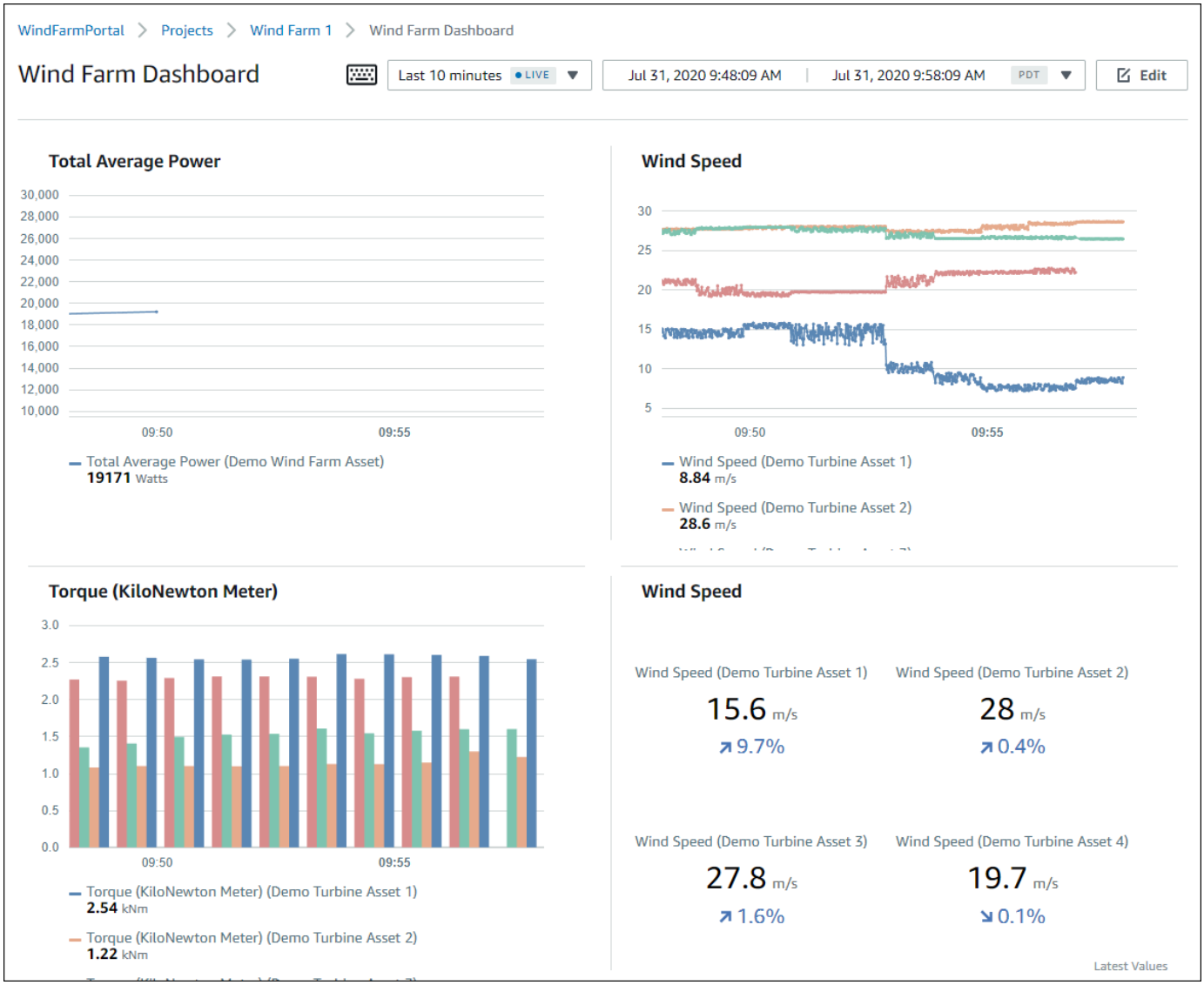


8. Repita as etapas 4 e 5 para as propriedades de Wind Direction das turbinas eólicas a fim de criar uma visualização da direção do vento.
9. Escolha o ícone de tipo de visualização para a visualização Wind Direction e selecione o ícone de gráficos de KPI (30%).



10. (Opcional) Faça outras alterações no título, nos títulos das legendas, no tipo, no tamanho e no local de cada visualização, conforme necessário.
11. Escolha Salvar painel no canto superior direito para salvar seu painel.

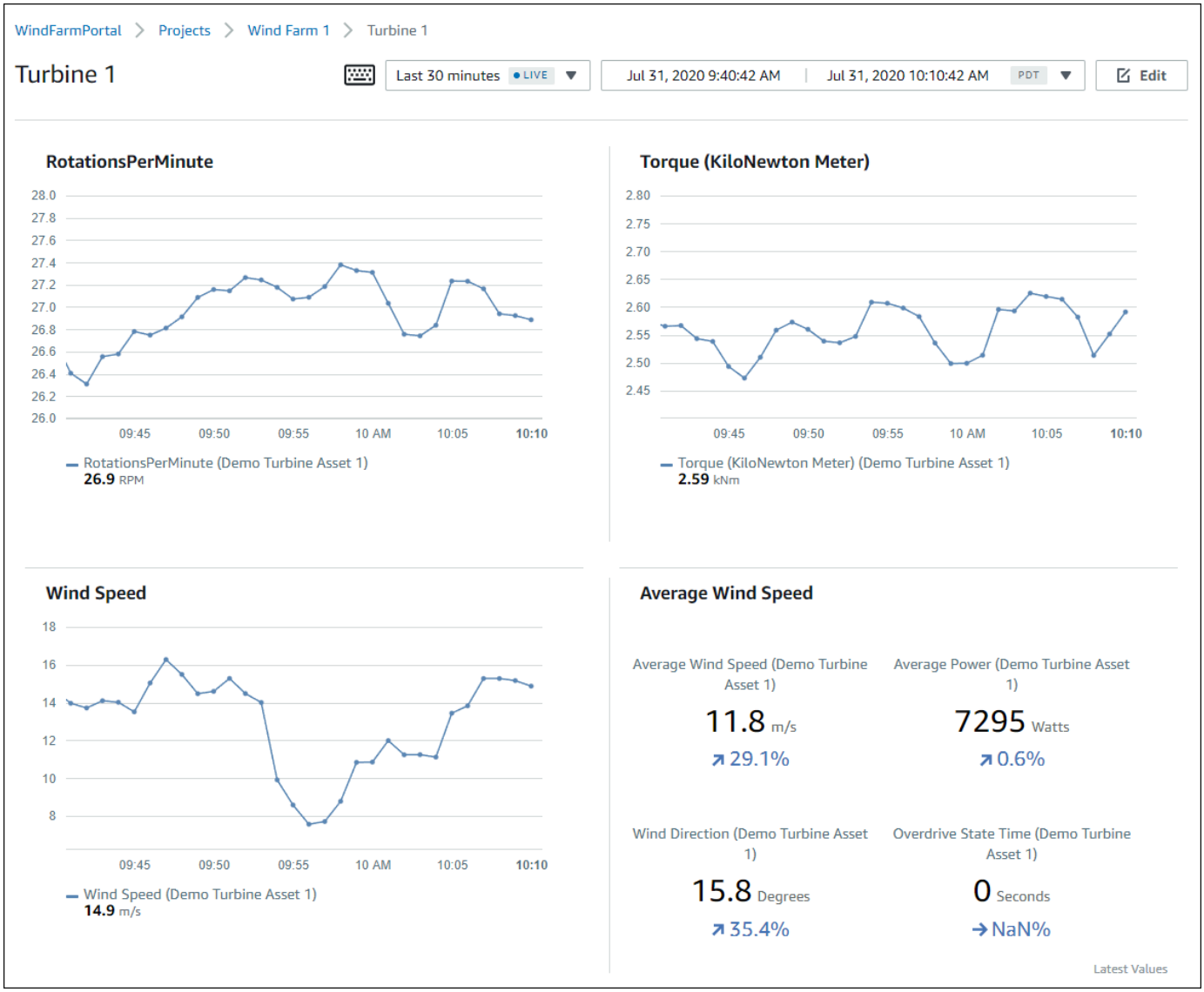
    Seu painel deve ser semelhante à imagem a seguir.



12. (Opcional) Crie um painel adicional para cada ativo de turbina eólica.

    Como uma das melhores práticas, recomendamos que você crie um painel para cada ativo com o intuito de permitir que os visualizadores investiguem quaisquer problemas em cada ativo individual. Você só pode adicionar até 5 ativos a cada visualização, portanto, você deve criar vários painéis para seus ativos hierárquicos em muitos cenários.

    Um painel para uma demonstração de turbina eólica pode ser semelhante à imagem a seguir.



13. (Opcional) Altere a linha do tempo ou selecione pontos de dados em uma visualização para explorar os dados em seu painel. Para obter mais informações, consulte Visualização de painéis no Guia do aplicativo do AWS IoT SiteWise Monitor .

Etapa 5: Explore o portal

Neste procedimento, você pode explorar o portal como um usuário com menos permissões do que um administrador do AWS IoT SiteWise portal.

Para explorar o portal e finalizar o tutorial

- (Opcional) Se você adicionou outros usuários ao projeto como proprietários ou visualizadores, você pode fazer o login no portal como esses usuários. Isso permite que você explore o portal como um usuário com menos permissões do que um administrador do portal.

  > **Important**
  >
  > Você é cobrado por cada usuário que faz login em um portal. Para obter mais informações, consulte Preços do AWS IoT SiteWise.

  Para explorar o portal como outros usuários, faça o seguinte:

  a. Escolha Fazer logout na parte inferior esquerda do portal para sair da aplicação web.

  b. Escolha Sair no canto superior direito do portal do aplicativo Centro de identidade do IAM para sair do seu usuário do Centro de identidade do IAM.

  c. Faça login no portal como o usuário do Centro de identidade do IAM que você atribuiu como proprietário do projeto ou visualizador do projeto. Para ter mais informações, consulte Etapa 2: Entrar em um portal.

Você concluiu o tutorial. Ao terminar de explorar seu parque eólico de demonstração no SiteWise Monitor, siga o próximo procedimento para limpar seus recursos.

Etapa 6: limpar os recursos após o tutorial

Depois de concluir o tutorial, é possível limpar os recursos. Você não será cobrado pelo AWS IoT SiteWise se os usuários não fizerem login no portal, mas poderá excluir o portal e os usuários do Diretório do Centro de Identidade do AWS IAM . Seus ativos de demonstração do parque de energia eólica são excluídos no final da duração que você escolheu ao criar a demonstração, ou você pode excluir a demonstração manualmente. Para ter mais informações, consulte Excluindo a demonstração AWS IoT SiteWise.

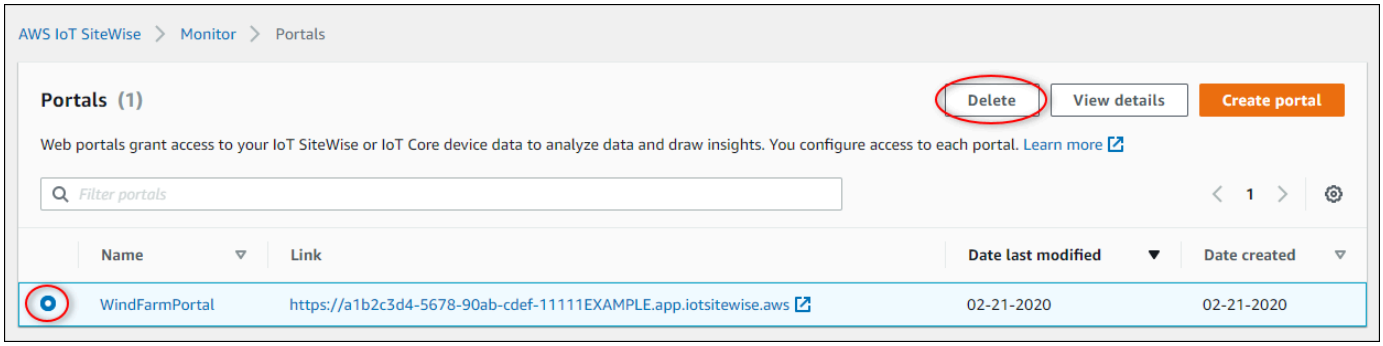
Use os procedimentos a seguir para excluir o portal e os usuários do Centro de identidade do IAM.

Como excluir um portal

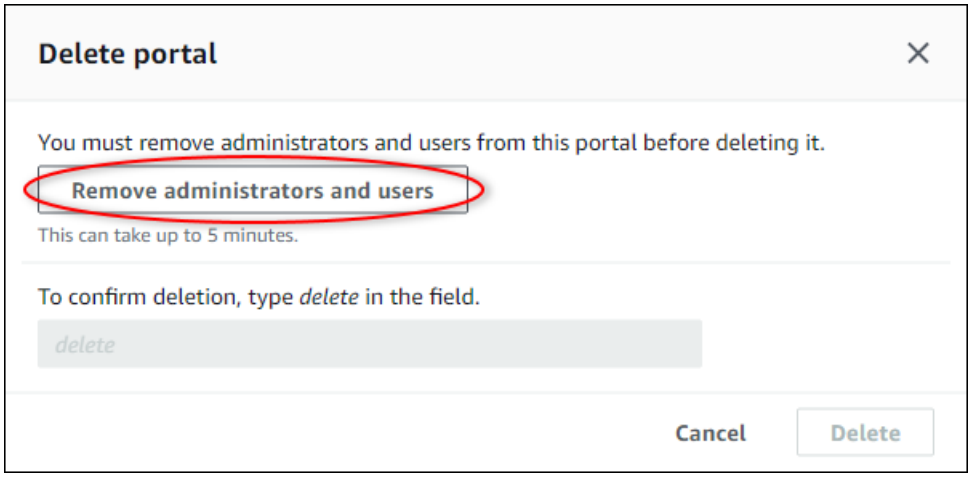
1. Navegue até o console do AWS IoT SiteWise.

2. No painel de navegação à esquerda, escolha Portais.
3. Escolha seu portal e WindFarmPortal, em seguida, escolha Excluir.

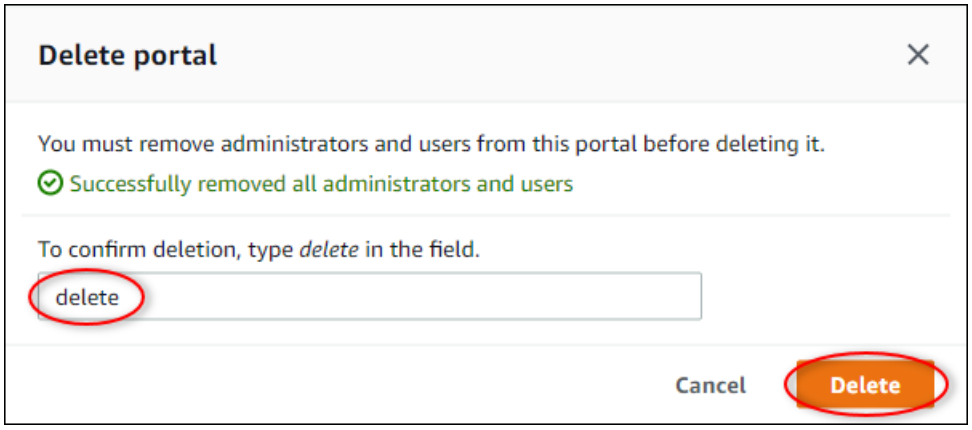
   Quando você exclui um portal ou projeto, os ativos associados a projetos excluídos não são afetados.



4. Na caixa de diálogo Excluir portal, escolha Remover administradores e usuários.

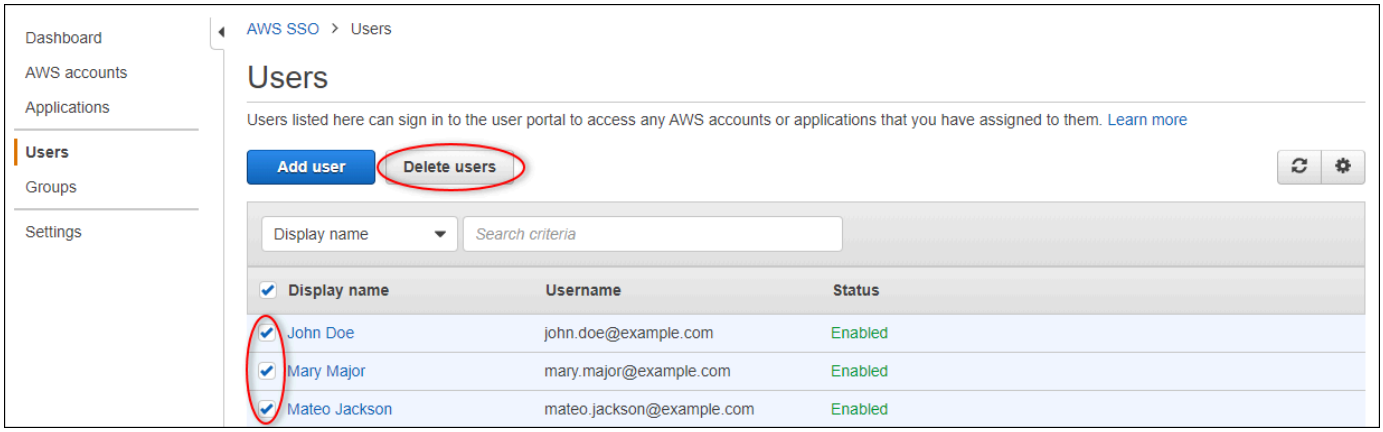


5. Digite **`delete`** para confirmar a exclusão e escolha Excluir.

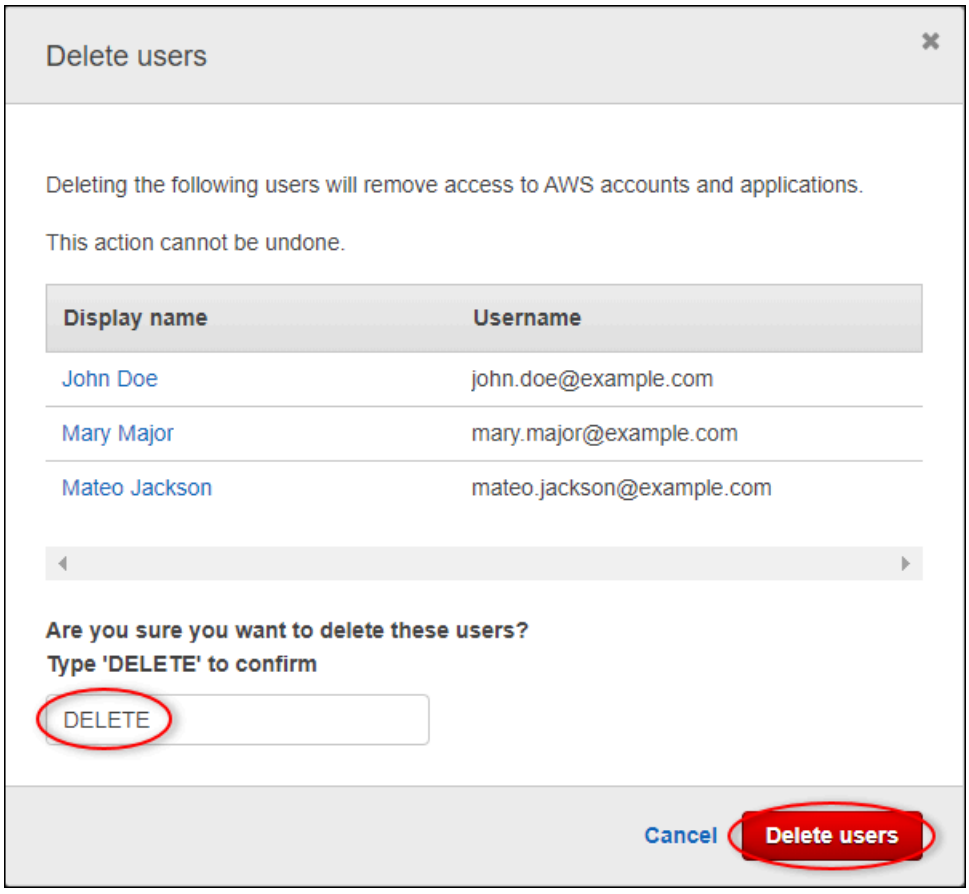


Excluir usuários do IAM Identity Center

1. Navegue até o console do Centro de identidade do IAM.
2. No painel de navegação à esquerda, escolha Usuários.
3. Marque a caixa de seleção de cada usuário a ser excluído e escolha Excluir usuários.



4. Na caixa de diálogo Excluir usuários, digite **DELETE** e depois escolha Excluir usuários.



Publicar atualizações de valor de propriedade no Amazon DynamoDB

Este tutorial apresenta uma forma conveniente de armazenar seus dados usando o Amazon DynamoDB, facilitando o acesso a dados históricos de ativos sem consultar repetidamente a API. AWS IoT SiteWise Depois de concluir este tutorial, você pode criar um software personalizado que consome os dados do seu ativo, como um mapa ao vivo da velocidade e direção do vento em um parque eólico inteiro. Se você quiser monitorar e visualizar seus dados sem implementar uma solução de software personalizada, consulteMonitorando dados com AWS IoT SiteWise Monitor.

Neste tutorial, você se baseia na AWS IoT SiteWise demonstração que fornece um conjunto de dados de amostra para um parque eólico. Você configura as atualizações de valor de propriedade da demonstração do parque de energia eólica para enviar dados pelas regras Core do AWS IoT a uma tabela do DynamoDB criada por você. Quando você ativa as atualizações do valor da propriedade, AWS IoT SiteWise envia seus dados para as AWS IoT Core mensagens do MQTT. Em seguida, defina as regras AWS IoT principais que executam ações, como a ação do DynamoDB, dependendo do conteúdo dessas mensagens. Para ter mais informações, consulte Interagindo com outros serviços AWS.

Tópicos

Pré-requisitos

Para concluir este tutorial, você precisará do seguinte:

- Uma AWS conta. Se você não tiver uma, consulte Configurando um Conta da AWS.

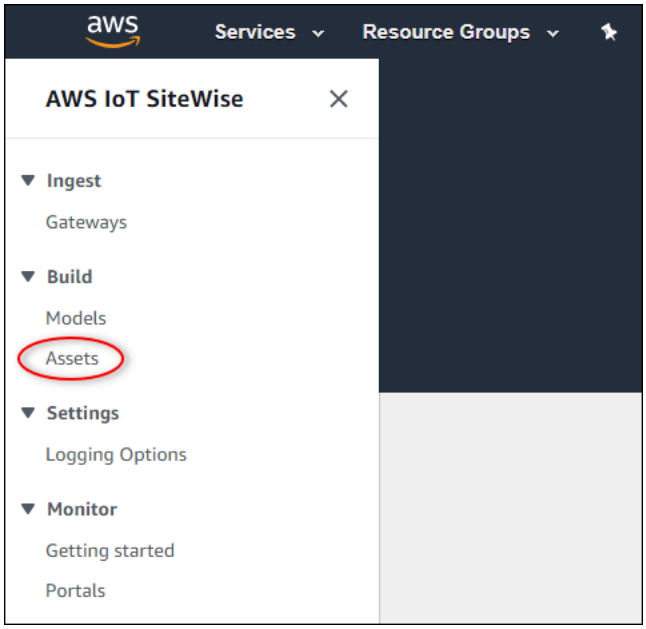
- Um computador de desenvolvimento executando Windows, macOS, Linux ou Unix para acessar o. AWS Management Console Para obter mais informações, consulte Conceitos básicos sobre o AWS Management Console.
- Um usuário do IAM com permissões de administrador.
- Uma demonstração em funcionamento de um parque AWS IoT SiteWise eólico. Quando você configura a demonstração, ela define modelos e ativos AWS IoT SiteWise e transmite dados para eles para representar um parque eólico. Para ter mais informações, consulte Usando a AWS IoT SiteWise demonstração.

Etapa 1: Configurar AWS IoT SiteWise para publicar atualizações de valores de propriedades

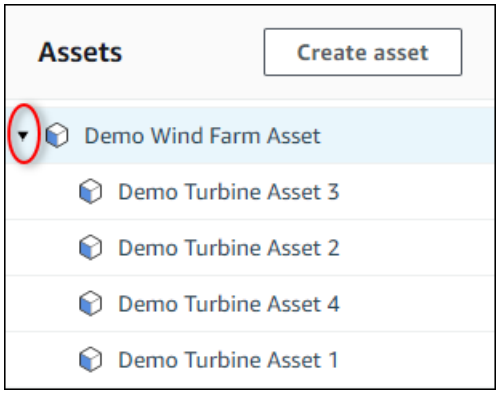
Neste procedimento, habilite as notificações de valor de propriedade das propriedades Wind Speed dos ativos da turbina de demonstração. Depois de ativar as notificações de valor da propriedade, AWS IoT SiteWise publica cada atualização de valor em uma mensagem MQTT no Core. AWS IoT

Como habilitar notificações de atualização de valor de propriedade nas propriedades do ativo

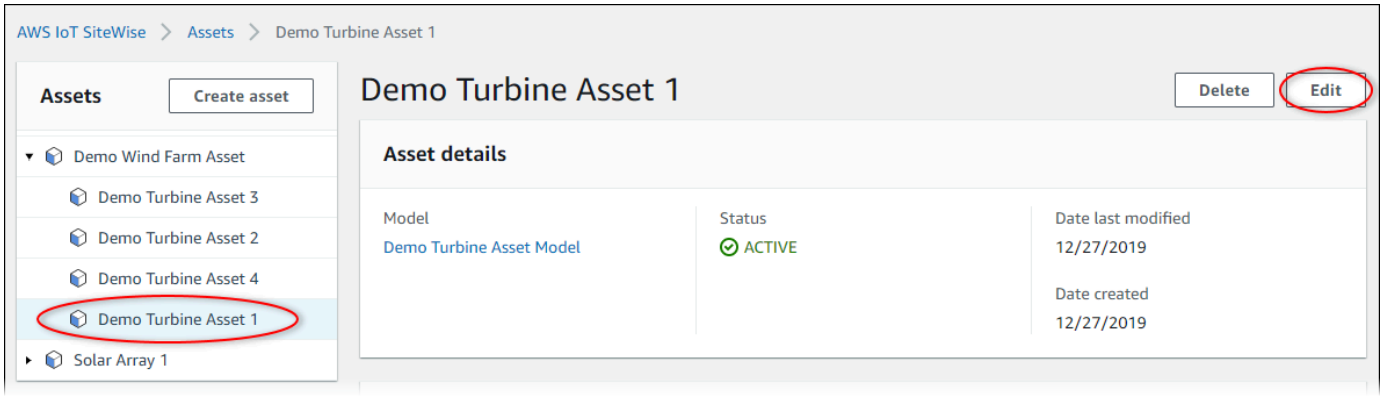
1. Faça login no AWS IoT SiteWise console.
2. Revise os AWS IoT SiteWise endpoints e as cotas em que AWS IoT SiteWise há suporte e troque de AWS região, se necessário. Mude para uma região onde você está executando a AWS IoT SiteWise demonstração.
3. No painel de navegação à esquerda, escolha Ativos.



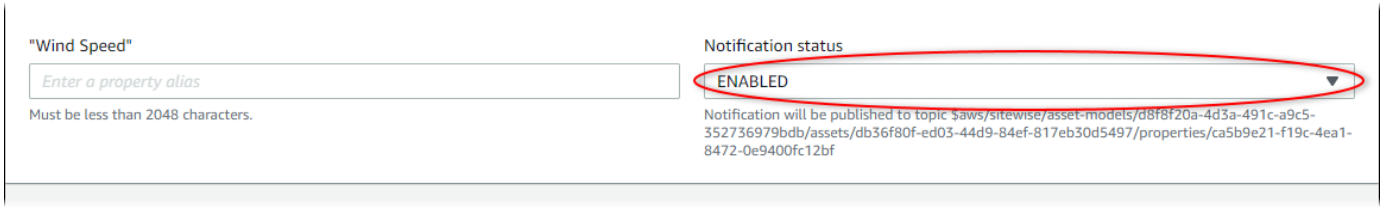
4. Selecione a seta ao lado de Demo Wind Farm Asset para expandir a hierarquia do ativo do parque de energia eólica.



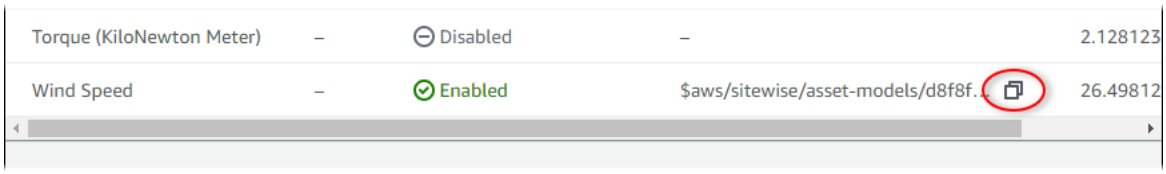
5. Escolha uma turbina de demonstração e escolha Edit (Editar).



6. Atualize o status de notificação da propriedade Wind Speed para ATIVADO.



7. Escolha Save asset (Salvar ativo) na parte inferior da página.
8. Repita as etapas 5 a 7 para cada ativo da turbina de demonstração.
9. Escolha uma turbina de demonstração (por exemplo, Demo Turbine Asset 1).
10. Selecione Measurements (Medidas).
11. Selecione o ícone de cópia ao lado da propriedade Wind Speed para copiar o tópico de notificação para a área de transferência. Salve o tópico de notificação para usar mais adiante neste tutorial. Você só precisa registrar o tópico de notificação de uma turbina.



O tópico de notificação deve ser semelhante ao exemplo a seguir.

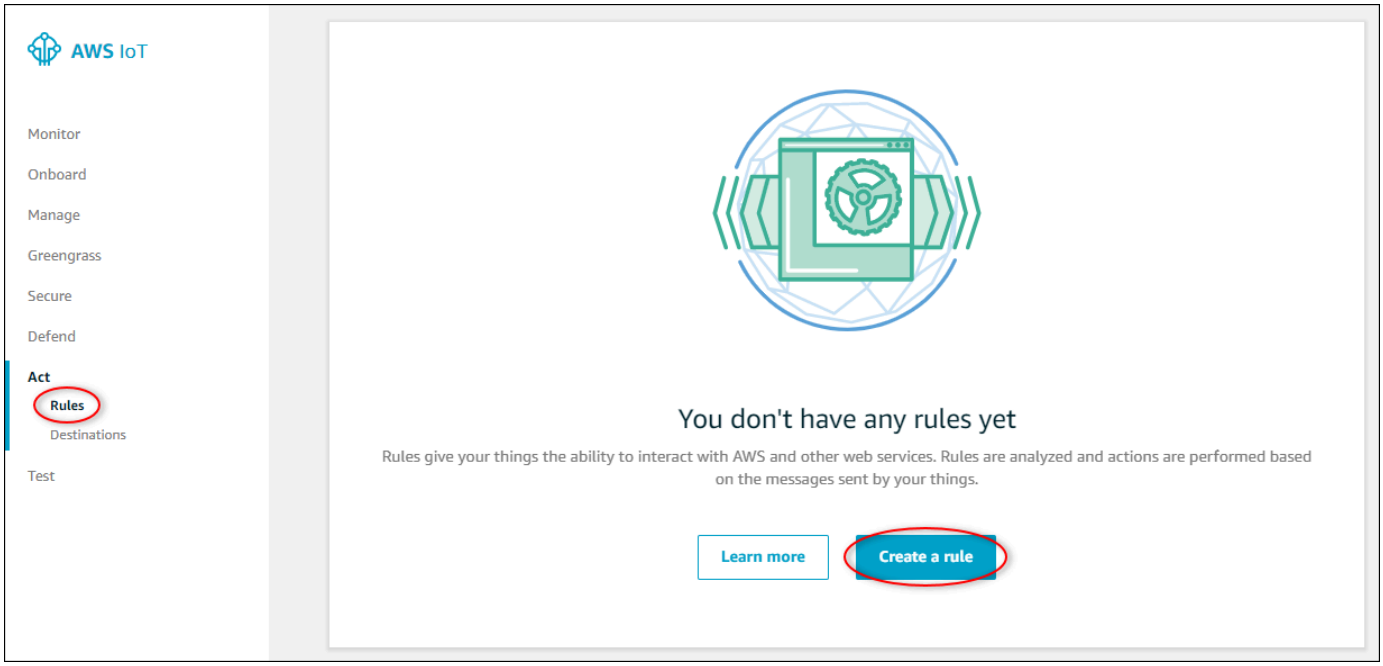
```
$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/
assets/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE/properties/a1b2c3d4-5678-90ab-
cdef-33333EXAMPLE
```

Etapa 2: criar uma regra no AWS IoT Core

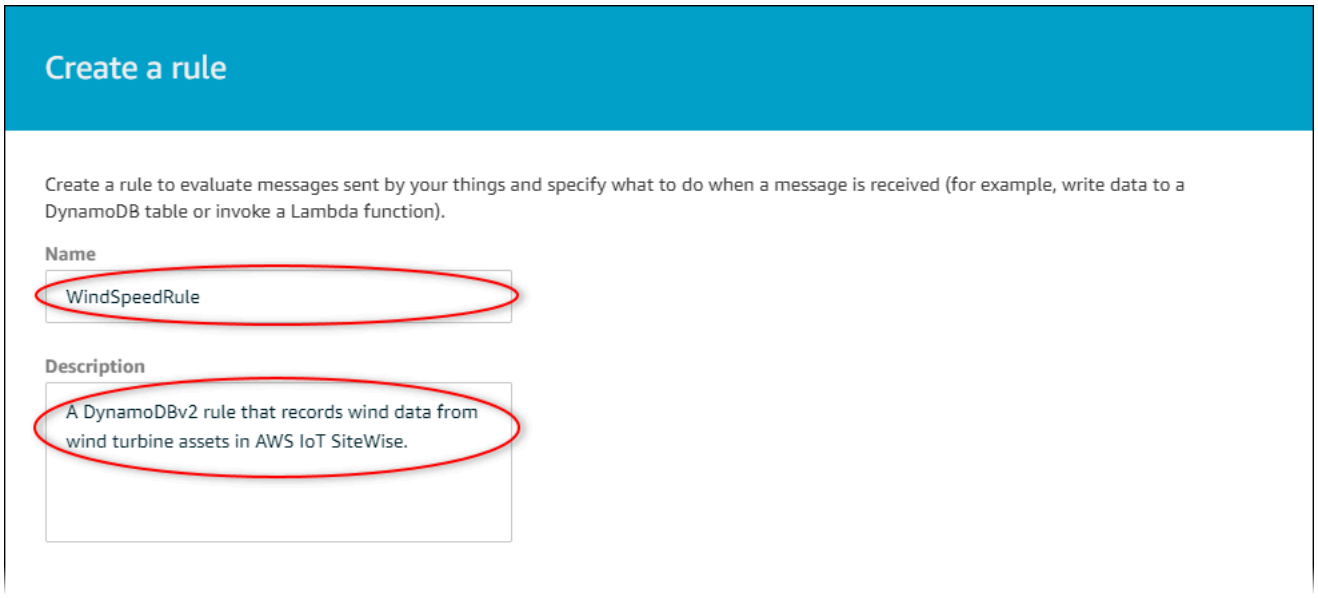
Neste procedimento, você cria uma regra no AWS IoT Core que analisa as mensagens de notificação do valor da propriedade e insere dados em uma tabela do Amazon DynamoDB. AWS IoT As regras básicas analisam as mensagens do MQTT e executam ações com base no conteúdo e no tópico de cada mensagem. Em seguida, você cria uma regra com uma ação do DynamoDB para inserir dados em uma tabela do DynamoDB criada como parte deste tutorial.

Como criar uma regra com uma ação do DynamoDB

1. Navegue até o console do AWS IoT. Se um botão Get started (Começar a usar) for exibido, selecione-o.
2. No painel de navegação esquerdo, escolha Agir e Regras.



3. Se uma caixa de diálogo Você ainda não tem regras, selecione Criar uma regra. De outro modo, escolha Create (Criar).
4. Insira um nome e uma descrição para a regra.



5. Encontre o tópico de notificação que você salvou anteriormente neste tutorial.

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

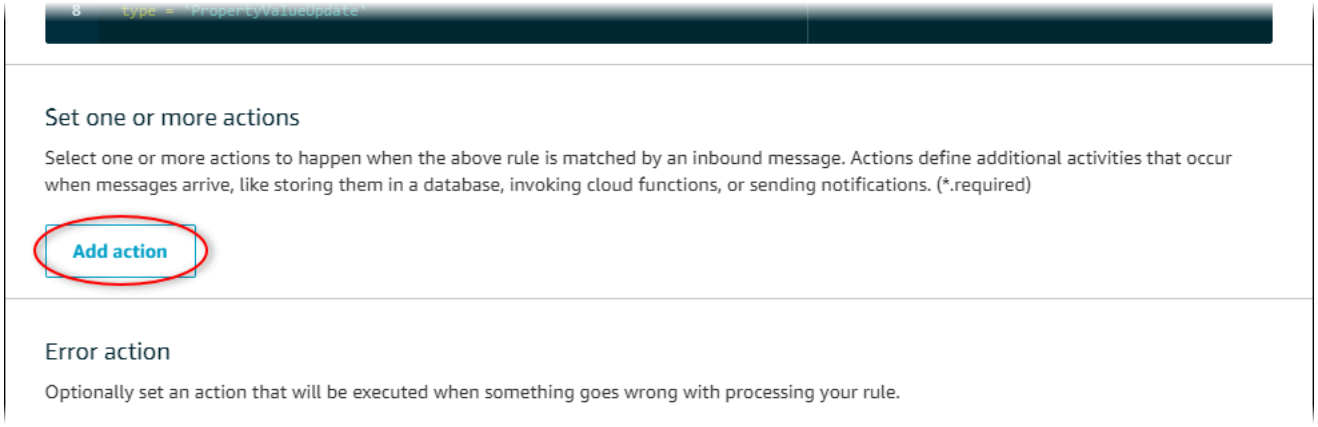
Substitua o ID do ativo (o ID posterior`assets/`) no tópico por um`+`. Isso seleciona a propriedade de velocidade do vento para todos os ativos de turbinas eólicas de demonstração. O filtro de tópico + aceita todos os nós de um único nível em um tópico. Seu tópico deve ser semelhante ao exemplo a seguir.

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

6. Insira a instrução de consulta de regra a seguir. Substitua o tópico na seção `FROM` pelo tópico de notificação.

```
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. Em Set one or more actions (Definir uma ou mais ações), selecione Add action (Adicionar ação).



8. Na página Selecionar uma ação, escolha Dividir mensagem em várias colunas de uma tabela do DynamoDB (DynamoDBv2).

9. Escolha Configurar ação na parte inferior da página.
10. Na página Configurar ação, selecione Criar um novo recurso.

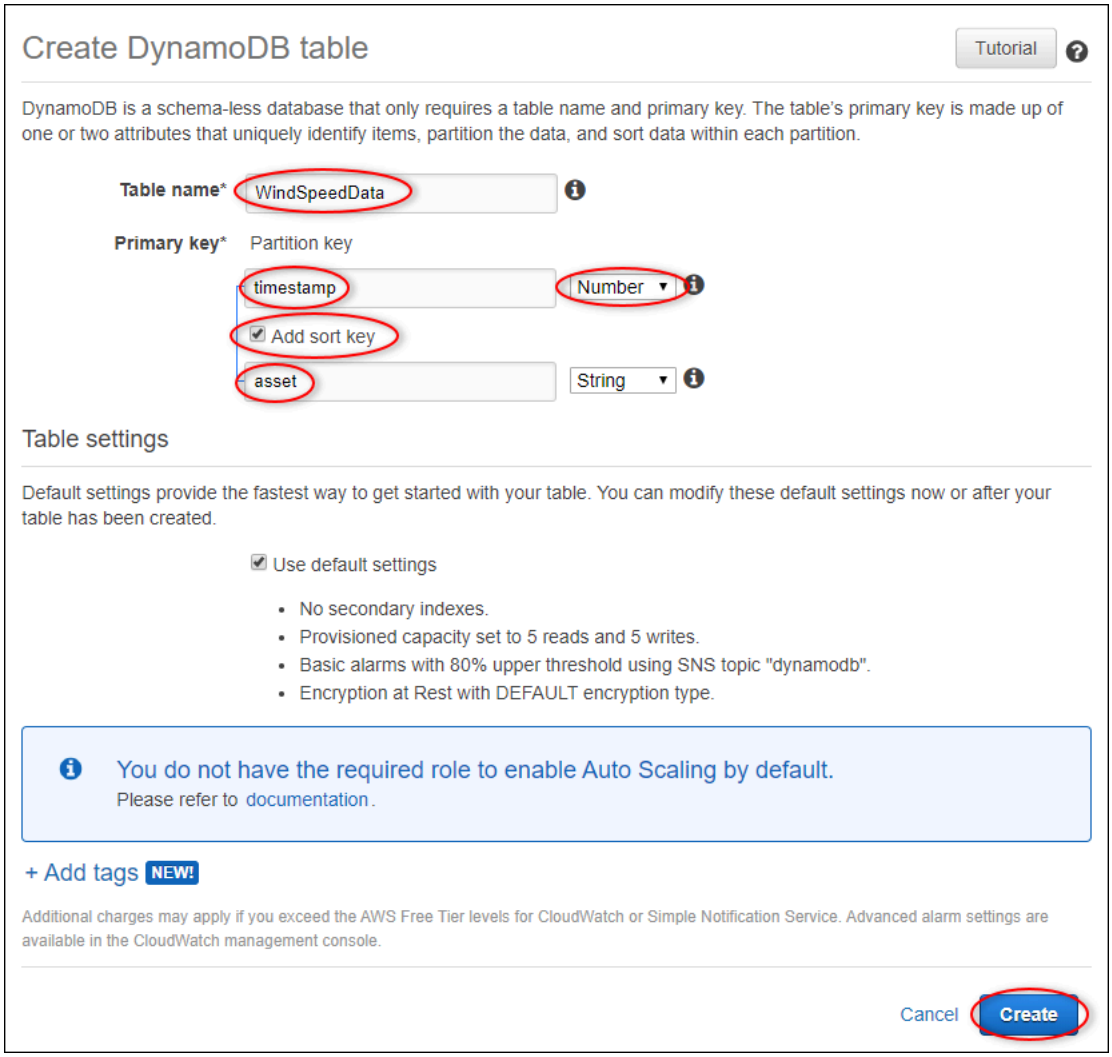
    O console do DynamoDB é aberto em uma nova guia. Mantenha a guia de ação da regra aberta enquanto você conclui os procedimentos a seguir.

Etapa 3: criar uma tabela do DynamoDB

Neste procedimento, você cria uma tabela do Amazon DynamoDB para receber dados de velocidade do vento da ação da regra.

Como criar uma tabela do DynamoDB

1. No painel do console do DynamoDB, escolha Criar tabela.
2. Insira um nome para a tabela.



3. Em Primary key (Chave primária), faça o seguinte:

   a. Digite **`timestamp`** como a chave de partição.

   b. Escolha o tipo Number (Número).

   c. Marque a caixa de seleção Add sort key (Adicionar chave de classificação).

   d. Digite **`asset`** como a chave de classificação e deixe o tipo de chave de classificação padrão String.

4. Escolha Criar.

   Quando o aviso Table is being created (A tabela está sendo criada) desaparece, a tabela está pronta.

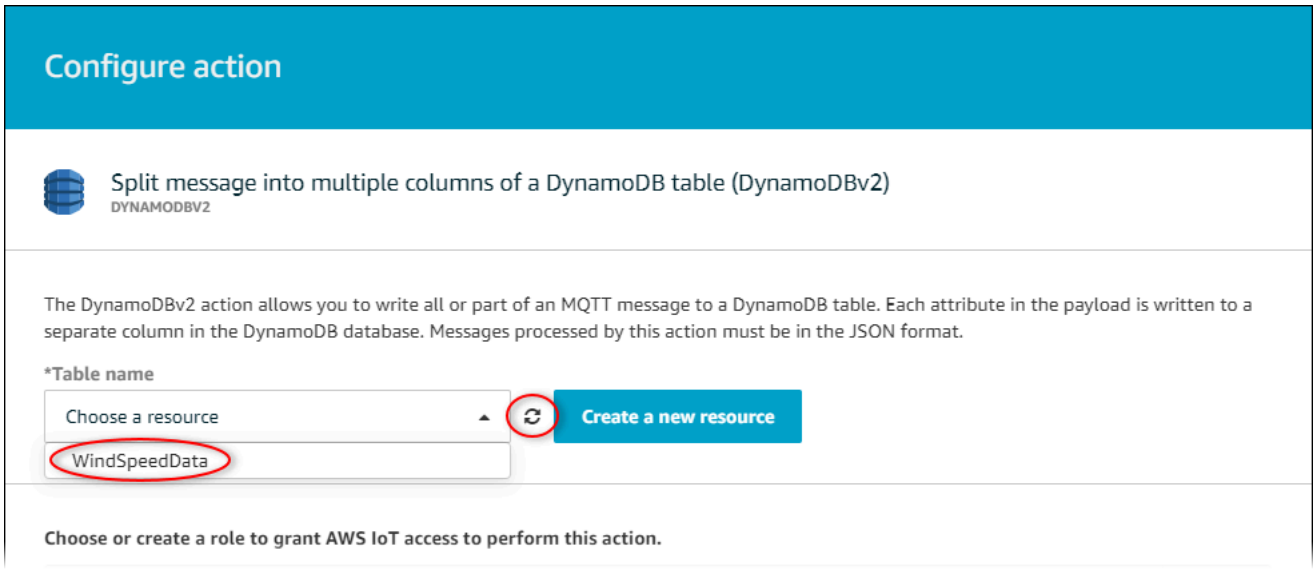
5. Retorne à guia com a página Configure action (Configurar ação). Mantenha a guia do DynamoDB aberta enquanto conclui os procedimentos a seguir.

Etapa 4: Configurar a ação da regra do DynamoDB

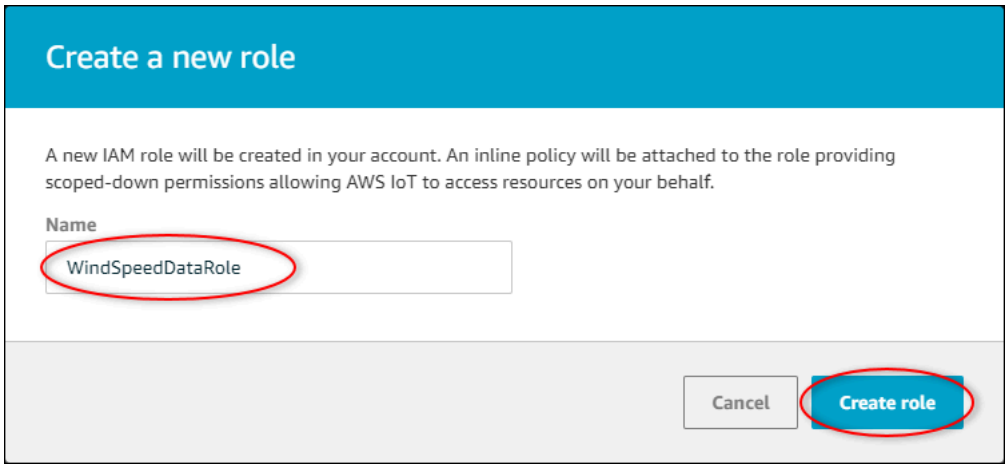
Neste procedimento, você configura a ação de regra do Amazon DynamoDB para inserir dados de atualizações de valores de propriedades em sua nova tabela do DynamoDB.

Como configurar a ação de regra do DynamoDB

1. Na página Configurar ação atualize a lista Nome da tabela e selecione a nova tabela do DynamoDB.



2. Escolha Criar função para criar uma função do IAM que conceda acesso AWS IoT principal para realizar a ação da regra.
3. Forneça um nome de função e escolha Create role (Criar função).



4. Selecione Adicionar ação.
5. Escolha Create rule (Criar regra) na parte inferior da página para concluir a criação da regra.

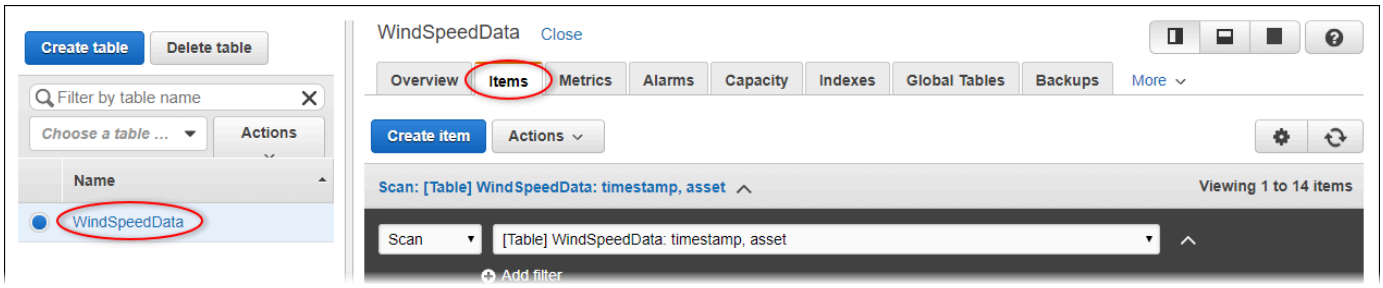
Os dados de ativo de demonstração devem começar a aparecer na tabela do DynamoDB.

Etapa 5: Explore os dados no DynamoDB

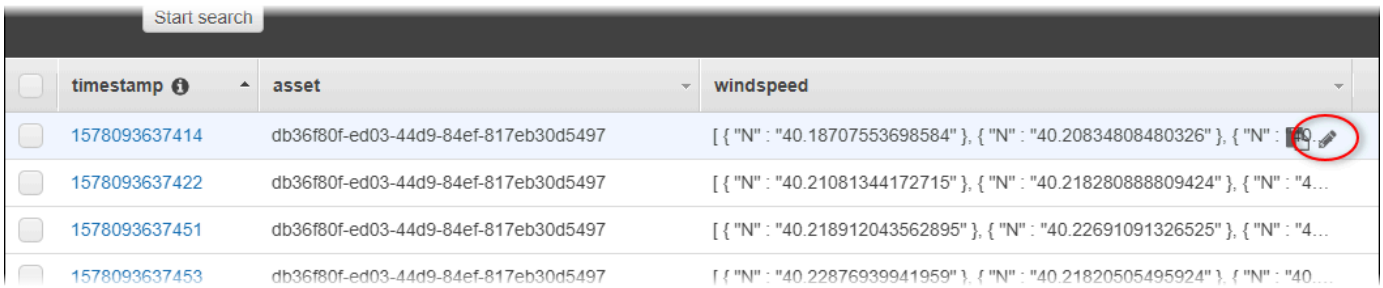
Neste procedimento, você explora os dados de velocidade do vento dos ativos de demonstração em sua nova tabela do Amazon DynamoDB.

Como explorar dados de ativo no DynamoDB

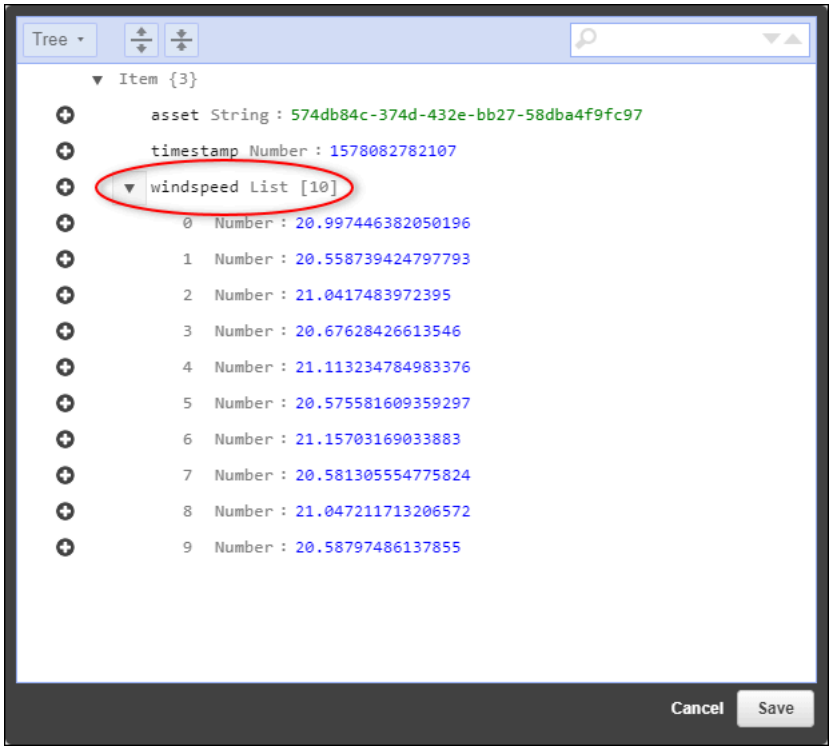
1. Retorne à guia com a tabela do DynamoDB aberta.
2. Na tabela criada anteriormente, escolha a guia Items (Itens) para exibir os dados na tabela. Atualize a página se você não vir linhas na tabela. Se as linhas não aparecerem após alguns minutos, consulte Solucionar problemas de uma regra.



3. Em uma linha na tabela, escolha o ícone de edição para expandir os dados.



4. Escolha a seta ao lado da estrutura windspeed para expandir a lista de pontos de dados de velocidade do vento. Cada lista reflete um lote de pontos de dados de velocidade do vento enviados AWS IoT SiteWise pela demonstração do parque eólico. Talvez você queira um formato de dados diferente se configurar uma ação de regra para seu próprio uso. Para ter mais informações, consulte Consultar mensagens de notificação de propriedade de ativos.



Agora que você concluiu o tutorial, desative ou exclua a regra e exclua sua tabela do DynamoDB para evitar cobranças adicionais. Para limpar seus recursos, consulteEtapa 6: limpar os recursos após o tutorial.

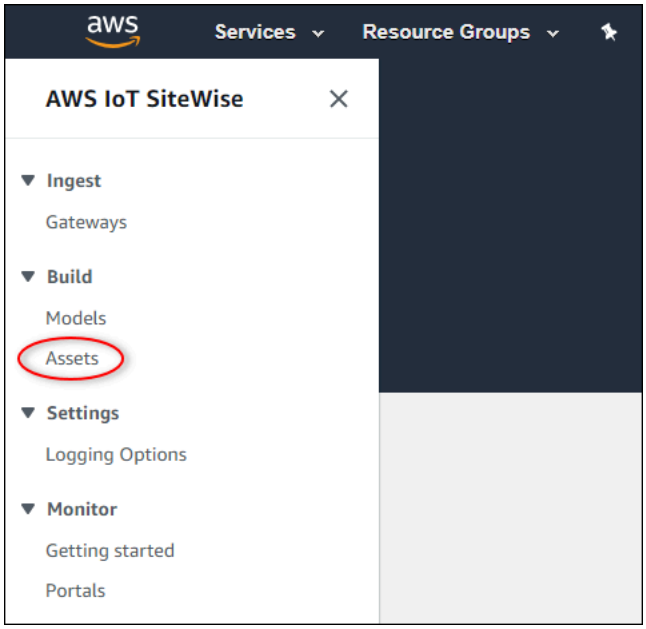
Etapa 6: limpar os recursos após o tutorial

Depois de concluir o tutorial, limpe os recursos para evitar a geração de cobranças adicionais. Seus ativos de demonstração do parque eólico são excluídos no final da duração que você escolheu ao criar a demonstração. Você também pode excluir a demonstração manualmente. Para ter mais informações, consulte Excluindo a demonstração AWS IoT SiteWise.

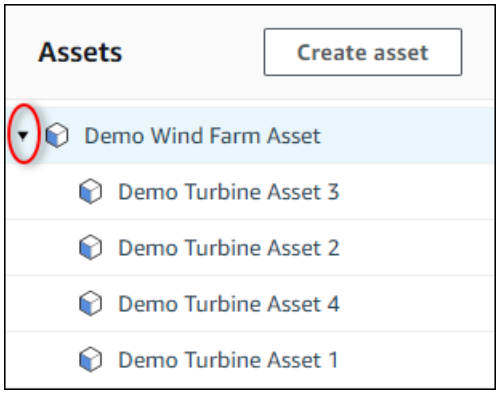
Use os procedimentos a seguir para desativar as notificações de atualização do valor da propriedade (se você não excluiu a demonstração), desativar ou excluir sua AWS IoT regra e excluir sua tabela do DynamoDB.

Como desabilitar notificações de atualização de valor de propriedade nas propriedades do ativo

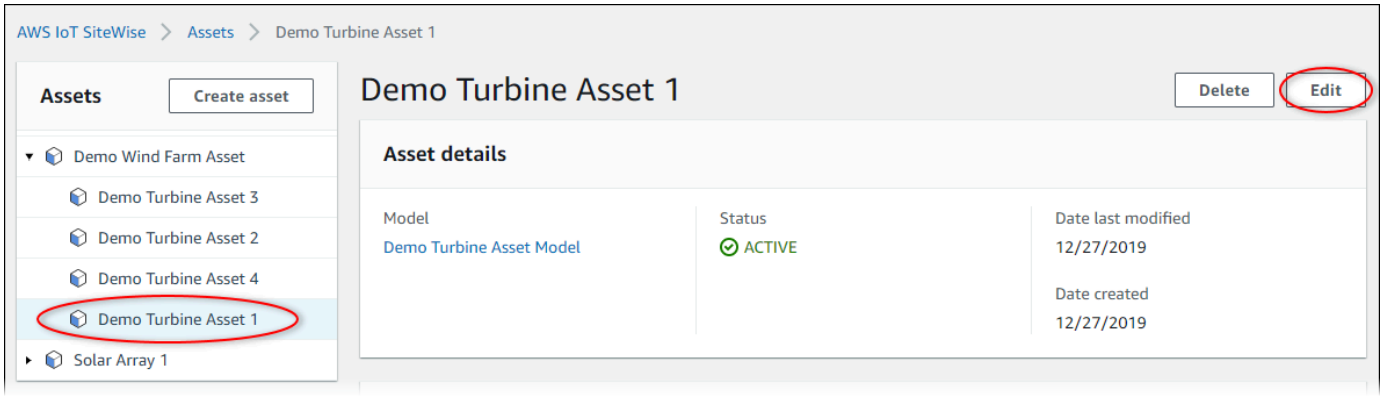
1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação à esquerda, escolha Ativos.



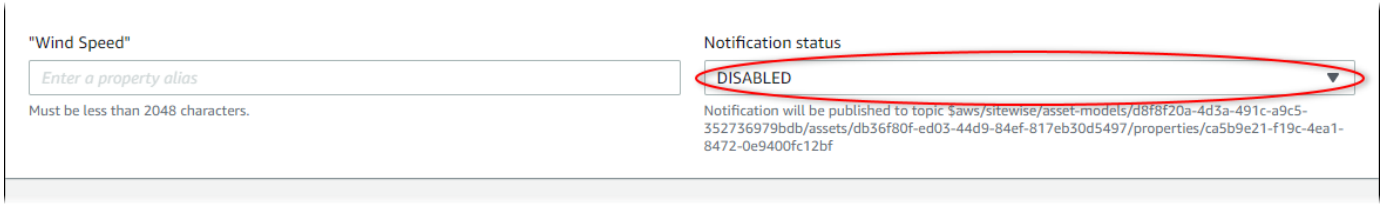
3. Selecione a seta ao lado de Demo Wind Farm Asset para expandir a hierarquia do ativo do parque de energia eólica.



4. Escolha uma turbina de demonstração e escolha Edit (Editar).



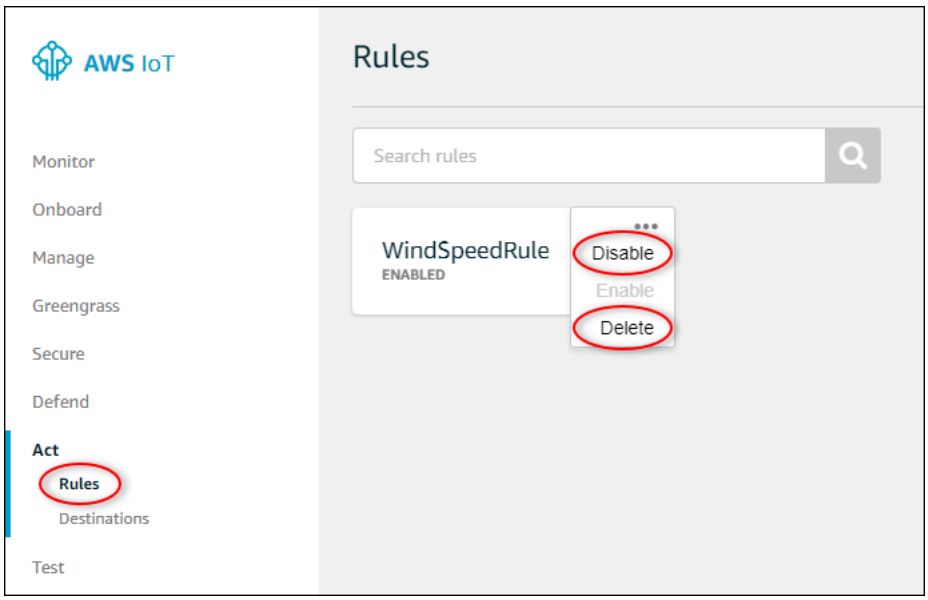
5. Atualize o status de notificação da propriedade Wind Speed para DESATIVADO.



6. Escolha Save asset (Salvar ativo) na parte inferior da página.
7. Repita as etapas de 4 a 6 para cada ativo da turbina de demonstração.

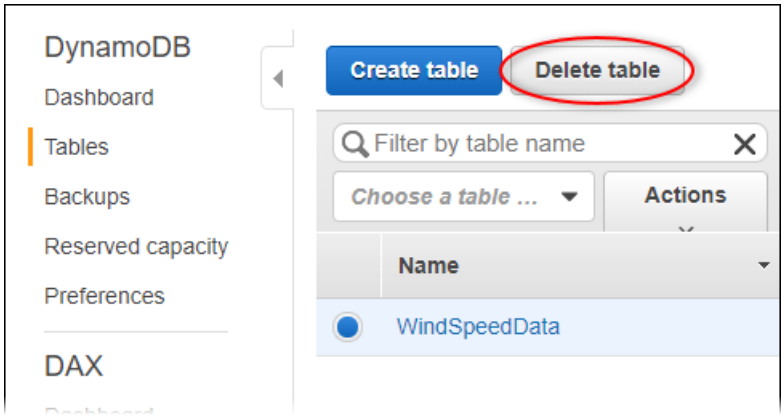
Para desativar ou excluir uma regra no AWS IoT Core

1. Navegue até o console do AWS IoT.
2. No painel de navegação esquerdo, escolha Agir e Regras.
3. Escolha o menu na regra e escolha Disable (Desativar) ou Delete (Excluir).

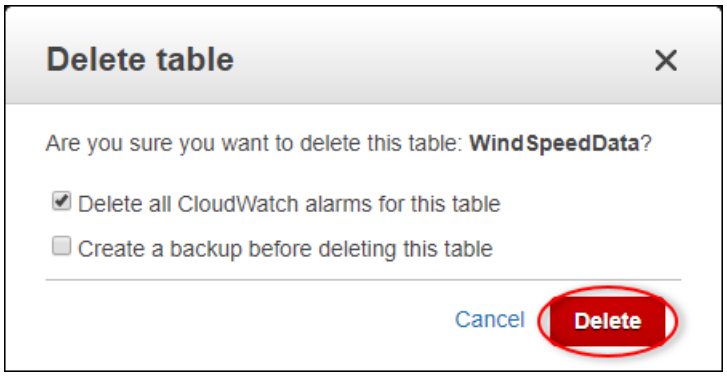


Como excluir uma tabela do DynamoDB

1. Navegue até o console do DynamoDB.
2. No painel de navegação à esquerda, selecione Tables (Tabelas).
3. Escolha a tabela criada anteriormente, WindSpeedData.
4. Selecione Delete table (Excluir tabela).



5. Na caixa de diálogo Delete table (Excluir tabela), selecione Delete (Excluir).



Ingestão de dados para AWS IoT SiteWise

AWS IoT SiteWise foi projetado para coletar e correlacionar de forma eficiente os dados industriais com os ativos correspondentes, representando vários aspectos das operações industriais. Esta documentação se concentra nos aspectos práticos da ingestão de dados AWS IoT SiteWise, oferecendo vários métodos personalizados para diversos casos de uso industrial. Para obter instruções sobre como criar sua operação industrial virtual, consulte Modelagem de ativos industriais.

Você pode enviar dados industriais para AWS IoT SiteWise usar qualquer uma das seguintes opções:

- AWS IoT SiteWise Edge — Use o gateway SiteWise Edge como intermediário entre seus AWS IoT SiteWise servidores de dados. AWS IoT SiteWise fornece AWS IoT Greengrass componentes que você pode implantar em qualquer plataforma que possa ser executada AWS IoT Greengrass para configurar um gateway SiteWise Edge. Essa opção oferece suporte à vinculação com o protocolo de servidor OPC-UA.
- AWS IoT SiteWise API — use a AWS IoT SiteWise API para fazer upload de dados de qualquer outra fonte. Use nossa BatchPutAssetPropertyValueAPI de streaming para ingestão em segundos ou a CreateBulkImportJobAPI orientada por lotes para facilitar a ingestão econômica em lotes maiores.
- AWS IoT Regras básicas — Use as regras AWS IoT básicas para carregar dados de mensagens MQTT publicadas por uma AWS IoT coisa ou outro AWS serviço.
- AWS IoT Events ações — Use AWS IoT Events ações acionadas por eventos específicos em AWS IoT Events. Esse método é adequado para cenários em que o upload de dados está vinculado a ocorrências de eventos.
- AWS IoT Greengrass gerenciador de fluxo — Use o gerenciador de AWS IoT Greengrass fluxo para carregar dados de fontes de dados locais usando um dispositivo de borda. Essa opção atende a situações em que os dados se originam de locais locais ou de borda.

Esses métodos oferecem uma variedade de soluções para gerenciar dados de diferentes fontes. Aprofunde-se nos detalhes de cada opção para obter uma compreensão abrangente dos recursos AWS IoT SiteWise de ingestão de dados fornecidos.

Gerenciar fluxos de dados

Antes de mergulhar na criação de modelos de ativos e ativos em AWS IoT SiteWise, comece configurando suas fontes de dados para enviar informações diretamente do seu equipamento industrial para a plataforma. AWS IoT SiteWise foi projetado para gerar automaticamente fluxos de dados que coletam seus dados brutos. Cada um dos fluxos de dados é identificado por um alias exclusivo, facilitando o controle da origem de cada dado.

Por exemplo, considere um parque eólico usando um gateway AWS IoT SiteWise Edge para enviar dados sobre temperatura do ar, velocidade de rotação da hélice e dados de série temporal de saída de energia de um servidor OPC-UA para. AWS IoT SiteWise O alias do fluxo de `server1-windfarm/3/turbine/7/temperature` dados identifica os valores de temperatura provenientes da turbina #7 no parque eólico #3. `server1`é o nome da fonte de dados OPC-UA. O `server1` prefixo é usado para todos os fluxos de dados provenientes desse servidor, ajudando a organizar os dados de acordo com sua fonte.

Depois de criar os modelos e ativos de ativos, organize o fluxo de dados associando cada fluxo de dados a propriedades específicas do ativo. Essa associação AWS IoT SiteWise permite não apenas coletar, mas também processar os dados de acordo com a estrutura de seus ativos. Se necessário, você também pode remover o vínculo entre os fluxos de dados e as propriedades do ativo.

Atualmente, você só pode associar fluxos de dados a medições. Medições são um tipo de propriedade de ativo que representa os fluxos de dados brutos do sensor de um dispositivo, como valores de temperatura com marcação de data/hora ou valores de rotação por minuto (RPM) com marcação de data/hora.

Quando essas medidas definem métricas ou transformações, os dados recebidos acionam cálculos específicos. É importante observar que uma propriedade de ativo só pode ser vinculada a um fluxo de dados por vez.

> **Note**
>
> Uma propriedade de ativo não pode ser associada a vários fluxos de dados ao mesmo tempo.

AWS IoT SiteWise usa `TimeSeries` o recurso Amazon Resource Name (ARN) para determinar suas cobranças de armazenamento. Para obter mais informações, consulte Preços do AWS IoT SiteWise.

As seções a seguir mostram como usar o AWS IoT SiteWise console ou a API para gerenciar fluxos de dados.

Tópicos

Gerenciar streams de dados

Para começar a gerenciar fluxos de dados, execute o seguinte.

> **Note**
>
> Se você for novato AWS IoT SiteWise depois de 24 de novembro de 2021, pode pular esta seção. Os clientes que começaram a usar AWS IoT SiteWise antes dessa data precisam definir as configurações do serviço para permitir AWS IoT SiteWise a ingestão de dados sem modelos e ativos de ativos.

- Certifique-se que seu perfil do IAM tenha as permissões mostradas no exemplo a seguir.

  Example Política de usuário do 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 dados em um fluxo de dados, faça o seguinte.
>
> - O recurso `time-series` deve ser autorizado se você usar um alias de propriedade para identificar o fluxo de dados.
> - O recurso do `asset` deve ser autorizado se você usar uma ID de ativo para identificar o ativo que contém a propriedade do ativo associada.

Para obter mais informações sobre a configuração de políticas do IAM, consulte Gerenciar políticas do IAM no Guia do usuário do IAM.

- Defina as configurações de ingestão de dados para permitir AWS IoT SiteWise a aceitação de fluxos de dados que não estão associados às propriedades do ativo.

Tópicos

Definindo as configurações de ingestão de dados

Console

Configure AWS IoT SiteWise para aceitar fluxos de dados não associados às propriedades do ativo usando o AWS IoT SiteWise console.

Para definir configurações de ingestão de dados (console)

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, em Configurações, selecione Ingestão de dados.
3. Na página Ingestão de dados, escolha Editar.
4. Na seção Ingestão de dados desassociados, escolha Habilitar ingestão de dados para fluxos de dados não associados às propriedades do ativo.

> **Important**
>
> Depois de configurar AWS IoT SiteWise para aceitar fluxos de dados não associados às propriedades do ativo, você não poderá desativar essa configuração.

5. Selecione Salvar.
6. Em Habilitar a ingestão de dados desassociados, escolha Atualizar. O status da Ingestão de dados desassociados se torna Ativo. O processo pode demorar alguns minutos para ser concluído.

AWS CLI

Configure AWS IoT SiteWise para aceitar fluxos de dados não associados às propriedades do ativo usando a operação da PutStorageConfigurationAPI. A seção a seguir usa o AWS CLI.

Para definir configurações de ingestão de dados (AWS CLI)

1. Para configurar AWS IoT SiteWise para receber fluxos de dados não associados às propriedades do ativo, execute o comando a seguir.

> **Important**
>
> Depois de configurar AWS IoT SiteWise para aceitar fluxos de dados não associados às propriedades do ativo, você não poderá desativar essa configuração.

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

É possível configurar o `storageType` para `MULTI_LAYER_STORAGE`. Para ter mais informações, consulte Gerenciando o armazenamento de dados.

Example Retorno

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

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

O processo pode demorar alguns minutos para ser concluído.

2. Para obter as informações de configuração do repositório, use o seguinte comando:

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

Example Retorno

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

Gerenciar fluxos de dados

Gerencie seus fluxos de dados usando o Console do AWS IoT SiteWise ou AWS CLI.

Console

Use o AWS IoT SiteWise console para gerenciar seus fluxos de dados.

Para gerenciar fluxos de dados (console)

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Fluxos de dados.
3. (Opcional) Para adicionar ou atualizar tags, selecione o fluxo de dados a ser editado, então escolha Gerenciar tags.

   Na página Editar tags, escolha Adicionar tag. No campo Chave, digite o nome da tag a ser usada.

Escolha Salvar.

4. (Opcional) Na tabela de fluxo de dados, você pode filtrar os fluxos de dados das seguintes maneiras.

   - No primeiro menu suspenso, selecione Prefixo do alias ou ID do ativo.
     - Prefixo do alias: o prefixo do alias do fluxo de dados. Você pode escolher essa opção se seus fluxos de dados de destino tiverem um prefixo de alias.
     - ID do ativo: o ID do ativo no qual a propriedade do ativo foi criada. Você pode escolher essa opção se seus fluxos de dados de destino forem associados a uma propriedade do ativo.
   - No segundo menu suspenso, selecione Todos os fluxos de dados, Fluxos de dados associados ou Fluxos de dados desassociados.
     - Todos os fluxos de dados: fluxos de dados associados ou não a uma propriedade do ativo.
     - Fluxos de dados associados: fluxos de dados que estão associados a uma propriedade do ativo.
     - Fluxos de dados desassociados: fluxos de dados que não estão associados a uma propriedade do ativo.
5. Selecione os fluxos de dados que você está gerenciando. AWS IoT SiteWise exibe os fluxos de dados que você escolheu em um gráfico na parte inferior da página. Se você selecionar mais de 10, o gráfico exibirá somente os 10 primeiros.
6. (Opcional) Configure o gráfico das seguintes maneiras.

   a. Para Função de agregação, selecione uma das opções a seguir.

      - Contagem de ponto de dados: retorna o número total de pontos de dados das variáveis fornecidas ao longo do intervalo de tempo atual.
      - Média: a média dos valores das variáveis fornecidas ao longo do intervalo de tempo atual.
      - Soma: a soma dos valores das variáveis fornecidas ao longo do intervalo de tempo atual.
      - Mínimo: o valor mínimo dos valores das variáveis fornecidas ao longo do intervalo de tempo atual.

- Máximo: o valor máximo das variáveis fornecidas ao longo do intervalo de tempo atual.

Para ter mais informações, consulte Usando funções de agregação em expressões de fórmulas.

b. Para Intervalo de tempo, selecione uma das opções a seguir.

- Última 1 hora: o gráfico exibe dados agregados na última hora.
- Últimas 2 horas: o gráfico exibe dados agregados nas duas últimas horas.
- Últimas 3 horas: o gráfico exibe dados agregados nas três últimas horas.
- Últimas 4 horas: o gráfico exibe dados agregados nas quatro últimas horas.

c. Para Intervalo de tempo, selecione uma das opções a seguir.

- 1 minuto: agrega dados a cada minuto no intervalo de tempo especificado.
- 1 hora: agrega dados a cada hora no intervalo de tempo especificado.

7. Escolha Gerenciar fluxos de dados.
8. Na seção Atualizar associações de fluxo de dados, na coluna Nome da medição, realize um dos procedimentos abaixo.

- Se o fluxo de dados estiver associado a uma medição, exclua a associação escolhendo o ícone de fechar.
- Se o fluxo de dados não estiver associado a uma medida, escolha Escolher medição.

9. Na tabela Escolher uma medição, navegue até o ativo de destino e escolha a medição que você está associando.
10. (Opcional) Na seção Atualizar aliases de propriedades do ativo, insira um alias exclusivo para cada medição.
11. Escolha Atualizar.

A coluna de Status pode exibir um dos valores abaixo.

- Pendente: você está atualizando a associação do fluxo de dados ou o alias da propriedade do ativo.
- Enviar: sua alteração à associação ou ao alias da propriedade do ativo é salva.

- Erro — AWS IoT SiteWise não foi possível processar sua solicitação para atualizar a associação do fluxo de dados ou o alias da medição.
- Sucesso: você atualizou com sucesso a associação do fluxo de dados ou o alias da medição.

AWS CLI

Use as seguintes operações de API para gerenciar seus fluxos de dados. Os exemplos de código usam o AWS CLI.

- AssociateTimeSeriesToAssetProperty— Associa um fluxo de dados (série temporal) a uma propriedade do ativo.
- DisassociateTimeSeriesFromAssetProperty— Desassocia um fluxo de dados de uma propriedade do ativo.
- DeleteTimeSeries— Exclui um fluxo de dados.
- DescribeTimeSeries— Recupera informações sobre um fluxo de dados.
- ListTimeSeries— Recupera uma lista paginada de fluxos de dados.

AssociateTimeSeriesToAssetProperty

Para associar um fluxos de dados à propriedade do ativo, execute o comando a seguir.

> **Important**
>
> A propriedade do ativo especificada não deve estar associada atualmente a um fluxo de dados.

- *data-stream-alias*Substitua pelo alias do fluxo de dados que você está associando.
- Substituir *asset-ID* pelo ID do ativo no qual a propriedade do ativo foi criada.
- Substituir *property-ID* pelo ID da propriedade do ativo.

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

DisassociateTimeSeriesFromAssetProperty

Para desassociar um fluxo de dados a uma propriedade do ativo, execute o comando a seguir.

- *data-stream-alias*Substitua pelo alias do fluxo de dados que você está desassociando.
- Substituir *asset-ID* pelo ID do ativo no qual a propriedade do ativo foi criada.
- Substituir *property-ID* pelo ID da propriedade do ativo.

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

DeleteTimeSeries

Para excluir um fluxo de dados, execute o seguinte comando.

*data-stream-alias*Substitua pelo alias do fluxo de dados que você está excluindo.

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

Para identificar um fluxo de dados, siga um destes procedimentos:

- Se o fluxo de dados não estiver associado a uma propriedade do ativo, especifique o `alias` do fluxo de dados.
- Se o fluxo de dados estiver associado a uma propriedade do ativo, especifique um dos seguintes:
  - O `alias` do fluxo de dados.
  - O `assetId` e `propertyId` que identifica a propriedade do ativo.

DescribeTimeSeries

Use a operação da `DescribeTimeSeries` API para verificar se você associou ou desassociou com êxito um fluxo de dados.

Para recuperar informações sobre um fluxo de dados, execute o comando a seguir.

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

Para identificar um fluxo de dados, siga um destes procedimentos:

- Se o fluxo de dados não estiver associado a uma propriedade do ativo, especifique o `alias` do fluxo de dados.
- Se o fluxo de dados estiver associado a uma propriedade do ativo, especifique um dos seguintes:
  - O `alias` do fluxo de dados.
  - O `assetId` e `propertyId` que identifica a propriedade do ativo.

ListTimeSeries

Use a operação `ListTimeSeries` da API para verificar se você excluiu com êxito um fluxo de dados.

Para recuperar uma lista paginada de fluxos de dados, execute o comando a seguir.

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

Ingestão de dados usando a API AWS IoT SiteWise

Use a AWS IoT SiteWise API para enviar dados industriais com data e hora às propriedades de atributo e medição de seus ativos. A API aceita uma carga que contém estruturas timestamp-quality-value (TQV).

Use a BatchPutAssetPropertyValueoperação para carregar seus dados. Com essa operação, você pode carregar várias entradas de dados ao mesmo tempo para coletar dados de vários dispositivos e enviar tudo em uma única solicitação.

> **Important**
>
> A BatchPutAssetPropertyValueoperação está sujeita às seguintes cotas:
>
> - Até 10 entradas por solicitação.
> - Até 10 valores de propriedade (pontos de dados TQV) por entrada.
> - AWS IoT SiteWise rejeita quaisquer dados com um timestamp datado de mais de 7 dias no passado ou mais de 10 minutos no futuro.

Para obter mais informações sobre essas cotas, consulte BatchPutAssetPropertyValuea Referência da AWS IoT SiteWise API.

Para identificar uma propriedade do ativo, especifique uma das seguintes opções:

- O `assetId` fim `propertyId` da propriedade do ativo para a qual os dados são enviados.
- O `propertyAlias`, que é um alias de fluxo de dados (por exemplo, `/company/windfarm/3/turbine/7/temperature`). Para usar esta opção, primeiro você deve definir o apelido da propriedade do seu ativo. Para definir aliases de propriedades, consulteMapeamento de fluxos de dados industriais para propriedades de ativos.

O exemplo a seguir demonstra como enviar leituras de temperatura e rotações por minuto (RPM) de uma turbina eólica a partir de uma carga útil armazenada em um arquivo JSON.

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

O exemplo de carga no `batch-put-payload.json` contém o conteúdo a seguir.

```
{
  "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 na carga contém um `entryId` que você pode definir como qualquer string exclusiva. Se qualquer entrada de solicitação falhar, cada erro conterá o `entryId` da solicitação correspondente, para que você saiba quais solicitações tentar novamente.

Cada estrutura na lista de `propertyValues` é uma estrutura timestamp-quality-value (TQV) que contém a, a `evalue`, `timestamp` opcionalmente, a. `quality`

- `value` – uma estrutura contendo um dos valores a seguir, a depender do tipo de propriedade sendo definida:
  - `booleanValue`
  - `doubleValue`
  - `integerValue`
  - `stringValue`
- `timestamp` – uma estrutura que contém o horário epoch Unix atual em segundos `timeInSeconds`. Você também pode definir a `offsetInNanos` chave na `timestamp` estrutura se tiver dados temporalmente precisos. AWS IoT SiteWise rejeita quaisquer pontos de dados com carimbos de data e hora anteriores a 7 dias ou mais recentes que 10 minutos no futuro.
- `quality` – (opcional) uma das seguintes strings de qualidade:
  - `GOOD` – (padrão) os dados não são afetados por nenhum problema.
  - `BAD` – os dados são afetados por um problema, como a falha do sensor.
  - `UNCERTAIN` – os dados são afetados por um problema, como a imprecisão do sensor.

Para obter mais informações sobre como AWS IoT SiteWise lidar com a qualidade de dados em cálculos, consulte Qualidade de dados em expressões de fórmulas.

Ingestão de dados usando regras AWS IoT Core

Envie dados para AWS IoT SiteWise AWS IoT coisas e outros AWS serviços usando regras em AWS IoT Core. As regras transformam as mensagens do MQTT e realizam ações para interagir com AWS os serviços. A ação da AWS IoT SiteWise regra encaminha os dados das mensagens para a BatchPutAssetPropertyValueoperação a partir da AWS IoT SiteWise API. Para obter mais informações, consulte Rules e a AWS IoT SiteWise ação no AWS IoT Developer Guide.

Para seguir um tutorial que mostra as etapas necessárias para configurar uma regra que ingere dados por meio das sombras do dispositivo, consulte. Ingestão de dados de coisas AWS IoT

Você também pode enviar dados AWS IoT SiteWise de outros AWS serviços. Para ter mais informações, consulte Interagindo com outros serviços AWS.

Tópicos

- Concedendo AWS IoT o acesso necessário
- Configurando a ação da AWS IoT SiteWise regra
- Reduzir custos com a ingestão básica

Concedendo AWS IoT o acesso necessário

Você usa funções do IAM para controlar os AWS recursos aos quais cada regra tem acesso. Antes de criar uma regra, você deve criar uma função do IAM com uma política que permita que a regra execute ações no AWS recurso necessário. AWS IoT assume essa função ao executar uma regra.

Se você criar a ação da regra no AWS IoT console, poderá escolher um ativo raiz para criar uma função que tenha acesso a uma hierarquia de ativos selecionada. Para obter mais informações sobre como definir manualmente uma função para uma regra, consulte Conceder AWS IoT o acesso necessário e Aprovar as permissões de função no Guia do AWS IoT desenvolvedor.

Para a ação da AWS IoT SiteWise regra, você deve definir uma função que permita `iotsitewise:BatchPutAssetPropertyValue` acesso às propriedades do ativo para as quais a regra envia dados. Para melhorar a segurança, você pode especificar um caminho AWS IoT SiteWise de hierarquia de ativos na `Condition` propriedade.

O exemplo de política de confiança a seguir concede acesso a um ativo específico e seus filhos.

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

Remova o `Condition` da política para permitir o acesso a todos os seus ativos. O exemplo de política de confiança a seguir concede acesso a todos os ativos na região atual.

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

Configurando a ação da AWS IoT SiteWise regra

A ação da AWS IoT SiteWise regra envia dados da mensagem MQTT que iniciou a regra para as propriedades do ativo em AWS IoT SiteWise. Você pode carregar várias entradas de dados em diferentes propriedades de ativos ao mesmo tempo, para enviar atualizações para todos os sensores

de um dispositivo em uma mensagem. Também é possível fazer upload de vários pontos de dados de uma vez para cada entrada de dados.

> **Note**
>
> Quando você envia dados para AWS IoT SiteWise com a ação de regra, seus dados devem atender a todos os requisitos da `BatchPutAssetPropertyValue` operação. Por exemplo, seus dados não podem ter um time stamp com mais de 7 dias do horário Unix epoch atual. Para obter mais informações, consulte Ingerir dados com a API do AWS IoT SiteWise.

Para cada entrada de dados na ação de regra, você identifica uma propriedade de ativo e especifica o time stamp, a qualidade e o valor de cada ponto de dados para essa propriedade de ativo. A ação da regra espera strings para todos os parâmetros.

Para identificar uma propriedade de ativo em uma entrada, especifique um dos seguintes elementos:

- O Asset ID (ID do ativo) (`assetId`) e o Property ID (ID da propriedade) (`propertyId`) da propriedade de ativo para a qual você está enviando dados. Você pode encontrar o ID do ativo e o ID da propriedade usando Console do AWS IoT SiteWise o. Se você souber o ID do ativo, poderá usar o AWS CLI to call DescribeAssetpara encontrar o ID da propriedade.
- O Property alias (Alias da propriedade) (`propertyAlias`), que é um alias de fluxo de dados (por exemplo, `/company/windfarm/3/turbine/7/temperature`). Para usar esta opção, primeiro você deve definir o apelido da propriedade do seu ativo. Para saber como definir apelidos de propriedades, consulte Mapeamento de fluxos de dados industriais para propriedades de ativos.

Para o timestamp em cada entrada, use o timestamp informado pelo seu equipamento ou o timestamp fornecido por. AWS IoT Core O time stamp tem dois parâmetros:

- Time in seconds (Tempo em segundos) (`timeInSeconds`) – o horário Unix epoch, em segundos, no qual o sensor ou equipamento reportou os dados.
- Offset in nanos (Deslocamento em nanossegundos) (`offsetInNanos`) – (opcional) o deslocamento em nanossegundos do tempo em segundos.

> **Important**
>
> Se seu time stamp for uma string, tiver uma parte decimal ou não estiver em segundos, AWS IoT SiteWise rejeitará a solicitação. Você deve converter o time stamp em segundos e o deslocamento em nanossegundos. Use os recursos do mecanismo de AWS IoT regras para converter o carimbo de data/hora. Para mais informações, consulte:
>
> - Obter time stamps para dispositivos que não informam a hora exata
> - Conversão de time stamps em formato de string

Também é possível usar modelos de substituição para vários parâmetros na ação para executar cálculos, invocar funções e extrair valores da carga de mensagem. Para obter mais informações, consulte Modelos de substituição no Guia do desenvolvedor do AWS IoT .

> **Note**
>
> Como uma expressão em um modelo de substituição é avaliado separadamente da instrução `SELECT`, não é possível usar um modelo de substituição para fazer referência a um alias criado usando uma cláusula `AS`. Você pode fazer referência somente às informações presentes na carga original, além das funções e dos operadores compatíveis.

Tópicos

Obter time stamps para dispositivos que não informam a hora exata

Se seu sensor ou equipamento não reportar dados de tempo precisos, obtenha a hora atual da época do Unix no mecanismo de AWS IoT regras com timestamp (). Essa função reporta o tempo em milissegundos, portanto, é necessário converter o valor para tempo em segundos e deslocamento em nanossegundos. Para fazer isso, use as seguintes conversões:

- Para Time in seconds (Tempo em segundos) (`timeInSeconds`), use **`${floor(timestamp() / 1E3)}`** para converter o tempo de milissegundos para segundos.
- Para Offset in nanos (Deslocamento em nanossegundos) (`offsetInNanos`), use **`${(timestamp() % 1E3) * 1E6}`** para calcular o deslocamento em nanossegundos do time stamp.

Conversão de time stamps em formato de string

Se seu sensor ou equipamento reportar dados de hora em formato de string (por exemplo,`2020-03-03T14:57:14.699Z`), use time_to_epoch (String, String). Essa função insere o time stamp e o padrão de formato como parâmetros e gera o tempo em milissegundos. Em seguida, você deve converter o tempo para tempo em segundos e o deslocamento em nanossegundos. Para fazer isso, use as seguintes conversões:

- Para Time in seconds (Tempo em segundos) (`timeInSeconds`), use **`${floor(time_to_epoch("2020-03-03T14:57:14.699Z", "yyyy-MM-dd'T'HH:mm:ss'Z'") / 1E3)}`** para converter o string do time stamp de milissegundos para segundos.
- Para Offset in nanos (Deslocamento em nanossegundos) (`offsetInNanos`), use **`${(time_to_epoch("2020-03-03T14:57:14.699Z", "yyyy-MM-dd'T'HH:mm:ss'Z'") % 1E3) * 1E6}`** para calcular o deslocamento em nanossegundos do string do time stamp.

> **Note**
>
> A função `time_to_epoch` suporta sequências de time stamp com precisão de até milissegundos. Para converter cadeias de caracteres com precisão de microssegundos ou nanossegundos, configure uma AWS Lambda função que sua regra chama para converter o timestamp em valores numéricos. Para ter mais informações, consulte Convertendo strings de time stamp de precisão de nanossegundos.

Convertendo strings de time stamp de precisão de nanossegundos

Se o seu dispositivo enviar informações de time stamp no formato de string (por exemplo, `2020-03-03T14:57:14.699728491Z`), use as etapas a seguir para configurar suaa ação da regra. Você pode criar uma AWS Lambda função que converta o timestamp de uma string em Time

in seconds (**`timeInSeconds`**) e Offset em nanos (). `offsetInNanos` Em seguida, use aws_lambda (functionArn, inputJSON) em seus parâmetros de ação de regra para invocar essa função Lambda e usar a saída em sua regra.

> **Note**
>
> Esta seção contém instruções avançadas que presumem que você esteja familiarizado com como criar os recursos a seguir:
>
> - Funções do Lambda. Para obter mais informações, consulte Criar uma função do Lambda com o console ou Uso do Lambda com a AWS CLI noAWS Lambda Guia do desenvolvedor.
> - AWS IoT regras com a ação da AWS IoT SiteWise regra. Para ter mais informações, consulte Ingestão de dados usando regras AWS IoT Core.

Para criar uma ação de AWS IoT SiteWise regra que analisa cadeias de caracteres de carimbo de data/hora

1. Crie uma função do Lambda com as seguintes propriedades:

   - Nome da função – use um nome descritivo de função (por exemplo, **`ConvertNanosecondTimestampFromString`**).
   - Tempo de execução — Use um tempo de execução do Python 3, como o Python 3.11 (). `python3.11`
   - Permissões — Crie uma função com permissões básicas do Lambda () AWS LambdaBasicExecutionRole.
   - Camadas — Adicione a camada AWS SDKpandas-Python311 para usar a função Lambda. `numpy`
   - Código de função – use o código de função a seguir, que consome um argumento de string chamado `timeInSeconds` e emite na saída os valores `timestamp` e `offsetInNanos` para esse time stamp.

     ```
     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
    }
```

Essa função Lambda insere cadeias de caracteres de timestamp no formato ISO 8601 usando datetime64 de. NumPy

> **Note**
>
> Se suas strings de time stamp não estiverem no formato ISO 8601, você poderá implementar uma solução com pandas que defina seu formato. Para obter mais informações, consulte pandas.to_datetime.

2. Ao configurar a AWS IoT SiteWise ação para sua regra, use os seguintes modelos de substituição para Tempo em segundos (`timeInSeconds`) e Deslocamento em nanos (). `offsetInNanos` Esses modelos de substituição presumem que a carga de mensagem contém a string de time stamp em `timestamp`. A função `aws_lambda` consome uma estrutura JSON para seu segundo parâmetro, assim você pode modificar os modelos de substituição abaixo, se necessário.

   - Para Time in seconds (Tempo em segundos) (`timeInSeconds`), use o seguinte modelo de substituição.

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

   - Para Offset in nanos (Deslocamento em nanos) (`offsetInNanos`), use o seguinte modelo de substituição.

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

Para cada parâmetro, substitua *region* e *account-id* por sua região e ID da AWS conta. Se você usou um nome diferente para sua função do Lambda, altere-o também.

3. Conceda AWS IoT permissões para invocar sua função com a `lambda:InvokeFunction` permissão. Para obter mais informações, consulte aws_lambda(functionArn, inputJson).
4. Teste sua regra (por exemplo, use o cliente de teste AWS IoT MQTT) e verifique se ela AWS IoT SiteWise recebe os dados que você envia.

   Se sua regra não funcionar como esperado, consulte Solução de problemas de uma ação de AWS IoT SiteWise regra.

> **Note**
>
> Esta solução invoca a função do Lambda duas vezes para cada string de time stamp. Você pode criar outra regra para reduzir o número de invocações de função do Lambda se sua regra manipular vários pontos de dados que têm o mesmo time stamp em cada carga. Para fazer isso, crie uma regra com uma ação de publicar novamente que invoque o Lambda e publique a carga original com a string de time stamp convertida para `timeInSeconds` e `offsetInNanos`. Em seguida, crie uma regra com uma ação de AWS IoT SiteWise regra para consumir a carga convertida. Com essa abordagem, você reduz o número de vezes que a regra invoca o Lambda, mas aumenta o número de ações de AWS IoT regras executadas. Considere a definição de preço de cada serviço caso você aplique essa solução ao seu caso de uso.

Configurações de regra de exemplo

Esta seção contém exemplos de configurações de regras para criar uma regra com uma AWS IoT SiteWise ação.

Example O exemplo de ação de regra que usa aliases de propriedade como tópicos de mensagem

O exemplo a seguir cria uma regra com uma AWS IoT SiteWise ação que usa o tópico (por meio de topic ()) como alias da propriedade para identificar as propriedades do ativo. Use este exemplo para definir uma regra para a ingestão de dados de tipo duplo em todas as turbinas eólicas em todos os parques eólicos. Este exemplo exige que você defina aliases de propriedade em todas as propriedades dos ativos da turbina. Você precisa definir uma segunda regra semelhante para ingerir dados de tipo inteiro.

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

O exemplo de carga no `sitewise-rule-payload.json` contém o conteúdo a seguir.

```
{
  "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"
      }
    }
```

```
  ]
}
```

Com essa ação de regra, envie a seguinte mensagem para um alias de propriedade de turbina eólica (por exemplo,`/company/windfarm/3/turbine/7/temperature`) como um tópico para ingerir dados.

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

Example Exemplo de ação de regra que usa time stamp() para determinar o tempo

O exemplo a seguir cria uma regra com uma AWS IoT SiteWise ação que identifica uma propriedade do ativo por IDs e usa timestamp () para determinar a hora atual.

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

O exemplo de carga no `sitewise-rule-payload.json` contém o conteúdo a seguir.

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

Com essa ação de regra, envie a seguinte mensagem `my/asset/property/topic` para ingerir dados.

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

Solucionar problemas de ação de regra do

Para solucionar problemas de sua ação de AWS IoT SiteWise regra AWS IoT Core, configure CloudWatch Logs ou configure uma ação de erro de republicação para sua regra. Para ter mais informações, consulte Solução de problemas de uma ação de AWS IoT SiteWise regra.

Reduzir custos com a ingestão básica

AWS IoT Core fornece um recurso chamado Basic Ingest, que você pode usar para enviar dados AWS IoT Core sem incorrer em custos de AWS IoT mensagens. A Ingestão básica otimiza fluxo de dados para cargas de ingestão de dados de volume alto removendo o agente de mensagem de publicação/assinatura do caminho de ingestão. É possível usar a Ingestão básica se souber para quais regras as mensagens devem ser roteadas.

Para usar a Ingestão básica, envie mensagens diretamente a uma regra específica usando um tópico especial, `$aws/rules/rule-name`. Por exemplo, para enviar uma mensagem a uma regra chamada `SiteWiseWindFarmRule`, envie uma mensagem ao tópico`$aws/rules/SiteWiseWindFarmRule`.

Se a ação de regra usa modelos de substituição que contêm topic(Decimal), é possível transmitir o tópico original ao fim do tópico especial de Ingestão básica, como `$aws/rules/rule-name/original-topic`. Por exemplo, para usar a Ingestão básica com o exemplo de alias de propriedade do parque de energia eólica da seção anterior, é possível enviar mensagens ao tópico a seguir.

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

> **Note**
>
> O exemplo acima inclui uma segunda barra (`//`) porque AWS IoT remove o prefixo Basic Ingest (`$aws/rules/rule-name/`) do tópico que está visível para a ação da regra. Neste exemplo, a regra recebe o tópico `/company/windfarm/3/turbine/7/temperature`.

Para obter mais informações, consulte Reducing messaging costs with basic ingest no AWS IoT Developer Guide.

Ingestão de dados de AWS IoT Events

Com AWS IoT Events, você pode criar aplicativos complexos de monitoramento de eventos para sua frota de IoT na AWS nuvem. Use a SiteWise ação de IoT AWS IoT Events para enviar dados às propriedades do ativo AWS IoT SiteWise quando ocorrer um evento.

AWS IoT Events foi projetado para agilizar o desenvolvimento de aplicativos de monitoramento de eventos para dispositivos e sistemas de IoT na AWS nuvem. Usando AWS IoT Events, você pode:

- Detecte e responda a mudanças, anomalias ou condições específicas em toda a sua frota de IoT.
- Melhore sua eficiência operacional e possibilite o gerenciamento proativo do seu ecossistema de IoT.

Ao se integrar por AWS IoT SiteWise meio da AWS IoT SiteWise ação, AWS IoT Events amplia seus recursos, permitindo que você atualize automaticamente as propriedades do ativo AWS IoT SiteWise em resposta a eventos específicos. Essa interação pode simplificar a ingestão e o gerenciamento de dados. Ele também pode capacitar você com insights acionáveis.

Para obter mais informações, consulte os tópicos a seguir no Guia do desenvolvedor do AWS IoT Events .

- O que é AWS IoT Events?
- Ações do AWS IoT Events
- Ação de IoT SiteWise

Usando o gerenciador de AWS IoT Greengrass streams

AWS IoT Greengrass O gerenciador de fluxo é um recurso de integração que facilita a transferência de fluxos de dados de fontes locais para a AWS nuvem. Ele atua como uma camada intermediária que gerencia os fluxos de dados, permitindo que os dispositivos que operam na borda coletem e armazenem dados antes de serem enviados AWS IoT SiteWise, para análise e processamento adicionais.

Adicione um destino de dados configurando uma fonte local no AWS IoT SiteWise console. Você também pode usar o gerenciador de streams em sua AWS IoT Greengrass solução personalizada para ingerir dados para AWS IoT SiteWise.

> **Note**
>
> Para ingerir dados de fontes OPC-UA, configure um gateway AWS IoT SiteWise Edge que seja executado em. AWS IoT Greengrass Para ter mais informações, consulte Usando gateways SiteWise Edge.

Para obter mais informações sobre como configurar um destino para dados de origem local, consulteConfigurar fontes de dados.

Para obter mais informações sobre como ingerir dados usando o gerenciador de streams em uma AWS IoT Greengrass solução personalizada, consulte os tópicos a seguir no Guia do AWS IoT Greengrass Version 2 desenvolvedor:

- O que AWS IoT Greengrassé
- Gerenciar streams de dados no núcleo do AWS IoT Greengrass core
- Exportação de dados para propriedades AWS IoT SiteWise de ativos

Ingestão de dados usando a API CreateBulkImportJob

Use a `CreateBulkImportJob` API para importar grandes quantidades de dados do Amazon S3. Seus dados devem ser salvos no formato CSV no Amazon S3. Os arquivos de dados podem ter as seguintes colunas.

> **Note**
>
> Para identificar uma propriedade do ativo, especifique uma das opções a seguir.
>
> - O `ASSET_ID` e `PROPERTY_ID` da propriedade do ativo para o qual você está enviando dados.
> - O `ALIAS`, que é um alias de fluxo de dados (por exemplo, `/company/windfarm/3/turbine/7/temperature`). Para usar esta opção, primeiro você deve definir o apelido da propriedade do seu ativo. Para saber como definir apelidos de propriedades, consulte the section called “Mapeamento de fluxos de dados industriais para propriedades de ativos”.

- `ALIAS` – O alias de propriedade que identifica a propriedade, como um caminho de stream de dados do servidor de OPC-UA (por exemplo, `/company/windfarm/3/turbine/7/temperature`). Para ter mais informações, consulte Mapeamento de fluxos de dados industriais para propriedades de ativos.
- `ASSET_ID` – O ID do ativo.
- `PROPERTY_ID` – O ID da propriedade do ativo.
- `DATA_TYPE` – O tipo de dado da propriedade pode ser um destes.
  - `STRING` – uma string com até 1024 bytes.
  - `INTEGER` – um número inteiro assinado de 32 bits com intervalo [-2.147.483.648, 2.147.483.647].
  - `DOUBLE` – um número de ponto flutuante com intervalo [-10^100, 10^100] e precisão dupla IEEE 754.
  - `BOOLEAN` – `true` ou `false`.
- `TIMESTAMP_SECONDS` – O time stamp do ponto de dados, no período Unix.
- `TIMESTAMP_NANO_OFFSET` – O deslocamento em nanossegundos convertido de `TIMESTAMP_SECONDS`.

- `QUALITY` – (opcional) A qualidade do valor da propriedade do ativo. O valor pode ser um dos seguintes:
  - `GOOD` – (padrão) os dados não são afetados por nenhum problema.
  - `BAD` – os dados são afetados por um problema, como a falha do sensor.
  - `UNCERTAIN` – os dados são afetados por um problema, como a imprecisão do sensor.

  Para obter mais informações sobre como AWS IoT SiteWise lidar com a qualidade de dados em cálculos, consulte Qualidade de dados em expressões de fórmulas.
- `VALUE` – O valor da propriedade do ativo.

Example arquivo(s) de dados no 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 fornece as seguintes operações de API para criar um trabalho de importação em massa e obter informações sobre um trabalho existente.

- CreateBulkImportJob— Cria um novo trabalho de importação em massa.
- DescribeBulkImportJob— Recupera informações sobre um trabalho de importação em massa.
- ListBulkImportJob— Recupera uma lista paginada de resumos de todos os trabalhos de importação em massa.

Criar um trabalho de importação em massa (AWS CLI)

Use a operação de CreateBulkImportJobAPI para transferir dados do Amazon S3 para o. AWS IoT SiteWise Use a CreateBulkImportJobAPI para ingerir dados em pequenos lotes de forma econômica. O exemplo a seguir usa AWS CLI.

> **Important**
>
> Antes de criar um trabalho de importação em massa, você deve habilitar o nível AWS IoT SiteWise quente ou o nível AWS IoT SiteWise frio. Para ter mais informações, consulte Definir configurações de armazenamento.
> A importação em massa foi projetada para armazenar dados históricos em AWS IoT SiteWise. Ele não inicia cálculos ou notificações no nível AWS IoT SiteWise quente ou no nível AWS IoT SiteWise frio.

Execute o seguinte comando . Substitua *file-name* pelo nome do arquivo que contém a configuração de trabalho de importação em massa.

```
aws iotsitewise create-bulk-import-job --cli-input-json file://file-name.json
```

Example Configuração do trabalho de importação em massa

Veja a seguir exemplos de definições de configuração:

- Substitua *adaptive-ingestion-flag* por `true` ou `false`.
  - Se definido como`false`, o trabalho de importação em massa ingere dados históricos em AWS IoT SiteWise.
  - Se definido como`true`, o trabalho de importação em massa faz o seguinte:
    - Ingere novos dados em. AWS IoT SiteWise
    - Calcula métricas e transformações, além de oferecer suporte a notificações de dados com um registro de data e hora em sete dias.
- Substitua *delete-files-after-import-flag* por `true` para excluir os dados do bucket de dados do S3 após serem ingeridos no armazenamento de camada AWS IoT SiteWise quente.
- Substitua o *error-bucket* pelo nome do bucket do Amazon S3 para o qual os erros associados a esse trabalho de importação em massa são enviados.

- *error-bucket-prefix*Substitua pelo prefixo do bucket do Amazon S3 para o qual os erros associados a esse trabalho de importação em massa são enviados.

  O Amazon S3 usa o prefixo como nome de pasta para organizar os dados no bucket. Cada objeto em um bucket do Amazon S3 tem uma chave que é seu identificador exclusivo no bucket. Cada objeto em um bucket tem exatamente uma chave. O prefixo deve terminar com uma barra (/). Para obter mais informações, consulte Organizing objects using prefixes no Guia do usuário do Amazon Simple Storage Service.
- Substitua *data-bucket* pelo nome do bucket do Amazon S3 do qual os dados são importados.
- *data-bucket-key*Substitua pela chave do objeto Amazon S3 que contém seus dados. Cada objeto tem uma chave que é um identificador exclusivo. Cada objeto tem exatamente uma chave.
- *data-bucket-version-id*Substitua pelo ID da versão para identificar uma versão específica do objeto Amazon S3 que contém seus dados. Esse parâmetro é opcional.
- Substitua o *column-name* pelo nome da coluna especificado no arquivo .csv.
- Substitua o *job-name* por um nome exclusivo que identifique o trabalho de importação em massa.
- *job-role-arn*Substitua pela função do IAM que AWS IoT SiteWise permite ler dados do Amazon S3.

> **Note**
>
> Certifique-se de que sua função tem as permissões do exemplo a seguir: Substitua o *data-bucket* pelo nome do bucket do Amazon S3 que contém seus dados. Além disso, substitua o *bucket de erros* pelo nome do bucket do Amazon S3 para o qual os erros associados a esse trabalho de importação em massa são enviados.

```
{
    "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 Retorno

```
{
   "jobId":"f8c031d0-01d1-4b94-90b1-afe8bb93b7e5",
   "jobStatus":"PENDING",
   "jobName":"myBulkImportJob"
}
```

Descrever um trabalho de importação em massa (AWS CLI)

Use a operação DescribeBulkImportJobda API para recuperar informações sobre um trabalho de importação em massa. O exemplo a seguir usa AWS CLI.

Substitua *Job-ID* pelo ID do trabalho de importação em massa que deseja recuperar.

```
aws iotsitewise describe-bulk-import-job --job-id job-ID
```

Example Retorno

```
{
   "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"
}
```

Listar trabalhos de importação em massa (AWS CLI)

Use a operação da ListBulkImportJobsAPI para recuperar uma lista paginada de resumos de todos os trabalhos de importação em massa. O exemplo a seguir usa AWS CLI.

```
aws iotsitewise list-bulk-import-jobs --filter COMPLETED
```

Example Retorno

```
{
   "jobSummaries":[
      {
         "id":"bdbbfa52-d775-4952-b816-13ba1c7cb9da",
         "name":"myBulkImportJob",
         "status":"COMPLETED"
      },
      {
         "id":"15ffc641-dbd8-40c6-9983-5cb3b0bc3e6b",
         "name":"myBulkImportJob2",
         "status":"RUNNING"
      }
   ]
}
```

Usando gateways SiteWise Edge

Um gateway AWS IoT SiteWise Edge serve como intermediário entre seu equipamento industrial e. AWS IoT SiteWise O gateway SiteWise Edge é executado com AWS IoT Greengrass V2 suporte à coleta e processamento de dados no local. Você pode usar o AWS OpsHub for AWS IoT SiteWise para gerenciar seus gateways SiteWise Edge e monitorar as operações no local.

Você pode monitorar dados localmente em suas instalações usando portais de SiteWise monitoramento em seus dispositivos locais. Para ter mais informações, consulte Habilitar seu portal na borda.

Tópicos

SiteWise Requisitos do gateway Edge

AWS IoT SiteWise Os gateways Edge funcionam AWS IoT Greengrass V2 como um conjunto de AWS IoT Greengrass componentes que oferecem suporte à coleta, processamento e publicação de

dados no local. Para configurar um gateway SiteWise Edge executado em AWS IoT Greengrass V2, você deve criar um gateway no Nuvem AWS e executar o software SiteWise Edge Gateway para configurar seu dispositivo local.

Requisitos

Os dispositivos locais devem atender aos seguintes requisitos para instalar e executar o software SiteWise Edge Gateway.

- Suporta a versão v2.3.0 ou mais recente do software AWS IoT Greengrass V2 Core. Para obter mais informações, consulte Requisitos no AWS IoT Greengrass Version 2 Guia do Desenvolvedor.
- Uma das plataformas a seguir são compatíveis:
  - SISTEMA OPERACIONAL: Ubuntu 20.04 ou posterior

    Arquitetura: x86_64 (AMD64) ou ARMv8 (Aarch64)
  - SO: Red Hat Enterprise Linux (RHEL) 8

    Arquitetura: x86_64 (AMD64) ou ARMv8 (Aarch64)
  - SO: Amazon Linux 2

    Arquitetura: x86_64 (AMD64) ou ARMv8 (Aarch64)
  - SO: Debian 11

    Arquitetura: x86_64 (AMD64) ou ARMv8 (Aarch64)
  - SO: Windows Server 2019 e posterior

    Arquitetura: x86_64 (AMD64)

  > **Note**
  >
  > As plataformas ARM oferecem suporte a gateways SiteWise Edge somente com o Data Collection Pack. O pacote de processamento de dados não é suportado.

- Mínimo de 4 GB de RAM.
- Espaço mínimo de 10 GB em disco disponível para o software SiteWise Edge Gateway.
- Se você planeja processar dados na borda com AWS IoT SiteWise, seu dispositivo local também deve atender aos seguintes requisitos:
  - Tem um processador quad-core x86 de 64 bits.

  - Ter pelo menos 16 GB de RAM.
  - Tem pelo menos 32 GB de RAM se estiver usando o Windows.
  - Ter pelo menos 256 GB de espaço livre em disco.
- Os requisitos mínimos de espaço em disco e capacidade computacional dependem de vários fatores que são exclusivos de sua implementação e caso de uso.
  - O espaço em disco necessário para armazenar dados em cache para conectividade com a Internet intermitente depende dos seguintes fatores:
    - Número de fluxos de dados carregados
    - Pontos de dados por fluxo de dados por segundo
    - Tamanho de cada ponto de dados
    - Velocidades de comunicação
    - O tempo de inatividade de rede esperado
  - A capacidade computacional necessária para sondar e carregar dados depende dos seguintes fatores:
    - Número de fluxos de dados carregados
    - Pontos de dados por fluxo de dados por segundo
- Configure seu dispositivo local para acessar o seguinte bucket S3:`iot-sitewise-gateway-<region>-748875242063`.
- Configure seu dispositivo local para garantir que as seguintes portas estejam acessíveis:
  - O dispositivo local deve permitir o tráfego de entrada da rede na porta 443.
  - O dispositivo local deve permitir tráfego de saída nas portas 443 e 8883.

    Para obter uma lista completa dos pontos finais de serviço de saída necessários, consulte Pontos de extremidade de serviço necessários para AWS IoT SiteWise gateways Edge.
  - As seguintes portas são reservadas para uso por AWS IoT SiteWise: 80, 443, 3001, 4569, 4572, 8000, 8081, 8082, 8084, 8085, 8445, 8086, 9000, 9500, 11080 e 50010. Usar uma porta reservada para tráfego pode resultar no encerramento de uma conexão.

> **Note**
>
> O componente AWS IoT Greengrass V2 Stream Manager tem seus próprios requisitos. Para obter mais informações, consulte Configuração no Guia do AWS IoT Greengrass Version 2 desenvolvedor.

- Java Runtime Environment (JRE) versão 11 ou superior. O Java deve estar disponível na variável de ambiente do PATH no dispositivo. Para usar o Java para desenvolver componentes personalizados, é necessário instalar um Java Development Kit (JDK). Recomendamos que você use o Amazon Corretto ou o OpenJDK.

Você deve ter as seguintes permissões para usar os gateways do SiteWise Edge:

> **Note**
>
> Se você usar o AWS IoT SiteWise console para criar seu gateway SiteWise Edge, essas permissões serão adicionadas para você.

- A função do IAM para seu gateway SiteWise Edge deve permitir que você use um gateway SiteWise Edge em um AWS IoT Greengrass V2 dispositivo para processar dados de modelos de ativos e dados de ativos.

  O perfil permite que o seguinte serviço presuma a função: `credentials.iot.amazonaws.com`.

  Detalhes da permissão

  A função deve ter as seguintes permissões:

  - `iotsitewise` — Permitir que as entidades principais recuperem dados do modelo de ativo e dados do ativo na borda.
  - `iot`— Permite que seus AWS IoT Greengrass V2 dispositivos interajam com AWS IoT.
  - `logs`— Permite que seus AWS IoT Greengrass V2 dispositivos enviem registros para o Amazon CloudWatch Logs.
  - `s3`— Permite que seus AWS IoT Greengrass V2 dispositivos baixem artefatos de componentes personalizados do 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": "*"
        }
    ]
}
```

Criando um gateway SiteWise Edge

Você pode usar o AWS IoT SiteWise console para criar um gateway SiteWise Edge. Este procedimento detalha como criar um gateway SiteWise Edge auto-hospedado que você instalará em seu próprio hardware. Para obter informações sobre a criação de um gateway SiteWise Edge executado no Siemens Industrial Edge, consulteRunning SiteWise Edge na Siemens Industrial Edge.

Crie um gateway SiteWise Edge

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, escolha Edge gateways.
3. Escolha Criar gateway.
4. Em Tipo de implantação, escolha Gateway auto-hospedado.

5. Insira um nome para seu gateway SiteWise Edge ou use o nome gerado por AWS IoT SiteWise.
6. Em Sistema operacional do dispositivo Greengrass, selecione o sistema operacional do dispositivo em que você instalará esse gateway SiteWise Edge.

   > **Note**
   >
   > O Pacote de Processamento de Dados está disponível somente em plataformas x86.

7. (Opcional) Para processar e organizar dados na borda, em Recursos do Edge, selecione Pacote de processamento de dados.

   > **Note**
   >
   > Para conceder aos grupos de usuários em seu diretório corporativo acesso a esse gateway do SiteWise Edge, consulte Configurar o recurso de borda

8. (Opcional) Na configuração avançada, faça o seguinte:

   - Para o dispositivo de núcleo do Greengrass, escolha uma das seguintes opções:

     - Configuração padrão — usa AWS automaticamente as configurações padrão para criar um dispositivo principal do Greengrass no. AWS IoT Greengrass V2

       1. Insira um nome para o dispositivo principal do Greengrass ou use o nome gerado por. AWS IoT SiteWise

     - Configuração avançada — Escolha essa opção se quiser usar um dispositivo principal do Greengrass existente ou criar um manualmente.

       1. Escolha um dispositivo de núcleo do Greengrass ou escolha Criar dispositivo de núcleo do Greengrass para criar um no console de AWS IoT Greengrass V2 . Para obter mais informações, consulte Configurando dispositivos AWS IoT Greengrass V2 principais no Guia do AWS IoT Greengrass Version 2 desenvolvedor.

9. Escolha Criar gateway.
10. Na caixa de diálogo do instalador do gateway Generate SiteWise Edge, escolha Gerar e baixar. AWS IoT SiteWise gera automaticamente um instalador que você pode usar para configurar seu dispositivo local.

> **Important**
>
> Certifique-se de salvar o arquivo do instalador em um local seguro. Você usará o arquivo posteriormente.

Agora que você criou o gateway SiteWise Edge, adicione fontes de dados, configure o componente editor e faça com que seu gateway SiteWise Edge receba dados e os envie para a AWS nuvem.

Instalando o software SiteWise Edge Gateway em seu dispositivo local

Depois de criar um gateway SiteWise Edge, você precisa instalar o software SiteWise Edge gateway em seu dispositivo local. SiteWise O software Edge Gateway pode ser instalado em dispositivos locais que tenham sistemas operacionais de servidor Linux ou Windows instalados.

> **Important**
>
> Verifique se o dispositivo local está conectado à Internet.

Linux

O procedimento a seguir usa SSH para se conectar ao seu dispositivo local. Como alternativa, você pode usar uma unidade flash USB ou outras ferramentas para transferir o arquivo do instalador para o dispositivo local. Se você não quiser usar o SSH, vá para a Etapa 2: Instale o software SiteWise Edge Gateway abaixo.

Pré-requisitos de SSH

Antes de se conectar ao seu dispositivo usando SSH, preencha os seguintes pré-requisitos.

- Obtenha o endereço IP do seu dispositivo.
- Obtenha o nome de usuário para se conectar ao seu dispositivo.
- Instale um cliente SSH no computador local conforme necessário.

O computador local pode ter um cliente SSH instalado por padrão. Isso pode ser verificado ao digitar ssh na linha de comando. Se o seu computador não reconhecer o comando, é possível instalar um cliente SSH.

- Linux e macOS – baixe e instale o OpenSSH. Para obter mais informações, consulte https://www.openssh.com.

Etapa 1: Copie o instalador para seu dispositivo de gateway SiteWise Edge

As instruções a seguir explicam como se conectar ao seu dispositivo local usando um cliente SSH.

1. Para se conectar ao seu dispositivo, execute o seguinte comando em uma janela de terminal em seu computador, substituindo *nome de usuário* e *IP* por um nome de usuário com privilégios e endereço IP elevados.

```
ssh username@IP
```

2. Para transferir o arquivo do instalador AWS IoT SiteWise gerado para seu dispositivo de gateway SiteWise Edge, execute o comando a seguir.

> **Note**
>
> - *path-to-saved-installer*Substitua pelo caminho em seu computador que você usou para salvar o arquivo do instalador e pelo nome do arquivo do instalador.
> - Substitua o *endereço IP* pelo endereço IP do seu dispositivo local.
> - *directory-to-receive-installer*Substitua pelo caminho em seu dispositivo local que você usa para receber o arquivo do instalador.

```
scp path-to-saved-installer.sh user-name@IP-address:directory-to-receive-installer
```

Etapa 2: instalar o software SiteWise Edge Gateway

Nos procedimentos a seguir, execute os comandos em uma janela de terminal no seu dispositivo de gateway SiteWise Edge.

1. Dê ao arquivo do instalador a permissão de execução.

```
chmod +x path-to-installer.sh
```

2. Execute o instalador.

```
sudo ./path-to-installer.sh
```

Windows server

Pré-requisitos

Você deve ter os seguintes pré-requisitos para instalar o software SiteWise Edge Gateway:

- Windows Server 2019 ou posterior instalado
- Privilégios de administrador
- PowerShell versão 5.1 ou posterior instalada
- SiteWise Instalador do gateway Edge baixado para o Windows Server, onde será provisionado

Etapa 1: Executar PowerShell como administrador

1. No servidor Windows em que você deseja instalar o SiteWise Edge Gateway, faça login como administrador.
2. Entre PowerShellna barra de pesquisa do Windows.
3. Nos resultados da pesquisa, abra o menu de contexto (clique com o botão direito do mouse) no PowerShell aplicativo do Windows. Escolha Executar como administrador.

Etapa 2: instalar o software SiteWise Edge Gateway

Execute os comandos a seguir em uma janela de terminal no seu dispositivo SiteWise Edge Gateway.

1. Desbloqueie o instalador do gateway SiteWise Edge.

```
unblock-file path-to-installer.ps1
```

2. Execute o instalador.

```
./path-to-installer.ps1
```

> **Note**
>
> Se a execução do script estiver desabilitada no sistema, altere a política de execução do script para `RemoteSigned`.
>
> ```
> Set-ExecutionPolicy RemoteSigned
> ```

Habilitar o processamento de dados de borda

Você pode usar o AWS IoT SiteWise Edge para coletar, armazenar, organizar e monitorar dados do equipamento localmente. Você pode usar o SiteWise Edge para modelar seus dados industriais e o SiteWise Monitor para criar painéis para que sua equipe operacional visualize os dados localmente. Você pode processar seus dados localmente e enviá-los para o Nuvem AWS, ou processá-los localmente usando a AWS IoT SiteWise API.

Com o AWS IoT SiteWise Edge, você pode processar dados brutos localmente e optar por enviar somente dados agregados para o Nuvem AWS para otimizar o uso da largura de banda e os custos de armazenamento na nuvem.

> **Note**
>
> - AWS IoT SiteWise retém seus dados de borda em seus gateways SiteWise Edge por até 30 dias. O período de retenção de seus dados depende do espaço disponível em disco do seu dispositivo.
> - Se seu gateway SiteWise Edge tiver sido desconectado do Nuvem AWS por 30 dias, o Pacote de Processamento de Dados será automaticamente desativado.

Configurar o recurso de borda

AWS IoT SiteWise fornece os seguintes pacotes que seu gateway SiteWise Edge pode usar para determinar como coletar e processar seus dados. Selecione pacotes para habilitar recursos de borda para seu gateway SiteWise Edge.

- O Data Collection Pack permite que seu gateway SiteWise Edge colete dados de vários servidores OPC-UA e, em seguida, exporte os dados da borda para o. Nuvem AWS Ele se torna ativo depois que você adiciona fontes de dados ao seu gateway SiteWise Edge.
- O Pacote de Processamento de Dados permite que seu gateway SiteWise Edge processe os dados do seu equipamento na borda. Por exemplo, você pode usar modelos de ativo para calcular métricas e transformações. Para obter mais informações sobre modelo de ativo de hierarquia e ativos, consulte Modelagem de ativos industriais.

> **Note**
>
> - O Pacote de Processamento de Dados está disponível somente em plataformas x86.
> - O pacote de processamento de dados não oferece suporte a proxies de rede.

Para configurar os recursos de borda

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, escolha Edge gateways.
3. Selecione o gateway SiteWise Edge para o qual você deseja ativar os recursos de borda.
4. Na seção Capacidades do Edge, escolha Editar
5. Na seção Recursos do Edge, selecione Ativar pacote de processamento de dados (incorre em cobranças adicionais).
6. (Opcional) Na seção Conexão LDAP do Edge, você pode conceder aos grupos de usuários em seu diretório corporativo acesso a esse gateway do SiteWise Edge. Os grupos de usuários podem usar as credenciais do Lightweight Directory Access Protocol (LDAP) para acessar o SiteWise gateway Edge. Em seguida, eles podem usar o AWS OpsHub para AWS IoT SiteWise aplicativos, operações de AWS IoT SiteWise API ou outras ferramentas para gerenciar o gateway SiteWise Edge. Para ter mais informações, consulte Gerenciando gateways SiteWise Edge.

> **Note**
>
> Você também pode usar as credenciais do Linux ou do Windows para acessar o gateway SiteWise Edge. Para ter mais informações, consulte Acessando seu gateway SiteWise Edge usando as credenciais do sistema operacional Linux.

a. Selecione Ativado.

b. Em Nome do provedor, insira um nome para o provedor de LDAP.

c. Em Nome do host ou endereço IP, insira o nome do host ou endereço IP do seu servidor LDAP.

d. Em Porta, digite um número da porta.

e. Em Nome diferenciado base (DN), insira um nome diferenciado (DN) para a base.

   Os seguintes tipos de atributos são suportados: CommonName (CN), LocalityName (L), Name (ST), stateOrProvince OrganizationName (O), (OU), CountryName (C), StreetAddress organizationalUnitName (STREET), DomainComponent (DC) e ID do usuário (UID).

f. Em DN do grupo de administradores, insira um DN.

g. Em DN do grupo de usuários, insira um DN.

7. Escolha Salvar.

Agora que você ativou os recursos de borda em seu gateway SiteWise Edge, você precisa configurar seu modelo de ativo para o edge. Sua configuração de modelo de ativos na borda especifica onde suas propriedades dos ativos são calculadas. Você pode calcular todas as propriedades na borda ou configurar as propriedades do seu modelo de ativos separadamente. As propriedades do modelo de ativos incluem métricas, transformações e medições.

Para obter mais informações sobre as propriedades dos ativos, consulte the section called “Definir propriedades de dados”.

Depois de criar seu modelo de ativo, você pode configurá-lo para a borda. Para obter mais informações sobre a configuração do modelo de ativos para a borda, consulte the section called “Criar um modelo de ativo (console)”.

> **Note**
>
> Modelos de ativos e painéis são sincronizados automaticamente entre o Nuvem AWS e seu gateway SiteWise Edge a cada 10 minutos. Você também pode sincronizar manualmente a partir do aplicativo SiteWise Edge Gateway local.

Processamento de dados na borda

Você deve configurar seu modelo de ativo para a borda antes de poder processar os dados do gateway SiteWise Edge na borda. Sua configuração de modelo de ativos na borda especifica onde suas propriedades dos ativos são calculadas. Você pode optar por calcular todas as propriedades na borda e enviar os resultados para o Nuvem AWS, ou personalizar onde calcular cada propriedade do ativo separadamente. Para ter mais informações, consulte Habilitar o processamento de dados de borda.

As propriedades dos ativos incluem métricas, transformações e medições:

- As métricas são dados agregados de ativos ao longo de um período especificado. Você pode calcular novas métricas usando dados métricos existentes. AWS IoT SiteWise sempre envia suas métricas para a AWS nuvem para armazenamento a longo prazo. AWS IoT SiteWise computa métricas na AWS nuvem por padrão. Você pode configurar seu modelo de ativos para calcular suas métricas na borda. AWS IoT SiteWise envia os resultados processados para a AWS nuvem.
- As transformações são expressões matemáticas que mapeiam pontos de dados de um ativo de um formato para outro. As transformações podem usar métricas como dados de entrada e devem ser calculadas e armazenadas no mesmo local de suas entradas. Se você configurar uma entrada métrica para computar na borda, AWS IoT SiteWise também calculará sua transformação associada na borda.
- As medições são formatadas como dados brutos que, por padrão, seu dispositivo coleta e envia para a Nuvem AWS . Você pode configurar seu modelo de ativo para armazenar esses dados em seu dispositivo local.

Para obter mais informações sobre as propriedades dos ativos, consulte the section called “Definir propriedades de dados”.

Depois de criar seu modelo de ativo, você pode configurá-lo para a borda. Para obter mais informações sobre a configuração do modelo de ativos para a borda, consulte the section called "Criar um modelo de ativo (console)".

> **Note**
>
> Modelos de ativos e painéis são sincronizados automaticamente entre a AWS nuvem e seu gateway SiteWise Edge a cada 10 minutos. Você também pode sincronizar manualmente a partir doGerenciando gateways SiteWise Edge.

Você pode usar as APIs AWS IoT SiteWise REST e o AWS Command Line Interface (AWS CLI) para consultar seu gateway do SiteWise Edge em busca de dados na borda. Antes de consultar seu gateway SiteWise Edge em busca de dados na borda, você deve atender aos seguintes pré-requisitos:

- Suas credenciais devem ser definidas para as APIs REST. Para obter mais informações sobre como configurar credenciais, consulte the section called "Gerenciando gateways SiteWise Edge".
- O endpoint do SDK deve apontar para o endereço IP do seu gateway SiteWise Edge. Você pode encontrar mais informações na documentação do SDK. Por exemplo, consulte Especificação de endpoints personalizados no AWS SDK for Java 2.x Guia do Desenvolvedor.
- Seu certificado de gateway SiteWise Edge deve ser registrado. Você pode encontrar mais informações sobre como registrar seu certificado de gateway SiteWise Edge na documentação do seu SDK. Por exemplo, consulte Registrando pacotes de certificados em Node.js no Guia do Desenvolvedor do AWS SDK for Java 2.x .

Para obter mais informações sobre como consultar dados com AWS IoT SiteWise, consulteConsultar dados de AWS IoT SiteWise.

Configurando o componente AWS IoT SiteWise Publisher

Depois de criar um gateway AWS IoT SiteWise Edge e instalar o software, configure o componente Publisher para que seu gateway SiteWise Edge possa exportar dados para a AWS nuvem. Para obter mais informações, consulte AWS IoT SiteWise Publisher no Guia do AWS IoT Greengrass Version 2 desenvolvedor.

Console

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, escolha Edge gateways.
3. Selecione o gateway SiteWise Edge para o qual você deseja configurar o editor.
4. Na seção Configuração do editor, escolha Editar
5. Em Ordem de publicação, escolha uma das seguintes opções:
   - Publique primeiro os dados mais antigos — Por padrão, o gateway SiteWise Edge publica primeiro os dados mais antigos na nuvem.
   - Publique primeiro os dados mais recentes — O gateway SiteWise Edge publica primeiro os dados mais recentes na nuvem.
6. (Opcional) Se você não quiser que o SiteWise Edge Gateway comprima seus dados, desmarque Ativar compactação ao fazer upload de dados.
7. (Opcional) Se você não quiser publicar dados antigos, escolha Excluir dados expirados e faça o seguinte:
   - Em Período limite, insira um valor e escolha uma unidade. O período limite deve ser entre cinco minutos e sete dias. Por exemplo, se o período limite for de três dias, os dados com mais de três dias não serão publicados na nuvem.
8. (Opcional) Para definir configurações personalizadas sobre como os dados são tratados em seu dispositivo local, escolha Configurações de armazenamento local e faça o seguinte:
   a. Em Período de retenção, insira um número e escolha uma unidade. O período de retenção deve ser entre um minuto e 30 dias e maior ou igual ao período de alternância. Por exemplo, se o período de retenção for de 14 dias, o gateway SiteWise Edge excluirá todos os dados na borda que sejam mais antigos do que o período limite especificado após serem armazenados por 14 dias.
   b. Em Período de alternância, insira um número e escolha uma unidade. O período de rotação deve ser maior que um minuto e igual ou menor que o período de retenção. Por exemplo, digamos que o período de rotação seja de dois dias, o gateway SiteWise Edge agrupa e salva dados anteriores ao período limite em um único arquivo. O gateway SiteWise Edge transfere um lote de dados para o seguinte diretório local uma vez a cada dois dias:`/greengrass/v2/work/aws.iot.SiteWiseEdgePublisher/exports`.

c. Em Capacidade de armazenamento, insira um valor maior ou igual a 1. Se a capacidade de armazenamento for de 2 GB, o gateway SiteWise Edge começará a excluir dados quando mais de 2 GB de dados forem armazenados localmente.

9. Escolha Salvar.

AWS CLI

Você pode usar a UpdateGatewayCapabilityConfigurationAPI para configurar o editor. Defina o parâmetro `capabilityNamespace` como `iotsitewise:publisher:2`.

O editor fornece os seguintes parâmetros de configuração que você pode personalizar:

`SiteWisePublisherConfiguration`

`publishingOrder`

A ordem na qual os dados são publicados na nuvem. O valor desse parâmetro pode ser um dos seguintes:

- `TIME_ORDER` (Publicar primeiro os dados mais antigos) — Por padrão, o gateway publica primeiro os dados mais antigos na nuvem.
- `RECENT_DATA` (Publicar primeiro os dados mais recentes) — O gateway publica primeiro os dados mais recentes na nuvem.

`dropPolicy`

(Opcional) Uma política que controla quais dados são publicados na nuvem.

`cutoffAge`

Os dados anteriores ao período limite não são publicados na nuvem. A idade limite deve ser entre cinco minutos e sete dias.

Você pode usar `m`, h e d ao especificar uma idade limite. Observe que `m` representa minutos, h representa horas e d representa dias.

`exportPolicy`

(Opcional) Uma política que gerencia o armazenamento de dados na borda. Esta política se aplica a dados anteriores à idade limite.

`retentionPeriod`

Seu gateway SiteWise Edge exclui todos os dados na borda anteriores ao período limite do armazenamento local após serem armazenados pelo período de retenção especificado. O período de retenção deve ser entre um minuto e 30 dias e maior ou igual ao período de alternância.

Você pode usar `m`, h e d ao especificar um período de retenção. Observe que `m` representa minutos, h representa horas e d representa dias.

`rotationPeriod`

O intervalo de tempo para agrupar e salvar dados anteriores ao período limite em um único arquivo. O gateway SiteWise Edge transfere um lote de dados para o seguinte diretório local no final de cada período de rotação:`/greengrass/v2/work/aws.iot.SiteWiseEdgePublisher/exports`. O período de alternância deve ser maior que um minuto e menor ou igual ao período de retenção.

Você pode usar `m`, h e d ao especificar um período de alternância. Observe que `m` representa minutos, h representa horas e d representa dias.

`exportSizeLimitGB`

O tamanho máximo permitido de dados armazenados localmente, em GB. Se essa cota for violada, o SiteWise Edge Gateway começará a excluir os dados mais antigos até que o tamanho dos dados armazenados localmente seja igual ou menor que a cota. O valor desse parâmetro deve ser maior ou igual a 1.

Example configuração do editor:

O namespace do editor: `iotsitewise:publisher:2`

```
{
"SiteWisePublisherConfiguration": {
    "publishingOrder": "TIME_ORDER",
    "dropPolicy": {
        "cutoffAge": "7d",
        "exportPolicy": {
            "retentionPeriod": "7d",
            "rotationPeriod": "6h",
            "exportLocation": "/greengrass/v2/work/aws.iot.SiteWiseEdgePublisher/
exports",
```

```
            "exportSizeLimitGB": 10
        }
    }
}
}
```

Configurar fontes de dados

Depois de configurar um gateway AWS IoT SiteWise Edge, você pode configurar fontes de dados para que seu gateway SiteWise Edge possa ingerir dados de equipamentos industriais locais para AWS IoT SiteWise. Cada fonte representa um servidor local, como um servidor OPC-UA, que seu gateway SiteWise Edge conecta e recupera fluxos de dados industriais. Para obter mais informações sobre como configurar um gateway SiteWise Edge, consulteConfigurando um gateway AWS IoT Greengrass V1 SiteWise Edge.

> **Note**
>
> AWS IoT SiteWise reinicia seu gateway SiteWise Edge sempre que você adiciona ou edita uma fonte. Seu gateway SiteWise Edge não ingere dados durante a reinicialização. O tempo para reiniciar o gateway SiteWise Edge depende do número de tags nas fontes do gateway SiteWise Edge. O tempo de reinicialização pode variar de alguns segundos (para um gateway SiteWise Edge com poucas tags) a vários minutos (para um gateway SiteWise Edge com muitas tags).

Depois de criar origens, você pode associar os fluxos de dados às propriedades do ativo. Para obter mais informações sobre como criar e usar ativos, consulte Modelagem de ativos industriais e Mapeamento de fluxos de dados industriais para propriedades de ativos.

Você pode visualizar CloudWatch métricas para verificar se uma fonte de dados está conectada AWS IoT SiteWise a. Para ter mais informações, consulte AWS IoT Greengrass Version 2 métricas de gateway.

Atualmente, AWS IoT SiteWise oferece suporte aos seguintes protocolos de fonte de dados:

- OPC-UA — Um protocolo de comunicação machine-to-machine (M2M) para automação industrial.

> **Note**
>
> SiteWise Os gateways Edge em execução AWS IoT Greengrass V2 atualmente não suportam fontes Modbus TCP e Ethernet IP.

Tópicos

Configurar uma origem OPC-UA

Você pode usar o AWS IoT SiteWise console ou um recurso de gateway SiteWise Edge para definir e adicionar uma fonte OPC-UA ao seu gateway SiteWise Edge para representar um servidor OPC-UA local.

Tópicos

Configurar uma origem OPC-UA (console)

Para configurar uma fonte OPC-UA usando o console AWS IoT SiteWise

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Gateways da .
3. Selecione o gateway SiteWise Edge para adicionar uma fonte OPC-UA.
4. Escolha Adicionar fonte de dados.
5. Insira um nome para a origem.

6. Insira o Local endpoint (Endpoint local) do servidor da fonte de dados. O endpoint pode ser o endereço IP ou o nome do host. Você também pode adicionar um número de porta ao endpoint local. Por exemplo, seu endpoint local pode ter a seguinte aparência: **`opc.tcp://203.0.113.0:49320`**

   > **Note**
   >
   > Se o seu gateway SiteWise Edge tiver um `Deployment type` dispositivo Siemens Industrial Edge - novo e você quiser ingerir dados do aplicativo Edge OPC UA Server executado no mesmo dispositivo Siemens Industrial Edge do aplicativo Edge, insira AWS IoT SiteWise . **`opc.tcp://ie-opcua:48010`**

7. (Opcional) Para seleção de ID de nó, adicione filtros de nó para limitar quais fluxos de dados são ingeridos no. Nuvem AWS Por padrão, os gateways do SiteWise Edge usam o nó raiz de um servidor para ingerir todos os fluxos de dados. Você pode usar filtros de nós para reduzir o tempo de inicialização e o uso da CPU do gateway SiteWise Edge, incluindo apenas caminhos para os dados nos quais você modela AWS IoT SiteWise. Por padrão, os gateways do SiteWise Edge carregam todos os caminhos OPC-UA, exceto aqueles que começam com. `/Server/` Para definir os filtros de nó do OPC-UA, é possível usar caminhos de nó e os caracteres curinga `*` e `**`. Para ter mais informações, consulte Usando filtros de nó OPC-UA.

8. Em Destinos, escolha o destino dos dados de origem:

   - AWS IoT SiteWise em tempo real — escolha essa opção para enviar dados diretamente para o AWS IoT SiteWise armazenamento. Ingira e monitore dados em tempo real e processe dados na borda.
   - AWS IoT SiteWise Armazenado em buffer usando o Amazon S3 — Envie dados em formato parquet para o Amazon S3 e depois importe para o armazenamento. AWS IoT SiteWise Escolha essa opção para ingerir dados em lotes e armazenar dados históricos de forma econômica. Você pode configurar sua localização preferida de bucket do Amazon S3 e a frequência com que deseja que os dados sejam carregados para o Amazon S3. Você também pode escolher o que fazer com os dados após a ingestão no AWS IoT SiteWise. Você pode optar por ter os dados disponíveis no Amazon S3 SiteWise e no Amazon S3 ou pode optar por excluí-los automaticamente do Amazon S3.
     - O bucket do Amazon S3 é um mecanismo de armazenamento e armazenamento em buffer e oferece suporte a arquivos no formato parquet.

- Se você marcar a caixa de seleção Importar dados para o AWS IoT SiteWise armazenamento, os dados serão carregados primeiro no Amazon S3 e depois no AWS IoT SiteWise armazenamento.
  - Se você marcar a caixa de seleção Excluir dados do Amazon S3, os dados serão excluídos do Amazon S3 após serem importados para o armazenamento. SiteWise
  - Se você desmarcar a caixa de seleção Excluir dados do Amazon S3, os dados serão armazenados no Amazon S3 e no armazenamento. SiteWise
- Se você desmarcar a caixa de seleção Importar dados para AWS IoT SiteWise armazenamento, os dados serão armazenados somente no Amazon S3. Não é importado para o SiteWise armazenamento.

Visite Gerenciando o armazenamento de dados para obter detalhes sobre as várias opções de armazenamento AWS IoT SiteWise oferecidas. Para saber mais sobre as opções de preços, consulte AWS IoT SiteWise preços.

- AWS IoT Greengrass gerenciador de streams — Use AWS IoT Greengrass o gerenciador de streams para enviar dados para os seguintes Nuvem AWS destinos: canais em AWS IoT Analytics, streams no Amazon Kinesis Data Streams, propriedades de ativos ou objetos AWS IoT SiteWise no Amazon Simple Storage Service (Amazon S3). Para obter mais informações, consulte Gerenciar fluxos de dados no AWS IoT Greengrass Core no Guia do AWS IoT Greengrass Version 2 desenvolvedor.

  Insira um nome para o AWS IoT Greengrass stream.

Ao configurar uma fonte de dados, o Node ID para seleção é usado para determinar o destino do fluxo de dados.

- Se os mesmos dados forem publicados AWS IoT SiteWise em tempo real e AWS IoT SiteWise armazenados em buffer usando o Amazon S3, você deverá adicionar duas fontes de dados que publiquem nos dois destinos.
- Para dividir os dados de forma que uma parte deles seja publicada AWS IoT SiteWise em tempo real e a outra parte no AWS IoT SiteWise Buffered usando o Amazon S3, você deve filtrar os seguintes aliases de dados:

```
/Alias01/Data1
/Alias02/Data1
/Alias03/Data1
```

```
/Alias03/Data2
```

Por exemplo, você pode adicionar uma fonte de dados apontando para o filtro do `/**/Data1` nó, para o AWS IoT SiteWise tempo real, e outra fonte de dados apontando para o `/**/Data2` AWS IoT SiteWise buffer usando o Amazon S3

9. No painel Configuração avançada, você pode fazer o seguinte:

   a. Escolha um modo de segurança de mensagem para conexões e dados em trânsito entre seu servidor de origem e seu gateway SiteWise Edge. Esse campo é a combinação da política de segurança de OPC-UA e do modo de segurança de mensagens. Escolha a mesma política de segurança e modo de segurança de mensagens que você especificou para seu servidor OPC-UA.

   b. Se sua fonte exigir autenticação, escolha um AWS Secrets Manager segredo na lista de configuração de autenticação. O gateway SiteWise Edge usa as credenciais de autenticação nesse segredo quando se conecta a essa fonte de dados. Você deve anexar segredos ao AWS IoT Greengrass componente do seu gateway SiteWise Edge para usá-los na autenticação da fonte de dados. Para ter mais informações, consulte the section called “Configurar a autenticação da fonte de dados”.

      > **Tip**
      >
      > Seu servidor de dados pode ter uma opção chamada Allow anonymous login (Permitir login anônimo). Se essa opção for Yes (Sim), a origem não exigirá autenticação.

   c. (Opcional) Insira um prefixo de fluxo de dados. O gateway SiteWise Edge adiciona esse prefixo a todos os fluxos de dados dessa fonte. Use um prefixo de stream de dados para distinguir entre streams de dados que têm o mesmo nome de origens diferentes. Cada stream de dados deve ter um nome exclusivo na conta.

   d. (Opcional) Para grupos de propriedades, escolha Adicionar novo grupo.

      i. Insira um Nome para o grupo de propriedades.

      ii. Para Propriedades:

         1. Para caminhos de nó, adicione filtros de nó OPC-UA para limitar quais caminhos OPC-UA são carregados. AWS IoT SiteWise O formato é semelhante ao Node ID para seleção.

iii. Em Configurações de grupo, faça o seguinte:

1. Em Configuração de qualidade de dados, escolha o tipo de qualidade de dados que você deseja que o AWS IoT SiteWise Collector ingira.
2. Para a configuração do modo de digitalização, configure as seguintes propriedades de assinatura padrão:
   - Para Modo de digitalização, escolha uma das seguintes opções: Para obter mais informações sobre o modo de digitalização, consultethe section called “Filtrar intervalos de ingestão de dados com OPC-UA”.
     - Para enviar todos os pontos de dados, escolha Inscrever-se e defina o seguinte:
       - Acionador de alteração de dados — A condição que inicia um alerta de alteração de dados.
       - Tamanho da fila de assinatura — A profundidade da fila em um servidor OPC—UA para uma métrica específica em que as notificações de itens monitorados são enfileiradas.
       - Intervalo de publicação da assinatura — O intervalo (em milissegundos) do ciclo de publicação especificado quando a assinatura é criada.
       - Intervalo do instantâneo — A configuração do tempo limite da frequência do instantâneo para garantir que o AWS IoT SiteWise Edge ingira um fluxo constante de dados.
       - Taxa de digitalização — A taxa em que você deseja que o gateway SiteWise Edge leia seus registros. AWS IoT SiteWise calcula automaticamente a taxa de varredura mínima permitida para seu gateway SiteWise Edge.
     - Para enviar pontos de dados em um intervalo específico, escolha Enquete e insira uma taxa de varredura.
3. Se você escolher o modo de digitalização de Assinatura, defina um tipo de banda morta e as configurações relacionadas para sua fonte. Isso controla quais dados sua fonte envia para você AWS IoT SiteWise e quais dados ela descarta. Para obter mais informações sobre as configurações de deadband, consulte the section called “Filtrar intervalos de ingestão de dados com OPC-UA”.

10. Selecione Save (Salvar).

Configurar uma origem OPC-UA (CLI)

Você pode definir fontes de dados OPC-UA para um gateway SiteWise Edge usando o. AWS CLI Para fazer isso, crie um arquivo JSON de configuração de capacidade OPC-UA e use o update-gateway-capability-configurationcomando para atualizar a configuração do gateway SiteWise Edge. Você deve definir todas as origens OPC-UA em uma única configuração de recursos.

Esse recurso tem o seguinte namespace.

- `iotsitewise:opcuacollector:2`

Sintaxe da solicitação

```
{
  "sources": [
    {
      "name": "string",
      "endpoint": {
        "certificateTrust": {
          "type": "TrustAny" | "X509",
          "certificateBody": "string",
          "certificateChain": "string",
        },
        "endpointUri": "string",
        "securityPolicy": "NONE" | "BASIC128_RSA15" | "BASIC256" | "BASIC256_SHA256" |
 "AES128_SHA256_RSAOAEP" | "AES256_SHA256_RSAPSS",
        "messageSecurityMode": "NONE" | "SIGN" | "SIGN_AND_ENCRYPT",
        "identityProvider": {
          "type": "Anonymous" | "Username",
          "usernameSecretArn": "string"
        },
        "nodeFilterRules": [
          {
            "action": "INCLUDE",
            "definition": {
              "type": "OpcUaRootPath",
              "rootPath": "string"
            }
          }
        ]
      },
      "measurementDataStreamPrefix": "string"
```

```
      "destination": {
         "type": "StreamManager",
         "streamName": "string",
         "streamBufferSize": integer
       },
       "propertyGroups": [
         {
           "name": "string",
           "nodeFilterRuleDefinitions": [
             {
               "type": "OpcUaRootPath",
               "rootPath": "string"
             }
           ],
           "deadband": {
             "type": "PERCENT" | "ABSOLUTE",
             "value": double,
             "eguMin": double,
             "eguMax": double,
             "timeoutMilliseconds": integer
           },
           "scanMode": {
             "type": "EXCEPTION" | "POLL",
             "rate": integer
           },
           "dataQuality": {
             "allowGoodQuality": true | false,
             "allowBadQuality": true | false,
             "allowUncertainQuality": true | false
           },
           "subscription": {
             "dataChangeTrigger": "STATUS" | "STATUS_VALUE" | "STATUS_VALUE_TIMESTAMP",
             "queueSize": integer,
             "publishingIntervalMilliseconds": integer,
             "snapshotFrequencyMilliseconds": integer
           }
         }
       ]
     }
   ]
}
```

Corpo da solicitação

fontes

Uma lista de estruturas de definição de fonte OPC-UA que contêm as seguintes informações:

name

Um nome exclusivo e amigável para a origem.

endpoint

Uma estrutura de endpoint que contém as seguintes informações:

Certificado de confiança

Uma estrutura de política de confiança de certificado que contém as seguintes informações:

tipo

O modo de confiança do certificado para a origem. Escolha uma das seguintes opções:

- **`TrustAny`**— O gateway SiteWise Edge confia em qualquer certificado quando se conecta à fonte OPC-UA.
- `X509`— O gateway SiteWise Edge confia em um certificado X.509 quando se conecta à fonte OPC-UA. Se você escolher essa opção, deverá definir `certificateBody` em `certificateTrust`. Também é possível definir `certificateChain` em `certificateTrust`.

Organismo certificado

(Opcional) O corpo de um certificado X.509.

Esse campo será obrigatório se você escolher `X509` para `type` em `certificateTrust`.

Cadeia de Certificados

(Opcional) A cadeia de confiança para um certificado X.509.

Esse campo é usado somente se você escolher `X509` para `type` em `certificateTrust`.

URI do ponto final

O endpoint local da fonte OPC-UA. Por exemplo, seu endpoint local pode ser semelhante a `opc.tcp://203.0.113.0:49320`.

Política de segurança

A política de segurança a ser usado para que você possa proteger mensagens que são lidas na origem OPC-UA. Escolha uma das seguintes opções:

- `NONE`— O gateway SiteWise Edge não protege as mensagens da fonte OPC-UA. Recomendamos que você escolha uma política de segurança diferente. Se você escolher essa opção, também deverá escolher `NONE` para `messageSecurityMode`.
- `BASIC256_SHA256` – A política de segurança de `Basic256Sha256`.
- `AES128_SHA256_RSAOAEP` – A política de segurança de `Aes128_Sha256_RsaOaep`.
- `AES256_SHA256_RSAPSS` – A política de segurança de `Aes256_Sha256_RsaPss`.
- `BASIC128_RSA15` – (Obsoleto) A política de segurança `Basic128Rsa15` está obsoleta na especificação de OPC-UA porque não é mais considerada segura. Recomendamos que você escolha uma política de segurança diferente. Para obter mais informações, consulte Basic128Rsa15.
- `BASIC256` – (Obsoleto) A política de segurança `Basic256` está obsoleta na especificação de OPC-UA porque não é mais considerada segura. Recomendamos que você escolha uma política de segurança diferente. Para obter mais informações, consulte Basic256.

> **Important**
>
> Se você escolher uma política de segurança diferente de `NONE`, deverá escolher `SIGN` ou `SIGN_AND_ENCRYPT` para `messageSecurityMode`. Você também deve configurar seu servidor de origem para confiar no gateway SiteWise Edge. Para ter mais informações, consulte Permitindo que seus servidores de origem OPC-UA confiem no SiteWise gateway Edge.

mensagem SecurityMode

O modo de segurança de mensagens a ser usado para proteger conexões com a fonte OPC-UA. Escolha uma das seguintes opções:

- `NONE`— O gateway SiteWise Edge não protege as conexões com a fonte OPC-UA. Recomendamos que você escolha um modo de segurança de mensagem diferente. Se você escolher essa opção, também deverá escolher `NONE` para `securityPolicy`.

- `SIGN`— Os dados em trânsito entre o gateway SiteWise Edge e a fonte OPC-UA são assinados, mas não criptografados.
- `SIGN_AND_ENCRYPT` – Os dados em trânsito entre o gateway e a origem OPC-UA são assinados e criptografados.

> **Important**
>
> Se você escolher um modo de segurança de mensagem diferente de`NONE`, deverá escolher `securityPolicy` outro que `NONE`. Você também deve configurar seu servidor de origem para confiar no gateway SiteWise Edge. Para ter mais informações, consulte Permitindo que seus servidores de origem OPC-UA confiem no SiteWise gateway Edge.

Provedor de identidade

Uma estrutura de provedor de identidade que contém as seguintes informações:

tipo

O tipo de credenciais de autenticação exigidas pela origem. Escolha uma das seguintes opções:

- `Anonymous` – A origem não requer autenticação para conectar-se.
- `Username` – A origem requer um nome de usuário e senha para conectar-se. Se você escolher essa opção, deverá definir `usernameSecretArn` em `identityProvider`.

nome de usuário SecretArn

(Opcional) O ARN de um AWS Secrets Manager segredo. O gateway SiteWise Edge usa as credenciais de autenticação nesse segredo quando se conecta a essa fonte. Você deve anexar segredos ao SiteWise conector IoT do seu gateway SiteWise Edge para usá-los na autenticação de origem. Para ter mais informações, consulte Configurar a autenticação da fonte de dados.

Esse campo será obrigatório se você escolher `Username` para `type` em `identityProvider`.

nodo FilterRules

Uma lista de estruturas de regras de filtro de nós que definem os caminhos do fluxo de dados OPC-UA a serem enviados para a AWS nuvem. Você pode usar filtros de nós para reduzir o tempo de inicialização e o uso da CPU do gateway SiteWise Edge, incluindo apenas caminhos para os dados nos quais você modela AWS IoT SiteWise. Por padrão, os gateways do SiteWise Edge carregam todos os caminhos OPC-UA, exceto aqueles que começam com. `/Server/` Para definir os filtros de nó do OPC-UA, é possível usar caminhos de nó e os caracteres curinga `*` e `**`. Para ter mais informações, consulte Usando filtros de nó OPC-UA.

Cada estrutura na lista deve conter as seguintes informações:

ação

A ação para essa regra de filtro de nó. Você pode escolher a seguinte opção:

- `INCLUDE`— O gateway SiteWise Edge inclui somente fluxos de dados que correspondem a essa regra.

definição

Uma estrutura de regra de filtro de nó que contém as seguintes informações:

tipo

O tipo de caminho do filtro de nó para essa regra. Você pode escolher a seguinte opção:

- `OpcUaRootPath`— O gateway SiteWise Edge avalia esse caminho de filtro de nó em relação à raiz da hierarquia de caminhos OPC-UA.

Caminho raiz

O caminho do filtro de nó a ser avaliado em relação à raiz da hierarquia de caminhos OPC-UA. Esse caminho deve começar com `/`.

DataStreamPrefixo de medição

Uma string que deve preceder todos os fluxos de dados da origem. O gateway SiteWise Edge adiciona esse prefixo a todos os fluxos de dados dessa fonte. Use um prefixo de stream de dados para distinguir entre streams de dados que têm o mesmo nome de origens diferentes. Cada stream de dados deve ter um nome exclusivo na conta.

Grupos de propriedades

(Opcional) A lista de grupos de propriedades que definem `deadband` e `scanMode` são solicitados pelo protocolo.

name

O nome do grupo de propriedade. Esse deve ser um identificador exclusivo.

faixa morta

A estrutura de `deadband` contém as seguintes informações:

tipo

Os tipos de deadband compatíveis. Os valores aceitos são `ABSOLUTE` e `PERCENT`.

value

O valor da deadband. Quando `type` é `ABSOLUTE`, esse valor é um duplo sem unidade. Quando `type` é `PERCENT`, esse valor é o dobro entre `1` e `100`.

Geumin

(Opcional) O mínimo da unidade de engenharia ao usar uma deadband de `PERCENT`. Você define isso se o servidor OPC-UA não tiver unidades de engenharia configuradas.

Egumax

(Opcional) O máximo da unidade de engenharia ao usar uma deadband de `PERCENT`. Você define isso se o servidor OPC-UA não tiver unidades de engenharia configuradas.

Tempo limite em milissegundos

A duração em milissegundos antes do tempo limite. O mínimo é `100`.

Modo de digitalização

A estrutura de `scanMode` contém as seguintes informações:

tipo

Os tipos compatíveis de `scanMode`. Os valores aceitos são `POLL` e `EXCEPTION`.

taxa

O intervalo de amostragem para o modo de verificação.

FilterRuleDefinições de nós

(Opcional) Uma lista de caminhos de nós a serem incluídos no grupo de propriedades. Os grupos de propriedades não podem se sobrepor. Se você não especificar um valor para esse campo, o grupo conterá todos os caminhos abaixo da raiz e você não poderá criar grupos de propriedades adicionais. A estrutura `nodeFilterRuleDefinitions` contém as seguintes informações:

tipo

`OpcUaRootPath` é o único tipo compatível. Isso especifica que o valor de `rootPath` é um caminho relativo à raiz do espaço de navegação de OPC-UA.

Caminho raiz

Uma lista delimitada por vírgulas que especifica os caminhos (em relação à raiz) a serem incluídos no grupo de propriedades.

Exemplos de configuração de recurso

O exemplo a seguir define uma configuração de capacidade de gateway OPC-UA SiteWise Edge a partir de uma carga armazenada em um arquivo JSON.

```
aws iotsitewise update-gateway-capability-configuration \
--capability-namespace "iotsitewise:opcuacollector:2" \
--capability-configuration file://opc-ua-configuration.json
```

Example : configuração da origem OPC-UA

O seguinte arquivo de `opc-ua-configuration.json` define uma configuração de origem 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 : configuração da origem OPC-UA com grupos de propriedades definidos

O seguinte arquivo de `opc-ua-configuration.json` define uma configuração de origem OPC-UA básica e insegura com grupos de propriedades 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 : configuração da origem OPC-UA com propriedades

O seguinte exemplo JSON para `opc-ua-configuration.json` define uma configuração de fonte OPC-UA com as seguintes propriedades:

- Confia em qualquer certificado.
- Usa a política de segurança de `BASIC256` para proteger as mensagens.
- Usa o modo `SIGN_AND_ENCRYPT` para proteger conexões.
- Usa credenciais de autenticação armazenadas em um segredo do Secrets Manager.
- Filtra stream de dados, com exceção daqueles cujo caminho começa com `/WindFarm/2/WindTurbine/`.
- Adiciona `/Washington` ao início de cada caminho de stream de dados para distinguir entre este “Parque eólico nº 2" e um “Parque eólico nº 2" em outra 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 : Configuração da fonte OPC-UA com certificado confiável

O seguinte exemplo JSON para `opc-ua-configuration.json` define uma configuração de fonte OPC-UA com as seguintes propriedades:

- Confia em um determinado certificado X.509.
- Usa a política de segurança de `BASIC256` para proteger as mensagens.
- Usa o modo `SIGN_AND_ENCRYPT` para proteger conexões.

```
{
    "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": ""

       }
    ]
}
```

Permitindo que seus servidores de origem OPC-UA confiem no SiteWise gateway Edge

Se você escolher uma opção `messageSecurityMode` diferente de Nenhuma ao configurar sua fonte OPC-UA, deverá permitir que seus servidores de origem confiem no AWS IoT SiteWise gateway Edge. O gateway SiteWise Edge gera um certificado que seu servidor de origem pode

exigir. O processo varia de acordo com seus servidores de origem. Para obter mais informações, consulte a documentação dos seus servidores.

O procedimento a seguir descreve as etapas básicas.

Para permitir que um servidor OPC-UA confie no SiteWise gateway Edge

1. Abra a interface para configurar seu servidor OPC-UA.
2. Insira o nome de usuário e a senha do administrador do servidor OPC-UA.
3. Localize Clientes confiáveis na interface e escolha AWS IoT SiteWise Cliente do gateway.
4. Escolha Trust (Confiar).

Exportar o certificado de cliente OPC-UA

Alguns servidores OPC-UA exigem acesso ao arquivo de certificado do cliente OPC-UA para confiar no gateway Edge. SiteWise Se isso se aplica aos seus servidores OPC-UA, você pode usar o procedimento a seguir para exportar o certificado do cliente OPC-UA do gateway Edge. SiteWise Depois, você pode importar o certificado no servidor OPC-UA.

Como exportar o arquivo de certificado de cliente OPC-UA para uma origem

1. Execute o comando a seguir a fim de mudar para o diretório que contém o arquivo de certificado. *Substitua o sitewise-work pelo caminho de armazenamento local para o aws.iot. SiteWiseEdgeCollectorOpcua Greengrass*, pasta de trabalho e substitua *source-name pelo nome* da fonte de dados.

   Por padrão, a pasta de trabalho do Greengrass é /greengrass/v2/work/aws.iot. SiteWiseEdgeCollectorOpcua em Linux e *C: /greengrass/v2/work/aws.iot. SiteWiseEdgeCollectorOpcua no Windows*.

   ```
   cd /sitewise-work/source-name/opcua-certificate-store
   ```

2. O certificado de cliente OPC-UA do gateway SiteWise Edge para essa fonte está no `aws-iot-opcua-client.pfx` arquivo.

   Execute o comando a seguir a fim de exportar o certificado para um arquivo `.pem` denominado `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. Transfira o arquivo do certificado,`aws-iot-opcua-client-certificate.pem`, do gateway SiteWise Edge para o servidor OPC-UA.

   Para fazer isso, é possível usar software comum, como o programa `scp`, para transferir o arquivo usando o protocolo SSH. Para obter mais informações, consulte Secure copy na Wikipédia.

   > **Note**
   >
   > Se o seu gateway SiteWise Edge estiver em execução no Amazon Elastic Compute Cloud (Amazon EC2) e você estiver se conectando a ele pela primeira vez, deverá configurar os pré-requisitos para se conectar. Para obter mais informações, consulte Connect to your Linux instance no Amazon EC2 User Guide.

4. Importe o arquivo de certificado`aws-iot-opcua-client-certificate.pem`,, no servidor OPC-UA para confiar no gateway SiteWise Edge. As etapas podem variar de acordo com o servidor de origem utilizado. Consulte a documentação do servidor.

Filtrar intervalos de ingestão de dados com OPC-UA

Você pode controlar a forma como os dados são ingeridos com uma origem OPC-UA usando o modo de verificação e os intervalos de deadband. Esses recursos permitem que você controle o tipo de dados a ser ingerido e como e quando o servidor e o gateway SiteWise Edge trocam essas informações.

Colete ou filtre dados com base na qualidade

Você pode definir suas configurações de qualidade de dados para controlar quais dados são coletados da fonte OPC-UA. A fonte de dados inclui a classificação de qualidade como metadados ao enviá-la. Você pode selecionar uma ou todas as seguintes opções:

- `Good`
- `Bad`
- `Uncertain`

Controle a frequência de coleta de dados com o modo de verificação

Você pode configurar seu modo de verificação OPC-UA para controlar a forma como você coleta dados da sua origem OPC-UA. Você pode escolher o modo de assinatura ou sondagem.

- Modo de assinatura — A fonte OPC-UA coleta dados para enviar ao seu gateway SiteWise Edge na frequência definida pela sua taxa de varredura. O servidor só envia dados quando o valor é alterado, então essa é a frequência máxima que seu gateway SiteWise Edge recebe dados.
- Modo de pesquisa — Seu gateway SiteWise Edge pesquisa a fonte OPC-UA em uma frequência definida pela sua taxa de varredura. O servidor envia dados independentemente de o valor ter sido alterado, então seu gateway SiteWise Edge sempre recebe dados nesse intervalo.

> **Note**
>
> A opção do modo de sondagem substitui suas configurações de deadband para essa origem.

Filtrar ingestão de dados com OPC-UA com intervalos de deadband

Você pode aplicar uma banda morta aos seus grupos de propriedades de origem do OPC-UA para filtrar e descartar determinados dados em vez de enviá-los para a nuvem. AWS Uma deadband especifica uma janela de flutuações esperadas nos valores de dados recebidos de sua origem OPC-UA. Se os valores estiverem dentro dessa janela, seu servidor OPC-UA não os enviará para a AWS nuvem. Você pode usar a filtragem de banda morta para reduzir a quantidade de dados que você está processando e enviando para a AWS nuvem. Para saber como configurar fontes OPC-UA para seu gateway SiteWise Edge, consulte. the section called “Configurar fontes de dados”

> **Note**
>
> O servidor exclui todos os dados que estão dentro da janela especificada pela deadband. Não é possível recuperar esses dados descartados.

Tipos de deadband

Você pode especificar dois tipos de deadband para o grupo de propriedades do servidor OPC-UA. Eles permitem que você escolha quantos dados são enviados para a AWS nuvem e quantos são descartados.

- Porcentagem — Você especifica uma janela usando uma porcentagem da flutuação esperada no valor da medição. O servidor calcula a janela exata a partir dessa porcentagem e envia dados para a AWS nuvem que excedem as quedas fora da janela. Por exemplo, especificar um valor de banda morta de 2% em um sensor com uma faixa de -100 graus Fahrenheit a +100 graus Fahrenheit faz com que o servidor envie dados para a nuvem quando o valor mudar em 4 graus Fahrenheit ou mais. AWS

  > **Note**
  >
  > Opcionalmente, você pode especificar um valor mínimo e máximo de deadband para essa janela se o servidor de origem não definir unidades de engenharia. Se um intervalo de unidades de engenharia não for fornecido, o servidor OPC-UA assume como padrão o intervalo total do tipo de dados de medição.

- Absoluto — Você especifica uma janela usando unidades exatas. Por exemplo, especificar um valor de deadband de 2 em um sensor faz com que o servidor envie dados para a Nuvem AWS quando seu valor mudar em pelo menos 2 unidades. Você pode usar a deadband absoluta para ambientes dinâmicos em que flutuações são esperadas regularmente durante as operações normais.

Tempo limite de deadband

Opcionalmente, você pode definir uma configuração de tempo limite de deadband. Após esse tempo limite, o servidor OPC-UA envia o valor da medição atual, mesmo que esteja dentro da flutuação esperada da deadband. Você pode usar a configuração de tempo limite para garantir que AWS IoT SiteWise esteja ingerindo um fluxo constante de dados o tempo todo, mesmo quando os valores não excederem a janela de banda morta definida.

Usando filtros de nó OPC-UA

Ao definir fontes de dados OPC-UA para um gateway SiteWise Edge, você pode definir filtros de nós. Os filtros de nós permitem limitar quais caminhos de fluxo de dados o gateway SiteWise Edge envia para a nuvem. Você pode usar filtros de nós para reduzir o tempo de inicialização e o uso da CPU do gateway SiteWise Edge, incluindo apenas caminhos para os dados nos quais você modela AWS IoT SiteWise. Por padrão, os gateways do SiteWise Edge carregam todos os caminhos OPC-UA, exceto aqueles que começam com. `/Server/` Você pode usar os caracteres curingas * e ** nos filtros de nó para incluir vários caminhos de fluxo de dados com um filtro. Para saber como configurar fontes OPC-UA para seu gateway SiteWise Edge, consulte. Configurar fontes de dados

> **Note**
>
> AWS IoT SiteWise reinicia seu gateway SiteWise Edge sempre que você adiciona ou edita uma fonte. Seu gateway SiteWise Edge não ingere dados durante a reinicialização. O tempo para reiniciar o gateway SiteWise Edge depende do número de tags nas fontes do gateway SiteWise Edge. O tempo de reinicialização pode variar de alguns segundos (para um gateway SiteWise Edge com poucas tags) a vários minutos (para um gateway SiteWise Edge com muitas tags).

A tabela a seguir lista os curingas que você pode usar para filtrar fontes de dados OPC-UA.

Curingas de filtro de nó OPC-UA

Curinga	Descrição
*	Corresponde a um único nível em um caminho de fluxo de dados.
**	Corresponde a vários níveis em um caminho de fluxo de dados.

> **Note**
>
> Se você configurar uma fonte com um filtro amplo e depois alterar a fonte para usar um filtro mais restritivo, AWS IoT SiteWise interrompe o armazenamento de dados que não correspondam ao novo filtro.

Example Exemplo de cenário usando filtros de nó

Considere os seguintes fluxos de dados 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`

Usando os fluxos de dados anteriores, é possível definir filtros de nó para limitar os dados a serem incluídos da fonte OPC-UA.

- Para selecionar todos os nós neste exemplo, use `/` ou `/**/`. É possível incluir vários diretórios ou pastas com caracteres curinga `**`.
- Para selecionar todos os fluxos de dados `PLC`, use `/*/*/*/PLC*` ou `/**/PLC*`.
- Para selecionar todos os contadores neste exemplo, use `/**/Counter*` ou `/*/*/*/Counter*`.
- Para selecionar todos os contadores da `Line 2`, use `/**/Line 2/Counter*`.

Configurar a autenticação da fonte de dados

Se seu servidor OPC-UA exigir credenciais de autenticação para se conectar, você pode usar AWS Secrets Manager para criar e implantar um segredo no seu SiteWise gateway Edge. AWS Secrets Manager criptografa segredos no dispositivo para manter seu nome de usuário e senha seguros até que você precise usá-los. Para obter mais informações sobre o componente gerenciador AWS IoT Greengrass secreto, visite Gerenciador secreto no Guia do AWS IoT Greengrass Version 2 desenvolvedor.

Para obter informações sobre como gerenciar o acesso aos segredos do Secrets Manager, visite:

- Quem tem permissão para seus AWS Secrets Manager segredos.
- Determinar se uma solicitação é permitida ou negada em uma conta.

Etapa 1: Criar segredos de autenticação de origem

Você pode usar AWS Secrets Manager para criar um segredo de autenticação para sua fonte de dados. No segredo, defina os pares de chave-valor **`username`** e **`password`** que contenham detalhes da autenticação para sua fonte de dados.

Para criar um segredo (console)

1. Navegue até o console do AWS Secrets Manager.
2. Selecione Armazenar um novo segredo.

3. Em Tipo de segredo, escolha Outro tipo de segredos.
4. Em Pares de chave/valor, faça o seguinte:
    1. Na primeira caixa de entrada, digite **`username`** e na segunda caixa de entrada digite o nome de usuário.
    2. Escolha Adicionar linha.
    3. Na primeira caixa de entrada, digite **`password`** e na segunda caixa de entrada digite a senha.
5. Em Chave de criptografia, selecione aws/secretsmanager e escolha Avançar.
6. Na página Armazenar um novo segredo, insira um Nome do segredo.
7. (Opcional) Insira uma Descrição que o ajude a identificar esse segredo e escolha Próximo.
8. (Opcional) Na página Armazenar um novo segredo, habilite Alternância automática. Para obter mais informações, consulte Alternar segredos no Guia do usuário do AWS Secrets Manager .
9. Especifique um cronograma de alternância.
10. Escolha uma função do Lambda que possa alternar esse segredo e, em seguida, escolha Próximo.
11. Revise suas configurações de segredo e escolha Armazenar.

Para autorizar seu gateway SiteWise Edge a interagir com AWS Secrets Manager, a função do IAM para seu gateway SiteWise Edge deve permitir a `secretsmanager:GetSecretValue` ação. Você pode usar o dispositivo principal do Greengrass para pesquisar a política do IAM. Para obter mais informações sobre a atualização de uma política do IAM, consulte Edição de políticas do IAM no Guia AWS Identity and Access Management do usuário.

Example política

Substitua *`secret-arn`* por nome do recurso da Amazon (ARN) do segredo que você criou na etapa anterior. Para obter informações sobre como obter o ARN de um segredo, consulte Recuperar segredos do AWS Secrets Manager no Guia do usuário do AWS Secrets Manager .

```
{
"Version":"2012-10-17",
"Statement":[
  {
     "Action":[
        "secretsmanager:GetSecretValue"
     ],
```

```
      "Effect":"Allow",
      "Resource":[
         "secret-arn"
      ]
   }
]
}
```

Etapa 2: implantar segredos em seu dispositivo de gateway SiteWise Edge

Você pode usar o AWS IoT SiteWise console para implantar segredos em seu gateway SiteWise Edge.

Para implantar um segredo (console)

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Gateways da .
3. Na lista Gateways, escolha o gateway SiteWise Edge de destino.
4. Na seção Configuração do gateway, escolha o link do dispositivo principal do Greengrass para abrir o AWS IoT Greengrass núcleo associado ao gateway SiteWise Edge.
5. No painel de navegação, escolha Implantação.
6. Escolha a implantação de destino e, em seguida, escolha Revisar.
7. Na página Especificar destino, escolha Próximo.
8. Na página Selecionar componentes, na seção Componentes públicos, desative Mostrar somente componentes selecionados.
9. Pesquise e escolha o aws.greengrass. SecretManagercomponente e, em seguida, escolha Avançar.
10. Na lista de componentes selecionados, escolha aws.greengrass. SecretManagercomponente e, em seguida, escolha Configurar componente.
11. No campo Configuração a ser mesclada, adicione o seguinte objeto JSON.

> **Note**
>
> Substitua *secret-arn* pelo ARN do segredo que você criou na etapa anterior. Para obter informações sobre como obter o ARN de um segredo, consulte Recuperar segredos do AWS Secrets Manager no Guia do usuário do AWS Secrets Manager .

```
{
"cloudSecrets":[
  {
     "arn":"secret-arn"
  }
]
}
```

12. Selecione a opção Confirmar.
13. Selecione Next (Próximo).
14. Na página Definir configurações de segurança, escolha Próximo.
15. Revise suas configurações de implantação e, em seguida, escolha Implantar.

Etapa 3: Adicionar configurações de autenticação

Você pode usar o AWS IoT SiteWise console para adicionar configurações de autenticação ao seu gateway SiteWise Edge.

Para adicionar configurações de autenticação (console)

1. Navegue até o console do AWS IoT SiteWise.
2. Na lista Gateways, escolha o gateway SiteWise Edge de destino.
3. Na lista Fonte de dados, escolha a fonte de dados de destino e, em seguida, escolha Editar.
4. Na página Adicionar uma fonte de dados, escolha Configuração avançada.
5. Para Configuração da autenticação, escolha o segredo implantado na etapa anterior.
6. Escolha Salvar.

Selecionar um destino para os dados do servidor de origem

Os dados são exportados da borda para AWS IoT SiteWise em tempo real ou em lotes usando o Amazon S3. Você também pode enviar o fluxo para outro componente usando um AWS IoT Greengrass fluxo.

- AWS IoT SiteWise em tempo real — escolha essa opção para enviar dados diretamente para o AWS IoT SiteWise armazenamento. Ingira e monitore dados em tempo real e processe dados na borda.
- AWS IoT SiteWise Armazenado em buffer usando o Amazon S3 — Envie dados em formato parquet para o Amazon S3 e depois importe para o armazenamento. AWS IoT SiteWise Escolha essa opção para ingerir dados em lotes e armazenar dados históricos de forma econômica. Você pode configurar sua localização preferida de bucket do Amazon S3 e a frequência com que deseja que os dados sejam carregados para o Amazon S3. Você também pode escolher o que fazer com os dados após a ingestão no AWS IoT SiteWise. Você pode optar por ter os dados disponíveis no Amazon S3 SiteWise e no Amazon S3 ou pode optar por excluí-los automaticamente do Amazon S3.
  - O bucket do Amazon S3 é um mecanismo de armazenamento e armazenamento em buffer e oferece suporte a arquivos no formato parquet.
  - Se você marcar a caixa de seleção Importar dados para o AWS IoT SiteWise armazenamento, os dados serão carregados primeiro no Amazon S3 e depois no AWS IoT SiteWise armazenamento.
    - Se você marcar a caixa de seleção Excluir dados do Amazon S3, os dados serão excluídos do Amazon S3 após serem importados para o armazenamento. SiteWise
    - Se você desmarcar a caixa de seleção Excluir dados do Amazon S3, os dados serão armazenados no Amazon S3 e no armazenamento. SiteWise
  - Se você desmarcar a caixa de seleção Importar dados para AWS IoT SiteWise armazenamento, os dados serão armazenados somente no Amazon S3. Não é importado para o SiteWise armazenamento.

  Visite Gerenciando o armazenamento de dados para obter detalhes sobre as várias opções de armazenamento AWS IoT SiteWise oferecidas. Para saber mais sobre as opções de preços, consulte AWS IoT SiteWise preços.
- AWS IoT Greengrass gerenciador de streams — Use AWS IoT Greengrass o gerenciador de streams para enviar dados para os seguintes Nuvem AWS destinos: canais em AWS IoT Analytics, streams no Amazon Kinesis Data Streams, propriedades de ativos ou objetos AWS IoT SiteWise no Amazon Simple Storage Service (Amazon S3). Para obter mais informações, consulte Gerenciar fluxos de dados no AWS IoT Greengrass Core no Guia do AWS IoT Greengrass Version 2 desenvolvedor.

O exemplo a seguir mostra a estrutura de mensagem de fluxo de dados necessária. Todos os campos são obrigatórios.

```
{
    "assetId": "string",
    "propertyAlias": "string",
    "propertyId": "string",
    "propertyValues": [
      {
         "quality": "string",
         "timestamp": {
            "offsetInNanos": number,
            "timeInSeconds": number
         },
         "value": {
            "booleanValue": boolean,
            "doubleValue": number,
            "integerValue": number,
            "stringValue": "string"
         }
      }
    ]
}
```

> **Note**
>
> A mensagem do fluxo de dados deve incluir (`assetIdepropertyId`) ou `propertyAlias` em sua estrutura.

`assetId`

(Opcional) O ID do ativo a ser atualizado.

`propertyAlias`

(Opcional) O alias que identifica a propriedade, como um caminho de fluxo de dados do servidor OPC-UA. Por exemplo: .

```
/company/windfarm/3/turbine/7/temperature
```

Para obter mais informações, consulte Mapeamento de fluxos de dados industriais para propriedades de ativos no Guia do AWS IoT SiteWise usuário.

`propertyId`

(Opcional) O ID da propriedade do ativo dessa entrada.

`propertyValues`

(Obrigatório) A lista de valores de propriedade a serem carregados. Você pode especificar até 10 elementos da `propertyValues` matriz.

`quality`

(Opcional) A qualidade do valor da propriedade do ativo.

`timestamp`

(Obrigatório) A data e hora do valor da propriedade do ativo.

`offsetInNanos`

(Opcional) O deslocamento de nanossegundos de. `timeInSeconds`

`timeInSeconds`

(Obrigatório) A data do carimbo de data/hora, em segundos, no formato Unix epoch. Os dados fracionários de nanossegundos são fornecidos por `offsetInNanos`.

`value`

(Obrigatório) O valor da propriedade do ativo.

> **Note**
>
> Somente um dos valores a seguir pode existir no `value` campo.

`booleanValue`

(Opcional) Dados da propriedade do ativo do tipo Boolean (`trueoufalse`).

`doubleValue`

(Opcional) Dados da propriedade do ativo do tipo double (número de ponto flutuante).

`integerValue`

(Opcional) Dados da propriedade do ativo do tipo inteiro (número inteiro).

`stringValue`

(Opcional) Dados da propriedade do ativo do tipo string (sequência de caracteres).

Adicionando fontes de dados de parceiros aos gateways SiteWise Edge

Ao usar um gateway AWS IoT SiteWise Edge, você pode conectar uma fonte de dados de parceiro ao seu gateway SiteWise Edge e receber dados do parceiro em seu gateway SiteWise Edge e na AWS nuvem. Essas fontes de dados de parceiros são componentes de AWS IoT Greengrass desenvolvidos em parceria entre AWS e o parceiro. Quando você adiciona uma fonte de dados de parceiro, AWS IoT SiteWise criará esse componente e o implantará em seu gateway SiteWise Edge.

Para adicionar uma fonte de dados de parceiro, faça o seguinte:

- Adicionar fonte de dados de parceiros
- Acesse o portal web do parceiro e configure a fonte de dados do parceiro para que ela se conecte ao gateway SiteWise Edge.

Tópicos

Segurança

Como parte do Modelo de Responsabilidade Compartilhada entre AWS, nossos clientes e nossos parceiros, o seguinte descreve quem é responsável pelos diferentes aspectos da segurança:

Responsabilidade do cliente

- Avaliação do parceiro.

- Configurar o acesso à rede concedido ao parceiro.

Responsabilidade da AWS

- Isolar o parceiro dos recursos de nuvem do AWS do cliente, exceto aqueles necessários para o parceiro. Nesse caso, ingestão de AWS IoT SiteWise.
- Restringir a solução do parceiro a um uso razoável dos recursos da máquina do gateway SiteWise Edge (CPU, memória, sistema de arquivos).

Responsabilidade do parceiro

- Usar padrões seguros.
- Manter a solução segura ao longo do tempo por meio de patches e outras atualizações adequadas.
- Manter a confidencialidade dos dados do cliente.

Adicionar fonte de dados de parceiros

Para conectar uma fonte de dados de parceiro ao seu gateway SiteWise Edge, adicione-a como fonte de dados. Quando você o adiciona como fonte de dados, AWS IoT SiteWise implantará um AWS IoT Greengrass componente privado no seu gateway SiteWise Edge.

Pré-requisitos

Para adicionar uma fonte de dados de parceiro, faça o seguinte:

- Crie uma conta com o parceiro.
- Vincule as contas.

Para criar um gateway SiteWise Edge com uma fonte de dados do parceiro

Se você quiser criar um novo gateway SiteWise Edge, conclua as etapas emCriando um gateway SiteWise Edge. Depois de criar o SiteWise Edge Gateway, siga as etapas Para adicionar uma fonte de dados de parceiro a um gateway SiteWise Edge existente para adicionar uma fonte de dados de parceiro.

Para adicionar uma fonte de dados de parceiro a um gateway SiteWise Edge existente

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Gateways da .

3. Escolha o gateway SiteWise Edge ao qual você deseja conectar a fonte de dados do parceiro.
4. Em Fontes de dados, escolha Adicionar uma fonte de dados.
5. Em Tipo de fonte, escolha o parceiro ao qual você deseja conectar seu gateway SiteWise Edge.

> **Note**
>
> Atualmente, EasyEdge é a única fonte de dados de parceiros disponível. Na primeira vez que você adicionar uma fonte de EasyEdge dados, precisará criar uma EasyEdge conta.

6. Insira um nome para a origem.
7. Para conceder ao parceiro acesso à fonte de dados, selecione Autorizar.
8. Para permitir que AWS IoT SiteWise atualize o componente do publicador de AWS IoT SiteWise e, se o pacote de processamento de dados estiver habilitado, o componente do processador AWS IoT SiteWise, selecione Atualizar componentes.
9. Escolha Salvar.

Configure o docker no seu SiteWise gateway Edge

Para adicionar uma fonte de dados parceira, o Docker Engine 1.9.1 ou posterior deve estar instalado em seu dispositivo local.

> **Note**
>
> A versão 20.10 é a versão mais recente verificada para funcionar com o software SiteWise Edge Gateway.

Para verificar se o Docker está instalado

Para verificar se o Docker está instalado, execute o seguinte comando em um terminal conectado ao seu gateway SiteWise Edge:

```
docker info
```

Se o comando retornar um resultado `docker is not recognized` ou se uma versão mais antiga do Docker estiver instalada, Instale o Docker Engine antes de continuar.

Para configurar o Docker

O usuário do sistema que executa um componente de contêiner do Docker deve ter permissões de raiz ou administrador, ou você deve configurar o Docker para executá-lo como usuário não raiz ou não administrador.

Em dispositivos Linux, você deve adicionar um usuário de `ggc_user` ao grupo de `docker` para chamar os comandos do Docker sem `sudo`.

Para adicionar `ggc_user` ou o usuário não raiz que você usa para executar componentes de contêiner do Docker ao grupo de `docker`, execute o seguinte comando:

```
sudo usermod -aG docker ggc_user
```

Para obter mais informações, consulte Etapas pós-instalação do Linux para o Docker Engine.

SiteWise Fontes de dados de parceiros do Edge Gateway

Use as informações abaixo para configurar uma fonte de dados do parceiro.

EasyEdge

Portal:

https://studio.easyedge.io/

EasyEdge documentação:

EasyEdge para AWS

EasyEdge requisitos — Informações sobre EasyEdge requisitos, incluindo terminais e portas necessários para configurar o firewall. Observação: você precisará de uma EasyEdge conta para acessar essa documentação.

Usar pacotes

AWS IoT SiteWise Os gateways Edge usam pacotes diferentes para determinar como coletar e processar seus dados.

Atualmente, os seguintes pacotes estão disponíveis:

- Pacote de coleta de dados — Use esse pacote para coletar seus dados industriais e encaminhá-los para destinos AWS na nuvem. Por padrão, esse pacote é habilitado automaticamente para seu gateway SiteWise Edge.
- Pacote de processamento de dados — Use este pacote para habilitar a comunicação do gateway SiteWise Edge com modelos e ativos de ativos configurados na borda. Você pode usar a configuração de borda para controlar quais dados do ativo devem ser computados e processados no local. Você pode então enviar seus dados para AWS IoT SiteWise ou outros AWS serviços. Para obter mais informações sobre o pacote de processamento de dados, consulte the section called “Habilitar o processamento de dados de borda”.

Atualizar pacotes

> **Important**
>
> A atualização das versões do pacote de processamento de dados anteriores (e incluindo) 2.0.x para a versão 2.1.x resultará na perda de dados das medições armazenadas localmente.

SiteWise Os gateways Edge usam pacotes diferentes para determinar como coletar e processar seus dados. Você pode usar o AWS IoT SiteWise console para atualizar pacotes.

Para atualizar pacotes (console)

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Gateways da .
3. Na lista Gateways, escolha o gateway SiteWise Edge com os pacotes que você deseja atualizar.
4. Na seção Configuração do gateway, escolha Atualizações de software disponíveis.
5. Na página de edição de versões de software, na seção Atualizações de componentes do Gateway, faça o seguinte:
   - Para atualizar o coletor OPC-UA, escolha uma versão e, em seguida, escolha Implantar.
   - Para atualizar o Publisher, escolha uma versão e, em seguida, escolha Implantar.
   - Para atualizar o pacote de processamento de dados, escolha uma versão e escolha Implantar.
6. Quando terminar de implantar novas versões, escolha Concluído.

Se você estiver tendo problemas para atualizar os pacotes, consulte Não é possível implantar pacotes nos gateways SiteWise Edge.

Gerenciando gateways SiteWise Edge

Você pode usar o AWS IoT SiteWise console e as operações da API para gerenciar os gateways do AWS IoT SiteWise Edge. Você também pode usar o aplicativo AWS OpsHub for AWS IoT SiteWise for Windows para gerenciar alguns aspectos do gateway SiteWise Edge a partir do seu dispositivo local.

É altamente recomendável que você use o AWS IoT SiteWise aplicativo AWS OpsHub for para monitorar o uso do disco em seu dispositivo local. Você também pode monitorar as CloudWatch métricas da `Gateway.UsedPercentageDiskSpace` Amazon `Gateway.AvailableDiskSpace` e criar alarmes para ser notificado quando o espaço em disco estiver ficando baixo. Para obter mais informações sobre CloudWatch os alarmes da Amazon, consulte Criar um CloudWatch alarme com base em um limite estático.

Certifique-se de que seu dispositivo tenha espaço suficiente para os próximos dados. Quando você está prestes a ficar sem espaço em seu dispositivo local, o serviço exclui automaticamente uma pequena quantidade de dados com os registros de data e hora mais antigos para abrir espaço para os próximos dados.

Para verificar se o serviço excluiu seus dados, faça o seguinte:

1. Faça login no AWS IoT SiteWise formulário AWS OpsHub de inscrição.
2. Escolha Configurações.
3. Em Logs, especifique um intervalo de tempo e escolha Baixar.
4. Descompacte o arquivo de log.
5. Se o arquivo de log contiver a seguinte mensagem, o serviço excluiu seus dados: o *`número`* de bytes de dados foi excluído para evitar que o armazenamento do SiteWise Edge Gateway fique sem espaço.

Gerenciando seu gateway SiteWise Edge com o AWS IoT SiteWise console

Você pode usar o AWS IoT SiteWise console para configurar, atualizar e monitorar todos os gateways do SiteWise Edge em sua AWS conta.

Você pode visualizar seus gateways do SiteWise Edge navegando até a página Edge Gateways no console.AWS IoT SiteWise Para acessar a página de detalhes do gateway Edge de um gateway específico, escolha o nome de um gateway Edge.

Na guia Visão geral da página de detalhes do gateway Edge, você pode fazer o seguinte:

- Na seção Fontes de dados, atualize a configuração da fonte de dados e configure fontes de dados adicionais
- Escolha Abrir CloudWatch métricas para visualizar o número de pontos de dados ingeridos por fonte de dados no console de CloudWatch métricas
- Na seção Recursos do Edge, adicione pacotes de dados ao seu gateway do SiteWise Edge clicando em Editar
- Na seção Configuração do gateway, visualize o status de conectividade dos seus gateways SiteWise Edge
- Na seção Configuração do editor, visualize o status de sincronização do gateway SiteWise Edge e a configuração do componente do AWS IoT SiteWise editor

Na guia Atualizações da página de detalhes do gateway Edge, você pode ver as versões atuais do componente e do pacote que estão implantadas no gateway Edge. Também é aqui que você implanta novas versões, quando elas estão disponíveis.

Gerenciando gateways SiteWise Edge usando AWS OpsHub para AWS IoT SiteWise

Você usa o AWS IoT SiteWise aplicativo AWS OpsHub for para gerenciar e monitorar seus gateways SiteWise Edge. Esse aplicativo fornece as seguintes opções de monitoramento e gerenciamento:

- Em Visão geral, você pode fazer o seguinte:
  - Veja os detalhes do gateway SiteWise Edge que ajudam você a obter informações sobre os dados do dispositivo do gateway SiteWise Edge, identificar problemas e melhorar o desempenho do gateway SiteWise Edge.
  - Veja SiteWise os portais do Monitor que monitoram os dados de servidores e equipamentos locais na borda. Para obter mais informações, consulte O que é o AWS IoT SiteWise Monitor no Guia do aplicativo do AWS IoT SiteWise Monitor .

- Em Health, há um painel que exibe dados do seu gateway SiteWise Edge. Especialistas no domínio, como engenheiros de processo, podem usar o painel para ter uma visão geral do comportamento do gateway SiteWise Edge.
- Em Ativos, visualize os ativos implantados no dispositivo local e o último valor coletado ou calculado para as propriedades do ativo.
- Em Configurações, faça o seguinte:
  - Se o Pacote de Processamento de Dados estiver instalado, visualize as informações de configuração do gateway SiteWise Edge e sincronize os recursos com a AWS nuvem.
  - Baixe os arquivos de autenticação que você pode usar para acessar o gateway SiteWise Edge usando outras ferramentas.
  - Baixe registros que você pode usar para solucionar problemas no gateway SiteWise Edge.
  - Veja os AWS IoT SiteWise componentes implantados no gateway SiteWise Edge.

> **Important**
>
> É necessário usar o seguinte AWS OpsHub para AWS IoT SiteWise:
>
> - Seu dispositivo local e o AWS IoT SiteWise aplicativo AWS OpsHub for devem estar conectados à mesma rede.
> - O pacote de processamento de dados deve estar ativado.

Para gerenciar gateways SiteWise Edge usando AWS OpsHub

1. Baixe e instale o aplicativo AWS OpsHubAWS IoT SiteWise for for Windows.
2. Abra o aplicativo .
3. Se você não tiver credenciais locais configuradas para seu gateway, siga as etapas abaixo Acessando seu gateway SiteWise Edge usando credenciais do sistema operacional local para configurá-las.
4. Você pode entrar no seu gateway SiteWise Edge com suas credenciais Linux ou Lightweight Directory Access Protocol (LDAP). Para entrar no seu gateway SiteWise Edge, faça o seguinte:

   Linux

   1. Em Nome do host ou endereço IP, insira o nome do host ou endereço IP do seu dispositivo local.

2. Para Autenticação, escolha Linux.
3. Em Nome de usuário, insira o nome de usuário do sistema operacional Linux.
4. Em Senha, insira a senha do sistema operacional Linux.
5. Escolha Logon.

LDAP

1. Em Nome do host ou endereço IP, insira o nome do host ou endereço IP do seu dispositivo local.
2. Para Autenticação, escolha LDAP.
3. Em Nome de usuário, insira o nome de usuário do LDAP.
4. Em Senha, insira a senha do LDAP.
5. Escolha Logon.

Acessando seu gateway SiteWise Edge usando credenciais do sistema operacional local

Além do Lightweight Directory Access Protocol (LDAP), você pode usar as credenciais do Linux ou do Windows para acessar seu SiteWise gateway Edge.

> **Important**
>
> Para acessar seu gateway SiteWise Edge com credenciais Linux, você deve ativar o pacote de processamento de dados para seu gateway SiteWise Edge.

Acessando seu gateway SiteWise Edge usando as credenciais do sistema operacional Linux

Essas etapas a seguir presumem que você usa um dispositivo com Ubuntu. Se você usa uma distribuição Linux diferente, consulte a documentação relevante do seu dispositivo.

Para criar um grupo de usuários Linux

1. Execute um dos comandos a seguir para criar um grupo de administradores.

```
sudo groupadd --system SWE_ADMIN_GROUP
```

Os usuários do SWE_ADMIN_GROUP grupo podem permitir acesso de administrador ao gateway SiteWise Edge.

2. Execute um dos comandos a seguir para criar um grupo de usuário.

```
sudo groupadd --system SWE_USER_GROUP
```

Os usuários do SWE_USER_GROUP grupo podem permitir acesso somente de leitura ao gateway SiteWise Edge.

3. Execute o seguinte comando para adicionar um usuário ao grupo de administradores. Substitua o *nome de usuário* e a *senha* pelo nome de usuário e senha que você deseja adicionar.

```
sudo useradd -p $(openssl passwd -1 password) user-name
```

4. Para adicionar um usuário a SWE_ADMIN_GROUP ou SWE_USER_GROUP, substitua o *nome de usuário* pelo nome de usuário que você adicionou na etapa anterior.

```
sudo usermod -a -G SWE_ADMIN_GROUP user-name
```

Agora você pode usar o nome de usuário e a senha para entrar no gateway SiteWise Edge no AWS IoT SiteWise aplicativo AWS OpsHub for.

Acessando seu gateway SiteWise Edge usando credenciais do Windows

Essas etapas a seguir presumem que você usa um dispositivo com Windows.

> **Important**
>
> A segurança é uma responsabilidade compartilhada entre você AWS e você. Crie uma política de senha forte com pelo menos 12 caracteres e uma combinação de maiúscula, minúscula, números e símbolos. Além disso, defina as regras do Firewall do Windows para permitir o tráfego de entrada na porta 443 e bloquear o tráfego de entrada em todas as outras portas.

Para criar um grupo de usuários no Windows Server

1. Execute PowerShell como administrador.

a. No servidor Windows em que você deseja instalar o SiteWise Edge Gateway, faça login como administrador.

b. Entre PowerShellna barra de pesquisa do Windows.

c. Nos resultados da pesquisa, clique com o botão direito do mouse no PowerShell aplicativo do Windows. Escolha Executar como administrador.

2. Execute um dos comandos a seguir para criar um grupo de administradores.

```
net localgroup SWE_ADMIN_GROUP /add
```

Você deve ser um usuário do `SWE_ADMIN_GROUP` grupo para permitir o acesso de administrador ao gateway SiteWise Edge.

3. Execute um dos comandos a seguir para criar um grupo de usuário.

```
net localgroup SWE_USER_GROUP /add
```

Você deve ser um usuário do `SWE_USER_GROUP` grupo para permitir acesso imediato ao gateway SiteWise Edge.

4. Execute o seguinte comando para adicionar usuário. Substitua o *`nome de usuário`* e a *`senha`* pelo nome de usuário e senha que você deseja criar.

```
net user user-name password /add
```

5. Execute o seguinte comando para adicionar um usuário ao grupo de administradores. Substitua o *`nome de usuário`* pelo nome de usuário que você deseja adicionar.

```
net localgroup SWE_ADMIN_GROUP user-name /add
```

Agora você pode usar o nome de usuário e a senha para entrar no gateway SiteWise Edge no AWS IoT SiteWise aplicativo AWS OpsHub for.

Gerenciando o certificado de gateway SiteWise Edge

Você pode usar o SiteWise Monitor e aplicativos de terceiros, como o Grafana, em seus dispositivos de gateway SiteWise Edge. Esses aplicativos exigem uma conexão TLS com o serviço. SiteWise Atualmente, os gateways Edge usam um certificado autoassinado. Se você usar um navegador para

abrir os aplicativos, como um portal do SiteWise Monitor, poderá receber um aviso de certificado não confiável.

A seguir, mostramos como baixar o certificado confiável do AWS IoT SiteWise aplicativo AWS OpsHub for.

1. Faça login no aplicativo.
2. Escolha Configurações.
3. Em Autenticação, escolha Baixar certificado.

O seguinte pressupõe que você usa o Google Chrome ou FireFox. Se você usa um outro navegador, consulte a documentação relevante do seu navegador. Para adicionar o certificado baixado na etapa anterior ao navegador, faça o seguinte:

- Se você usa o Google Chrome, vá até Configurar certificados na documentação de ajuda do Google Chrome Enterprise.
- Se você usa o Firefox, vá até Para carregar o certificado no navegador Mozilla ou Firefox na documentação da Oracle.

Alterando a versão dos pacotes de componentes do SiteWise Edge Gateway

Você pode usar o AWS IoT SiteWise console para alterar a versão dos pacotes de componentes em seus gateways SiteWise Edge.

Para alterar a versão de um pacote de componentes do SiteWise Edge Gateway

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação à esquerda, escolha Gateways.
3. Selecione o gateway SiteWise Edge para o qual você gostaria de alterar as versões do pacote.
4. Em Configuração do gateway, escolha Exibir versões do software.
5. Na página Editar versões de software, para o pacote do qual você deseja atualizar a versão, selecione a versão que deseja implantar e escolha Implantar.
6. Escolha Concluído.

Running SiteWise Edge na Siemens Industrial Edge

Você pode ingerir dados do seu dispositivo Siemens Industrial Edge para o seu Conta da AWS executando um gateway SiteWise Edge no dispositivo. Para fazer isso, você cria um recurso de gateway SiteWise Edge com um destino de implantação do dispositivo Siemens Industrial Edge - novo, baixa o arquivo de configuração e o carrega em seu aplicativo Siemens por meio do portal Siemens Industrial Edge Management (IEM). Para obter mais informações sobre como executar o AWS IoT SiteWise Edge no Siemens Industrial Edge, incluindo como configurar os recursos necessários da Siemens, consulte O que é o Industrial Edge? na documentação da Siemens.

> **Note**
>
> A Siemens não é fornecedora nem fornecedora do Edge. AWS IoT SiteWise O Siemens Industrial Edge Marketplace é um mercado independente.

Tópicos

Pré-requisitos

Para executar o AWS IoT SiteWise Edge no Siemens Industrial Edge, você precisa do seguinte:

- Uma conta da Siemens Digital Exchange Platform
- Uma conta do Siemens Industrial Edge Hub (iehub)
- Uma instância do Siemens Industrial Edge Management (IEM)
- Um dispositivo Siemens Industrial Edge (IED) ou um dispositivo virtual Siemens Industrial Edge (iEVD)
- Acesso à meta de implantação do dispositivo Siemens Industrial Edge. Para obter acesso, acesse o AWS IoT SiteWise console e escolha Solicitar acesso.

Segurança

Como parte do Modelo de Responsabilidade Compartilhada entre AWS nossos clientes e nossos parceiros, o seguinte descreve quem é responsável pelos diferentes aspectos da segurança:

Responsabilidade do cliente

- Avaliação do parceiro.
- Configurar o acesso à rede concedido ao parceiro.
- Protegendo fisicamente o dispositivo que executa o AWS IoT SiteWise Edge.

AWS responsabilidade

- Isolando o parceiro dos recursos de AWS nuvem do cliente.

Responsabilidade do parceiro

- Usar padrões seguros.
- Manter a solução segura ao longo do tempo por meio de patches e outras atualizações adequadas.
- Manter a confidencialidade dos dados do cliente.
- Verificando outros aplicativos disponíveis no mercado de parceiros.

Durante a fase de pré-visualização desse recurso, os dados do cliente armazenados em AWS IoT SiteWise cache no dispositivo do parceiro podem ser acessados pelo parceiro e por outros aplicativos instalados por meio do mercado parceiro.

Criar o arquivo de configuração

Depois de ter as contas e instâncias IEM adequadas da Siemens, você pode criar um gateway SiteWise Edge do tipo de implantação do dispositivo Siemens Industrial Edge.

Para criar o arquivo de configuração

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, escolha Edge gateways.
3. Escolha Criar gateway.
4. Para o tipo de implantação, escolha o dispositivo Siemens Industrial Edge - novo.
5. Insira um nome para seu gateway SiteWise Edge ou use o nome gerado por AWS IoT SiteWise.
6. (Opcional) Na configuração avançada, faça o seguinte:

- Insira um nome para sua AWS IoT Core coisa ou use o nome gerado por AWS IoT SiteWise.

7. Escolha Criar gateway.
8. Na caixa de diálogo Gerar arquivo de configuração do gateway SiteWise Edge, escolha Gerar e baixar. AWS IoT SiteWise gera automaticamente um arquivo de configuração que você usará para configurar o aplicativo AWS IoT SiteWise Edge.

> **Important**
>
> Certifique-se de salvar o arquivo de configuração em um local seguro. Você usará o arquivo posteriormente.

Agora que você criou o gateway SiteWise Edge, faça o seguinte para concluir a configuração do gateway SiteWise Edge:

1. Adicionar fontes de dados
2. Configurar o componente Publisher

Depois de ter o arquivo de configuração e o gateway SiteWise Edge estar configurado, baixe o aplicativo AWS IoT SiteWise Edge do Siemens Industrial Edge Marketplace e instale-o usando o portal Siemens Industrial Edge Management (IEM). Em seguida, acesse seu dispositivo Siemens Industrial Edge por meio do portal Siemens Industrial Edge Management (IEM) e carregue o arquivo de configuração no dispositivo em que você deseja instalar o SiteWise gateway Edge.

Solução de problemas

Para solucionar problemas do gateway SiteWise Edge em seu dispositivo Siemens Industrial Edge, você pode acessar os registros do aplicativo por meio dos portais Siemens Industrial Edge Management (IEM) ou Siemens Industrial Edge Device (IED). Para obter mais informações, consulte Download de registros na documentação da Siemens.

Eu vejo 'SESSION_TAKEN_OVER' ou 'com.aws.greengrass.mqttclient. MqttClient: Falha ao publicar a mensagem via Spooler e tentarei novamente. ' nos registros

Se você ver um aviso que inclui `SESSION_TAKEN_OVER` ou um erro incluído `com.aws.greengrass.mqttclient.MqttClient: Failed to publish the message via`

`Spooler and will retry.` em seus registros em`/greengrass/v2/logs/greengrass.log`, você pode estar tentando usar o mesmo arquivo de configuração para vários gateways do SiteWise Edge em vários dispositivos. Cada gateway SiteWise Edge precisa de um arquivo de configuração exclusivo para se conectar ao seu Conta da AWS.

Eu vejo 'com.aws.greengrass.deployment. IotJobsHelper: Nenhum trabalho de implantação encontrado. ' ou “Resultado da implantação já reportado”. nos registros

Se você ver `com.aws.greengrass.deployment.IotJobsHelper: No deployment job found.` ou `Deployment result already reported.` aparecer em seus registros em`/greengrass/v2/logs/greengrass.log`, talvez esteja tentando reutilizar o mesmo arquivo de configuração.

Há várias soluções:

- Se você quiser reutilizar o arquivo de configuração, faça o seguinte:
  1. Navegue até o console do AWS IoT SiteWise.
  2. No painel de navegação, selecione Gateways da .
  3. Escolha o gateway SiteWise Edge que você deseja reutilizar.
  4. Escolha a guia Atualizações.
  5. Selecione uma versão diferente do Publisher e escolha Implantar.
- Siga as etapas Criar o arquivo de configuração para criar um novo arquivo de configuração.

Eu vejo 'Arquivo de configuração ausente AWS_REGION' nos registros.

Se você ver `Config file missing AWS_REGION` nos registros da Siemens, o JSON do arquivo de configuração foi corrompido. Você precisará criar um novo arquivo de configuração. Siga as etapas Criar o arquivo de configuração para criar um novo arquivo de configuração.

Entre em contato conosco

- Se você quiser solicitar acesso ao aplicativo, acesse o AWS IoT SiteWise console e escolha Solicitar acesso.
- Se precisar de ajuda para solucionar problemas do aplicativo, acesse o AWS IoT SiteWise console, navegue até a página de detalhes do gateway SiteWise Edge e escolha Obter suporte.

Filtrando ativos em um gateway SiteWise Edge

Você pode usar a filtragem de borda para gerenciar seus ativos com mais eficiência enviando somente um subconjunto de ativos para um gateway SiteWise Edge específico para uso no processamento de dados. Se seus ativos estiverem organizados em uma estrutura de árvore, ou pai-filho, você pode configurar uma política do IAM anexada à função do IAM de um gateway do SiteWise Edge que permite que somente a raiz da árvore, ou pai, e seus filhos sejam enviados para um gateway SiteWise Edge específico.

> **Note**
>
> Se você estiver organizando os ativos existentes em uma estrutura de árvore, depois de criar a estrutura, acesse cada ativo existente que você adicionou à estrutura e escolha Editar e, em seguida, escolha Salvar para garantir que a nova estrutura seja AWS IoT SiteWise reconhecida.

Configurar a filtragem de borda

Configure a filtragem de SiteWise borda no seu gateway do Edge adicionando a seguinte política do IAM à função do IAM do gateway do SiteWise Edge, substituindo *< root-asset-id >* pelo ID do ativo raiz que você deseja enviar para o gateway do SiteWise Edge.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "iotsitewise:DescribeAsset",
                "iotsitewise:ListAssociatedAssets"
            ],
            "Resource": "arn:aws:iotsitewise:*:*:asset/*",
            "Condition": {
                "StringNotLike": {
                    "iotsitewise:assetHierarchyPath": "/<root-asset-id>*"
                }
            }
        }
    ]
```

```
}
```

Se houver ativos atualmente no gateway do SiteWise Edge que você gostaria de remover, faça login no gateway do SiteWise Edge e execute o comando a seguir para forçar a sincronização do gateway do SiteWise Edge AWS IoT SiteWise excluindo o cache.

```
sudo rm /greengrass/v2/work/aws.iot.SiteWiseEdgeProcessor/sync-app/
sync_resource_bundles/edge.json
```

Usar APIs AWS IoT SiteWise na borda

Você pode usar um subconjunto de APIs AWS IoT SiteWise disponíveis junto com APIs específicas de borda para interagir com modelos de ativo e seus ativos na borda. Os modelos de ativos devem ser configurados para serem executados na borda. Para ter mais informações, consulte Processamento de dados na borda.

Use essas APIs para coletar dados sobre seus modelos de ativo e ativos, monitorar seus portais implantados e métricas de painel e obter dados de ativos coletados na borda. Isso fornece um host central na rede para interações com AWS IoT SiteWise sem exigir uma chamada de API da web.

Tópicos

- Todas as APIs disponíveis para uso com dispositivos na borda de AWS IoT SiteWise
- APIs somente de borda para uso com dispositivos de borda do AWS IoT SiteWise
- Tutorial: Obter uma lista de modelos de ativos em um gateway SiteWise Edge

Todas as APIs disponíveis para uso com dispositivos na borda de AWS IoT SiteWise

Ao trabalhar com dispositivos na borda, você pode usar uma variedade de APIs para interagir com AWS IoT SiteWise e concluir tarefas localmente no dispositivo.

APIs AWS IoT SiteWise disponíveis

As seguintes APIs AWS IoT SiteWise estão disponíveis em dispositivos na borda:

- ListAssetModels

- DescribeAssetModel
- ListAssets
- DescribeAsset
- DescribeAssetProperty
- ListAssociatedAssets
- GetAssetPropertyAggregates
- GetAssetPropertyValue
- GetAssetPropertyValueHistory
- ListDashboards
- ListPortals
- ListProjectAssets
- ListProjects
- DescribeDashboard
- DescribePortal
- DescribeProject

APIs somente de borda disponíveis

As seguintes APIs são usadas localmente em dispositivos na borda:

- Authenticate — Use essa API para obter as credenciais temporárias do SigV4 que você usará para fazer chamadas de API.

APIs somente de borda para uso com dispositivos de borda do AWS IoT SiteWise

Além das APIs AWS IoT SiteWise que estão disponíveis na borda, existem outras específicas para borda. Essas APIs específicas para borda são descritas abaixo.

Authenticate

Obtém as credenciais do gateway SiteWise Edge. Você precisará adicionar usuários locais ou se conectar ao seu sistema usando LDAP ou um grupo de usuários Linux. Para obter mais informações sobre como adicionar usuários, consulte LDAP ou grupo de usuários Linux.

Sintaxe da solicitação

```
POST /authenticate HTTP/1.1
Content-type: application/json
{
  "username": "string",
  "password": "string",
  "authMechanism": "string"
}
```

Parâmetros da solicitação de URI

A solicitação não usa nenhum parâmetro de URI.

Corpo da solicitação

A solicitação aceita os dados a seguir no formato JSON.

username

O nome de usuário usado para validar a chamada de solicitação.

Tipo: sequência

Obrigatório: Sim

password

A senha do usuário solicitando as credenciais.

Tipo: sequência

Obrigatório: Sim

authMechanism

O método de autenticação para validar esse usuário no host.

Tipo: string

Valores válidos: `ldap`, `linux`, `winnt`

Obrigatório: sim

Sintaxe da resposta

```
HTTP/1.1 200
Content-type: application/json
{
  "accessKeyId": "string",
  "secretAccessKey": "string",
  "sessionToken": "string",
  "region": "edge"
}
```

Elementos de resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON.

accessKeyId

O ID da chave de acesso que identifica as credenciais de segurança temporárias.

Restrições de tamanho: tamanho mínimo de 16. Comprimento máximo de 128.

Padrão: `[\w]*`

secretAccessKey

A chave de acesso secreta para assinar solicitações.

Tipo: string

sessionToken

O token que os usuários devem passar para a API do serviço para usar as credenciais temporárias.

Tipo: string

região

A região que você está direcionando para chamadas de API.

Tipo: CONSTANT - `edge`

Erros

IllegalArgumentException

A solicitação foi rejeitada porque o documento do corpo fornecido estava malformado. A mensagem de erro descreve o erro específico.

Código de Status HTTP: 400

AccessDeniedException

O usuário não tem credenciais válidas com base no provedor de identidade atual. A mensagem de erro descreve o mecanismo de autenticação.

Código de Status HTTP: 403

TooManyRequestsException

A solicitação atingiu o limite de tentativas de autenticação. A mensagem de erro contém a quantidade de tempo de espera até que novas tentativas de autenticação sejam feitas.

Código de Status HTTP: 429

Tutorial: Obter uma lista de modelos de ativos em um gateway SiteWise Edge

Você pode usar um subconjunto de APIs AWS IoT SiteWise disponíveis junto com APIs específicas de borda para interagir com modelos de ativo e seus ativos na borda. Este tutorial orientará você na obtenção de credenciais temporárias em um gateway do AWS IoT SiteWise Edge e na obtenção de uma lista dos modelos de ativos no gateway do SiteWise Edge.

Pré-requisitos

Nas etapas deste tutorial, você pode usar uma variedade de ferramentas. Para usar essas ferramentas, certifique-se de que você tem os pré-requisitos correspondentes instalados.

Para concluir este tutorial, você precisará do seguinte:

- Um SiteWise Requisitos do gateway Edge implantado e em execução
- Acesso ao seu gateway SiteWise Edge na mesma rede pela porta 443.
- OpenSSL instalado

- (AWS OpsHubparaAWS IoT SiteWise) O AWS IoT SiteWiseaplicativo AWS OpsHub for
- (curl) curl instalado
- (Python) urllib3 instalado
- (Python) Python3 instalado
- (Python) Boto3 instalado
- (Python) instalado BotoCore

Etapa 1: Obter um certificado assinado pelo serviço SiteWise Edge Gateway

Para estabelecer uma conexão TLS com as APIs disponíveis no gateway SiteWise Edge, você precisa de um certificado confiável. Você pode gerar esse certificado usando um AWS OpsHub OpenSSL ou for. AWS IoT SiteWise

OpenSSL

> **Note**
>
> Você precisa do OpenSSL instalado para executar esse comando.

Abra um terminal e execute o comando a seguir para obter um certificado assinado do gateway SiteWise Edge. `<sitewise_gateway_ip>`Substitua pelo IP do gateway SiteWise Edge.

```
openssl s_client -connect <sitewise_gateway_ip>:443 </dev/null 2>/dev/null | openssl
 x509 -outform PEM > GatewayCert.pem
```

AWS OpsHub for AWS IoT SiteWise

Você pode usar AWS OpsHub para AWS IoT SiteWise. Para ter mais informações, consulte Gerenciando gateways SiteWise Edge.

O caminho absoluto para o certificado de gateway SiteWise Edge baixado é usado neste tutorial. Execute o comando a seguir para exportar o caminho completo do seu certificado, substitua `<absolute_path_to_certificate>` pelo caminho para o certificado:

```
export PATH_TO_CERTIFICATE='<absolute_path_to_certificate>'
```

Etapa 2: Obtenha o nome de host SiteWise do gateway Edge

> **Note**
>
> Você precisa do OpenSSL instalado para executar esse comando.

Para concluir o tutorial, você precisará do nome do host do seu gateway SiteWise Edge. Para obter o nome do host do seu gateway SiteWise Edge, execute o seguinte, `<sitewise_gateway_ip>` substituindo pelo IP do gateway SiteWise Edge:

```
openssl s_client -connect <sitewise_gateway_ip>:443 </dev/null 2>/dev/null | grep -Po
 'CN = \K.*'| head -1
```

Execute o comando a seguir para exportar o nome do host para uso posterior, `<your_edge_gateway_hostname>` substituindo-o pelo nome do host do seu gateway SiteWise Edge:

```
export GATEWAY_HOSTNAME='<your_edge_gateway_hostname>'
```

Etapa 3: Obtenha credenciais temporárias para seu gateway SiteWise Edge

Agora que você tem o certificado assinado e o nome do host do seu gateway SiteWise Edge, você precisa obter credenciais temporárias para poder executar APIs no gateway. Você pode obter essas credenciais AWS OpsHub por meio AWS IoT SiteWise ou diretamente do gateway SiteWise Edge usando APIs.

> **Important**
>
> As credenciais expiram a cada 4 horas, então você deve obtê-las antes de usar as APIs no seu gateway Edge. SiteWise Não armazene credenciais no cache por mais de 4 horas.

Obtenha credenciais temporárias usando AWS OpsHub para AWS IoT SiteWise

> **Note**
>
> Você precisa do AWS OpsHub para o aplicativo do AWS IoT SiteWise instalado.

Para usar o AWS OpsHub para o aplicativo do AWS IoT SiteWise para obter suas credenciais temporárias, faça o seguinte:

1. Faça login no aplicativo.
2. Escolha Configurações.
3. Em Autenticação, escolha Copiar credenciais.
4. Expanda a opção adequada ao seu ambiente e escolha Copiar.
5. Salve as credenciais para usar depois.

Obtenha credenciais temporárias usando a API do SiteWise Edge Gateway

Para usar a API do gateway do SiteWise Edge para obter as credenciais temporárias, você pode usar um script Python ou curl. Primeiro, você precisará ter um nome de usuário e uma senha para SiteWise o gateway do Edge. Os gateways SiteWise Edge usam autenticação e autorização SigV4. Para obter mais informações sobre como adicionar usuários, consulte LDAP ou grupo de usuários Linux. Essas credenciais serão usadas nas etapas a seguir para obter as credenciais locais em seu gateway SiteWise Edge que são necessárias para usar as AWS IoT SiteWise APIs.

Python

> **Note**
>
> Você precisa ter urllib3 e Python3 instalados.

Para obter as credenciais usando Python

1. Crie um arquivo chamado get_credentials.py e copie o código a seguir nele.

```
'''
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. Execute o get_credentials.py a partir do terminal substituindo `<gateway_username>` e `<gateway_password>` pelas credenciais que você criou.

```
python3 get_credentials.py -e https://$GATEWAY_HOSTNAME -c $PATH_TO_CERTIFICATE
 -u '<gateway_username>' -p '<gateway_password>' -m 'linux'
```

curl

> **Note**
>
> Você precisa ter o curl instalado.

Para obter as credenciais usando curl

1. Execute o comando a seguir a partir do terminal substituindo <gateway_username> e <gateway_password> pelas credenciais que você criou.

```
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"
}'
```

   A resposta deve ser parecida com o seguinte:

```
{
    "username": "sweuser",
    "accessKeyId": "<accessKeyId>",
    "secretAccessKey": "<secretAccessKey>",
    "sessionToken": "<sessionToken>",
    "sessionExpiryTime": "2022-11-17T04:51:40.927095Z",
    "authMechanism": "linux",
    "role": "edge-user"
}
```

2. Execute o seguinte comando no seu terminal.

```
export AWS_ACCESS_KEY_ID=<accessKeyId>
export AWS_SECRET_ACCESS_KEY=<secretAccessKey>
export AWS_SESSION_TOKEN=<sessionToken>
export AWS_REGION=edge
```

Etapa 4: Obtenha uma lista dos modelos de ativos no gateway SiteWise Edge

Agora que você tem um certificado assinado, o nome de host do gateway SiteWise Edge e credenciais temporárias do gateway SiteWise Edge, você pode usar a `ListAssetModels` API para obter uma lista dos modelos de ativos no gateway SiteWise Edge.

Python

> **Note**
>
> Você precisa do Python3, do Boto3 e instalado. BotoCore

Para obter a lista de modelos de ativo usando Python

1. Crie um arquivo chamado list_asset_model.py e copie o código a seguir nele.

```
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. Execute o list_asset_model.py a partir do terminal.

```
python3 list_asset_model.py
```

curl

> **Note**
>
> Você precisa ter o curl instalado.

Para obter a lista de modelos de ativo usando curl

Execute o comando a seguir no 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"
```

A resposta deve ser parecida com o seguinte:

```
{
    "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
}
```

Faça backup e restaure gateways SiteWise Edge

Este tópico aborda como restaurar gateways do SiteWise Edge e fazer backup de seus dados métricos. Se você estiver enfrentando problemas com um gateway SiteWise Edge quebrado na mesma máquina e precisar solucionar o problema, leia a AWS IoT SiteWise documentação Solução de problemas do gateway SiteWise Edge.

> **Note**
>
> A orientação abordada neste tópico é para gateways SiteWise Edge instalados na AWS IoT Greengrass V2 versão 2.1.0 ou superior.

Backups diários de dados métricos

Criar um backup é importante caso queira transferir ou restaurar os dados em uma nova máquina. O backup de seus dados reduz consideravelmente o risco de perda de dados operacionais durante um processo de transferência ou restauração.

O caminho da pasta influxdb é o seguinte:

Linux

```
/greengrass/v2/work/aws.iot.SiteWiseEdgeProcessor/influxdb
```

Windows

```
C:\greengrass\v2\work\aws.iot.SiteWiseEdgeProcessor\influxdb
```

Recomendamos que você faça backup de toda a pasta com tudo que tiver nela.

Recomendamos que você faça backup periódico de seus dados métricos do 1.0 SiteWise Edge para um disco rígido externo ou para a AWS nuvem.

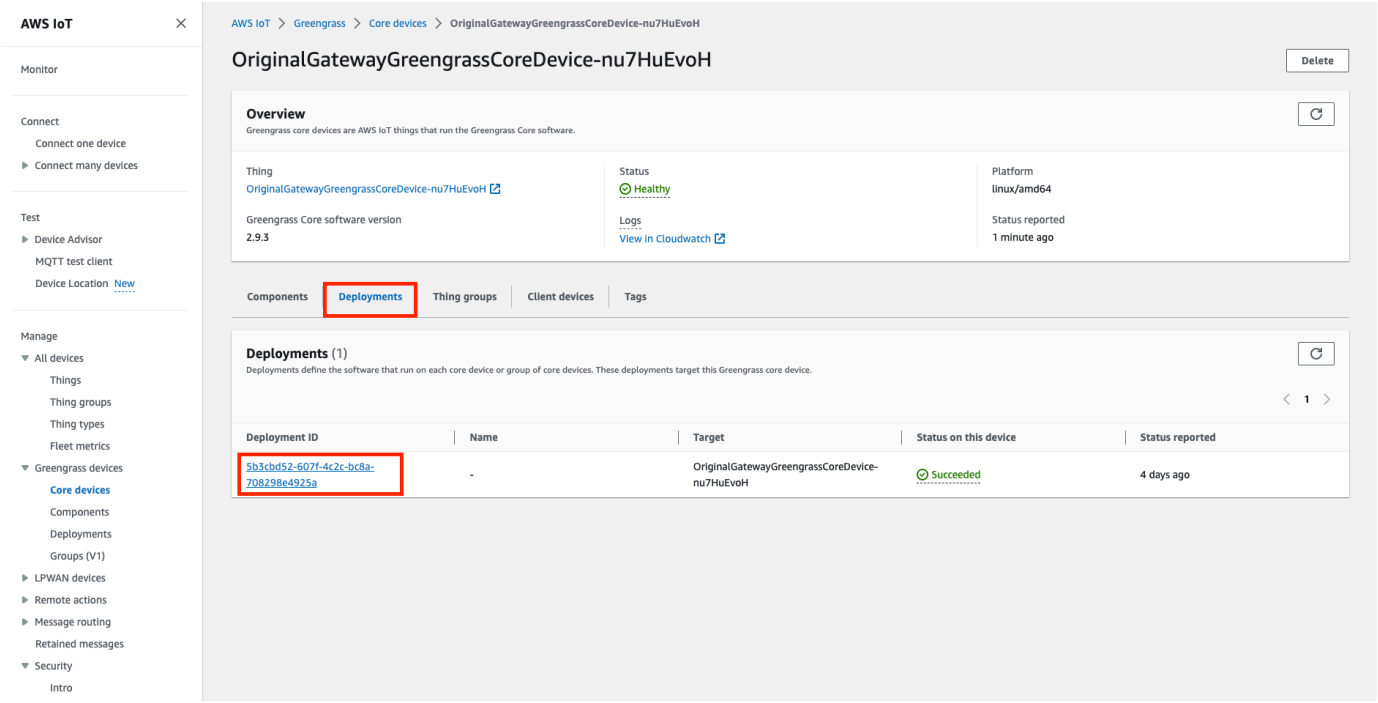
Restaurar um gateway SiteWise Edge

Use o procedimento a seguir para restaurar um gateway SiteWise Edge:

1. Use o script de instalação baixado ao criar o SiteWise Edge Gateway para restaurar o SiteWise Edge Gateway na nova máquina. Leia o procedimento Instalando o software SiteWise Edge Gateway em seu dispositivo local para configurar o SiteWise Edge Gateway.

   Se você perder ou não conseguir encontrar o script de instalação, entre em contato com o Suporte ao Cliente da AWS.
2. Depois que o gateway SiteWise Edge for instalado, faça login no AWS IoT Greengrass console.
3. Para reimplantar os componentes, navegue até Gerenciar e em dispositivos do AWS IoT Greengrass selecione dispositivos de núcleo.

4. Na tabela de dispositivos AWS IoT Greengrass principais, selecione o dispositivo principal correspondente ao seu gateway SiteWise Edge.
5. Ao acessar a página do dispositivo, abra a guia Implantações e selecione sua ID de implantação. Isso abrirá a página Implantações com a ID selecionada.



6. Assim que estiver na página Implantações, no canto superior direito, pressione o botão Ações e selecione a opção Revisar para iniciar uma nova implantação. Configure a implantação. Se você quiser manter a implantação como está, vá para Revisar e Implantar.
7. Aguarde até que o Status de implantação se torne `Completed`.

> **Note**
>
> Também serão necessários alguns minutos para que todos os componentes do SiteWise Edge sejam totalmente configurados e executados.

Restaurar AWS IoT SiteWise dados

Use o procedimento a seguir para restaurar dados em uma nova máquina.

1. Copie a pasta `influxdb` na nova máquina.
2. Pare o SiteWise EdgeProcessor componente executando o seguinte comando em seu 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. Localize o caminho onde você fez o backup de seus dados e execute o comando a seguir:

   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 o SiteWiseEdgeProcessor componente:

   Linux

   ```
   sudo /greengrass/v2/bin/greengrass-cli component restart -n
   aws.iot.SiteWiseEdgeProcessor
   ```

   Windows

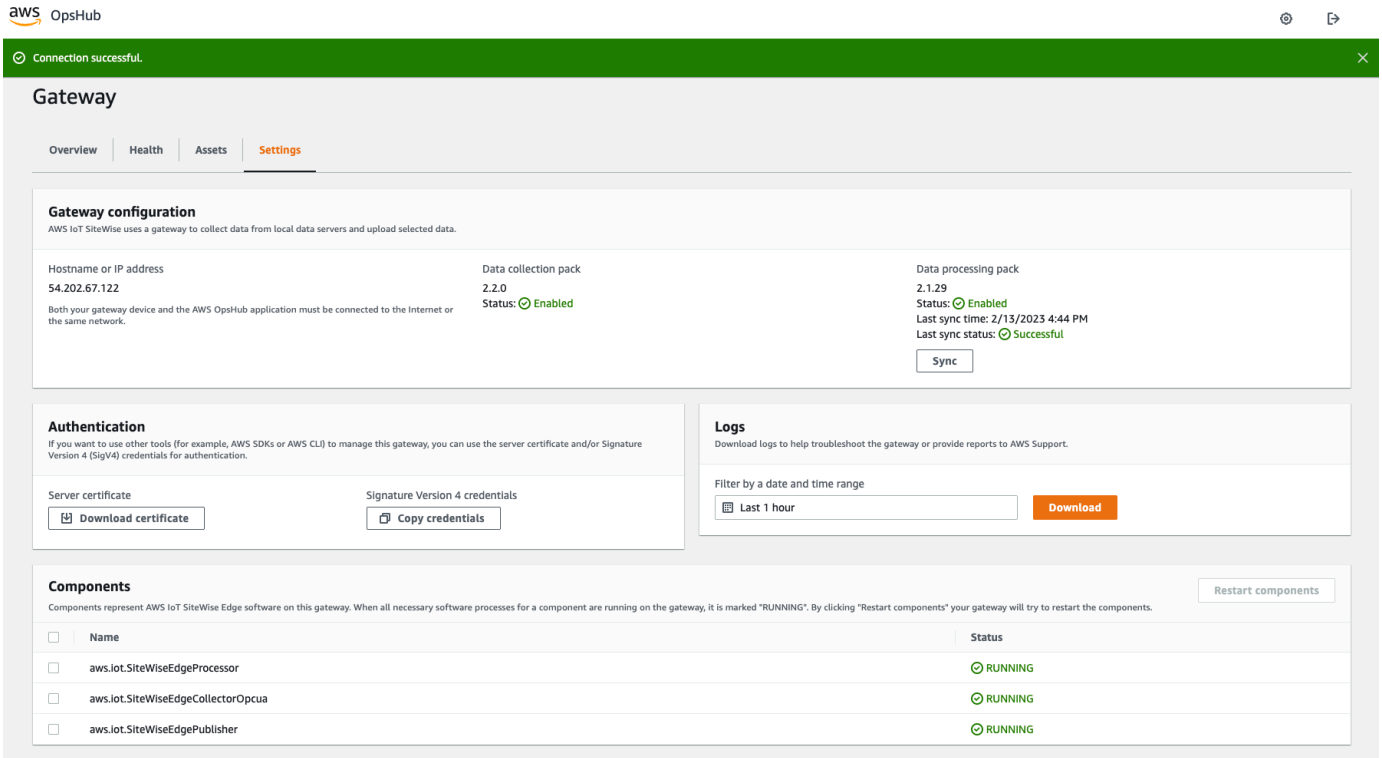
   ```
   C:\greengrass\v2\bin\greengrass-cli component restart -n
   aws.iot.SiteWiseEdgeProcessor
   ```

Valide backups e restaurações bem-sucedidos

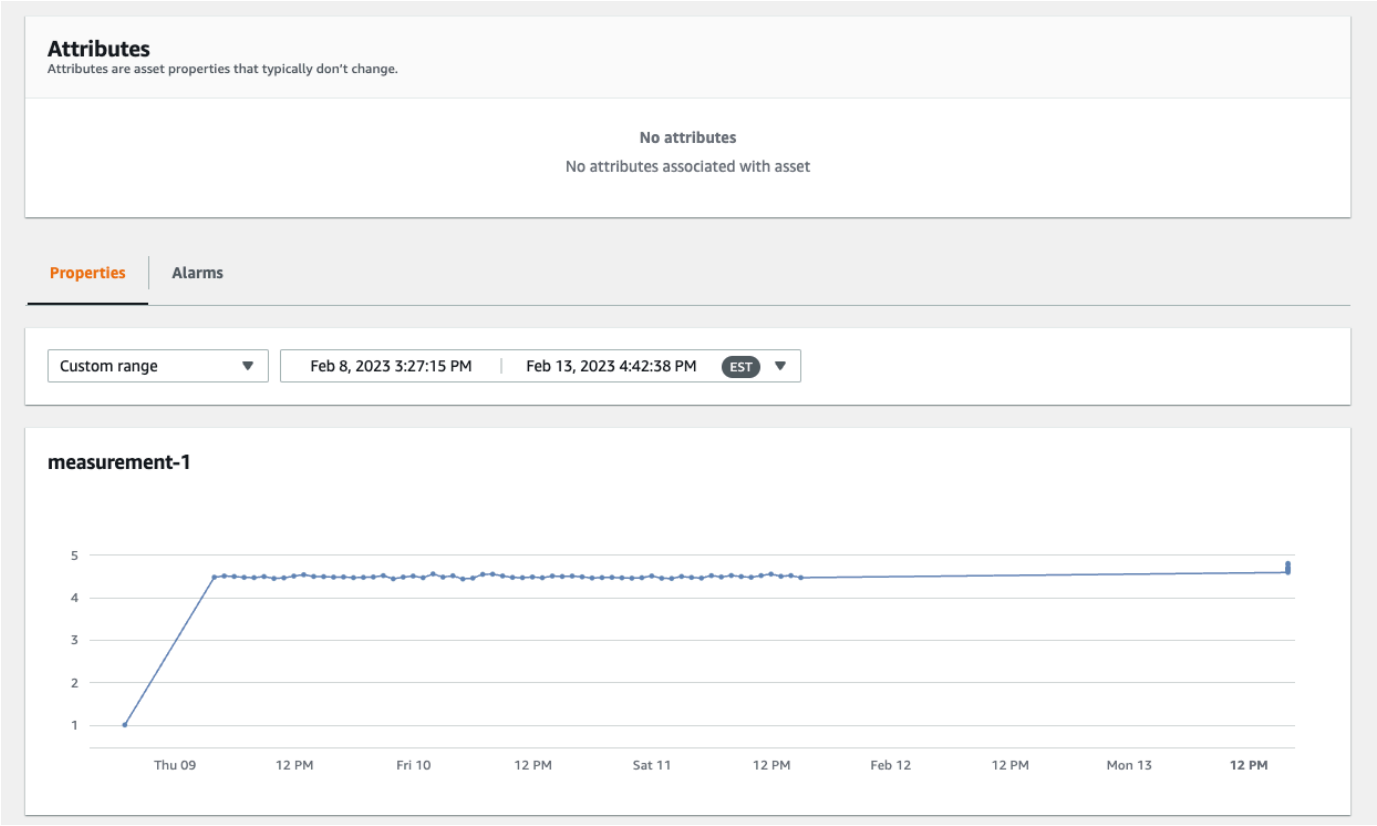
Use esse procedimento para validar seus dados de backup e as restaurações do SiteWise Edge Gateway.

> **Note**
>
> Este procedimento requer que você tenha instalado AWS OpsHub para AWS IoT SiteWise. Para obter mais informações, consulte Gerenciando gateways SiteWise Edge usando AWS OpsHub for AWS IoT SiteWise.

1. Aberto AWS OpsHub para AWS IoT SiteWise.
2. Na página Configurações do SiteWise Edge Gateway, verifique o status de cada componente listado na tabela Componentes. Verifique se a cor do status é verde e se a leitura exibe EM EXECUÇÃO.



3. Valide seus dados anteriores no painel do portal para verificar se os dados antigos e os dados novos estão configurados corretamente. Haverá um tempo de inatividade entre dados antigos e novos. É esperado que, por um período, não haja pontos de dados coletados.



Se você tiver problemas com o backup ou a restauração de um gateway SiteWise Edge, consulte os seguintes tópicos de solução de problemas: Solução de problemas de um gateway AWS IoT SiteWise Edge.

Configurando gateways SiteWise Edge ()AWS IoT Greengrass Version 1

> **Note**
>
> SiteWise Os gateways Edge em execução AWS IoT Greengrass V1 estão disponíveis somente se você começou a usar esse recurso antes de 29 de julho de 2021. Caso contrário, você configura os gateways do SiteWise Edge em execução em. AWS IoT Greengrass V2

Você pode enviar dados industriais para AWS IoT SiteWise usar um gateway SiteWise Edge para carregar dados de equipamentos industriais. O gateway SiteWise Edge serve como intermediário entre AWS IoT SiteWise e seu equipamento industrial de dados. AWS IoT SiteWise fornece AWS

IoT Greengrass componentes que você pode implantar em qualquer dispositivo que possa ser executado AWS IoT Greengrass para configurar um gateway SiteWise Edge. AWS IoT SiteWise suporta vinculação com o protocolo de servidor OPC-UA.

Se você tiver gateways AWS IoT SiteWise Edge que funcionam AWS IoT Greengrass V1, você pode atualizar seus gateways SiteWise Edge para. AWS IoT Greengrass V2 Para obter mais informações, consulte Instruções para atualizar os gateways SiteWise Edge de AWS IoT Greengrass V1 para. AWS IoT Greengrass V2

Tópicos

- Escolhendo um dispositivo de gateway AWS IoT Greengrass V1 SiteWise Edge
- Configurando um gateway AWS IoT Greengrass V1 SiteWise Edge
- Configurando fontes de dados em gateways AWS IoT Greengrass V1 SiteWise Edge

Escolhendo um dispositivo de gateway AWS IoT Greengrass V1 SiteWise Edge

Escolha um dispositivo local que melhor se adapte à sua operação industrial. Você pode configurar um gateway SiteWise Edge em qualquer dispositivo que possa ser executado AWS IoT Greengrass. Todos os dispositivos locais devem atender aos seguintes requisitos:

- Compatível com o software AWS IoT Greengrass Core v1.10.2 ou posterior. Para obter mais informações, consulte Plataformas com suporte e requisitos no Guia do desenvolvedor do AWS IoT Greengrass Version 1 .
- Tem pelo menos 4 GB de RAM.
- Ter pelo menos 10 GB de espaço livre em disco.
- Oferecer suporte a uma máquina virtual Java 8 (JVM).

Se você planeja processar dados na borda com AWS IoT SiteWise, seu dispositivo local também deve atender aos seguintes requisitos:

- Tem um processador quad-core x86 de 64 bits.
- Ter pelo menos 16 GB de RAM.
- Tem pelo menos 32 GB de RAM se estiver usando o Windows.
- Ter pelo menos 256 GB de espaço livre em disco.

O espaço em disco necessário para armazenar dados em cache para conectividade com a Internet intermitente depende dos seguintes fatores:

- Número de fluxos de dados carregados
- Pontos de dados por fluxo de dados por segundo
- Tamanho de cada ponto de dados
- Velocidades de comunicação
- O tempo de inatividade de rede esperado

A capacidade computacional necessária para sondar e carregar dados depende dos seguintes fatores:

- Número de fluxos de dados carregados
- Pontos de dados por fluxo de dados por segundo

Configurando um gateway AWS IoT Greengrass V1 SiteWise Edge

Um gateway AWS IoT SiteWise Edge serve como intermediário entre seu equipamento industrial e. AWS IoT SiteWise Você pode implantar o software SiteWise Edge Gateway em qualquer dispositivo que possa ser executado AWS IoT Greengrass. Para ter mais informações, consulte Escolhendo um dispositivo de gateway AWS IoT Greengrass V1 SiteWise Edge.

Você pode AWS IoT SiteWise habilitar o processamento de dados localmente em seus dispositivos de borda usando o pacote de processamento de dados em seu gateway SiteWise Edge. Você faz isso ao adicionar seu gateway SiteWise Edge AWS IoT SiteWise a. Para obter mais informações sobre o processamento de dados na borda, consulte the section called “Habilitar o processamento de dados de borda”.

> **Note**
>
> Recomendamos que execute as seguintes etapas com uma conta que tenha acesso administrativo de TI às suas redes corporativa e local. Essas etapas podem exigir que alguém com conhecimento de seu equipamento industrial e autoridade defina as configurações do firewall.

Tópicos

- Configurando o ambiente do SiteWise Edge Gateway
- Criar um perfil e política do IAM
- Configurando um grupo AWS IoT Greengrass
- Configurando o conector AWS IoT SiteWise
- Adicionando o gateway SiteWise Edge ao AWS IoT SiteWise

Configurando o ambiente do SiteWise Edge Gateway

Neste procedimento, você instala AWS IoT Greengrass e configura seu gateway SiteWise Edge para uso com AWS IoT SiteWise.

> **Note**
>
> Esta seção inclui instruções para instalar pacotes usando o comando `apt`. Isso é aplicável a sistemas que executam o Ubuntu ou similar. Se você não estiver usando um sistema semelhante, consulte a documentação para sua distribuição e use o instalador de pacotes recomendado.

Para configurar o gateway SiteWise Edge

1. Conforme apropriado, modifique as configurações do BIOS do gateway SiteWise Edge da seguinte forma.
   a. Certifique-se de que o gateway SiteWise Edge seja reiniciado automaticamente após uma possível falha de energia, se aplicável.
   b. Certifique-se de que o gateway SiteWise Edge não hiberne nem hiberne, se aplicável.
2. Certifique-se de que o gateway SiteWise Edge se conecte à Internet.
3. (Opcional) Para usar o gateway SiteWise Edge sem o mouse, o teclado e o monitor, siga as etapas a seguir para configurar `ssh` o gateway SiteWise Edge:
   a. Se você ainda não tiver instalado o pacote SSH, execute o comando a seguir.

      ```
      sudo apt install ssh
      ```

   b. Execute o seguinte comando .

```
service ssh status
```

c. Procure `Active: active (running)` na saída para confirmar que o servidor SSH está em execução.

d. Pressione Q para sair.

Execute o comando a seguir para usar o SSH para se conectar ao gateway SiteWise Edge de outro computador. *`Substitua o nome de usuário pelo login do usuário e o IP pelo endereço IP do gateway SiteWise Edge.`*

```
ssh username@IP
```

É possível usar o argumento `-p port-number` para se conectar a uma porta diferente da porta padrão 22.

4. Baixe e instale o software AWS IoT Greengrass Core v1.10.2 ou posterior e crie um AWS IoT Greengrass grupo para seu SiteWise gateway Edge. Para fazer isso, siga as instruções em Conceitos básicos do AWS IoT Greengrass no Guia do desenvolvedor do AWS IoT Greengrass .

   Recomendamos que você execute o script de configuração do dispositivo do AWS IoT Greengrass para começar rapidamente. Se você quiser analisar AWS IoT Greengrass os requisitos e os processos mais de perto, siga as etapas do Módulo 1 e do Módulo 2 para configurar AWS IoT Greengrass.

   > **Important**
   >
   > Analise as AWS regiões em AWS IoT SiteWise que há suporte. Ao escolher uma região para AWS IoT Greengrass, certifique-se de que a região também ofereça suporte AWS IoT SiteWise. Caso contrário, você não poderá conectar seu gateway SiteWise Edge AWS IoT SiteWise a.

   Antes de continuar com a próxima etapa, você deve ter o software AWS IoT Greengrass Core instalado em seu gateway SiteWise Edge.

5. Execute os comandos a seguir para instalar o Java 8.

```
sudo apt update
```

```
      sudo apt install openjdk-8-jre
```

O software de gateway SiteWise Edge que você instalará posteriormente neste guia usa um tempo de execução do Java 8.

6. Execute os comandos a seguir para verificar se a instalação desse Java foi bem-sucedida.

```
java -version
```

7. O software AWS IoT Greengrass Core assume um `java8` diretório. Execute o comando a seguir para vincular sua instalação Java a esse diretório `java8`.

```
sudo ln -s /usr/bin/java /usr/bin/java8
```

8. Execute o comando a seguir para criar um diretório de `/var/sitewise` dados e conceder as `ggc_user` permissões para esse diretório. AWS IoT SiteWise armazena dados nesse diretório. Você criou o `ggc_user` quando configurou AWS IoT Greengrass anteriormente neste procedimento.

```
sudo mkdir /var/sitewise
      sudo chown ggc_user /var/sitewise
      sudo chmod 700 /var/sitewise
```

O `/var/sitewise` é o diretório padrão que AWS IoT SiteWise usa. Você pode personalizar o caminho do diretório (por exemplo, `/var/sitewise` substituir por`/var/`*`custom`*`/`*`path`*`/`), mas isso requer etapas adicionais após a criação do gateway SiteWise Edge. Para obter mais informações, consulte a etapa 6 em Configurando o conector AWS IoT SiteWise.

9. Se necessário, peça ao administrador de TI para adicionar os seguintes endpoints e portas à lista de permissões de rede local:

   - Portas: 443, 8443 e 8883

> **Important**
>
> Você pode configurar o AWS IoT Greengrass Core para usar somente a porta 443 para todas as comunicações de rede. Para obter mais informações, consulte Conectar-se à porta 443 ou por meio de um proxy de rede no Guia do desenvolvedor do AWS IoT Greengrass .

- O endereço IP do seu gateway SiteWise Edge (porta 443). Para obter o endereço IP, execute o comando `ip address` ou `ifconfig` e anote o valor de `inet` (por exemplo, `203.0.113.0`).
- O endpoint de AWS IoT SiteWise dados: `data.iotsitewise.`*`region`*`.amazonaws.com` (porta 443).
- Os seguintes AWS endpoints que o gateway SiteWise Edge usa. É possível encontrá-los no arquivo */*`greengrass-root`*`/config/config.json`. Substitua o *`greengrass-root`* pela raiz da instalação do AWS IoT Greengrass .
  - ggHost: `greengrass-ats.iot.`*`region`*`.amazonaws.com` (portas 443, 8443 e 8883).
  - iotHost: *`prefix`*`-ats.iot.`*`region`*`.amazonaws.com` (portas 443, 8443 e 8883).

  Para obter mais informações, consulte AWS IoT Greengrass Endpoints e cotas.

10. Se o software AWS IoT Greengrass principal ainda não estiver em execução, execute o comando a seguir para iniciar o software AWS IoT Greengrass principal. Substitua *`greengrass-root pela raiz`* da sua instalação. AWS IoT Greengrass O padrão *`greengrass-root`* é `/greengrass`.

    ```
    cd /greengrass-root/ggc/core
          sudo ./greengrassd start
    ```

    Você deverá ver esta mensagem: `Greengrass successfully started with PID:` *`some-PID-number`*

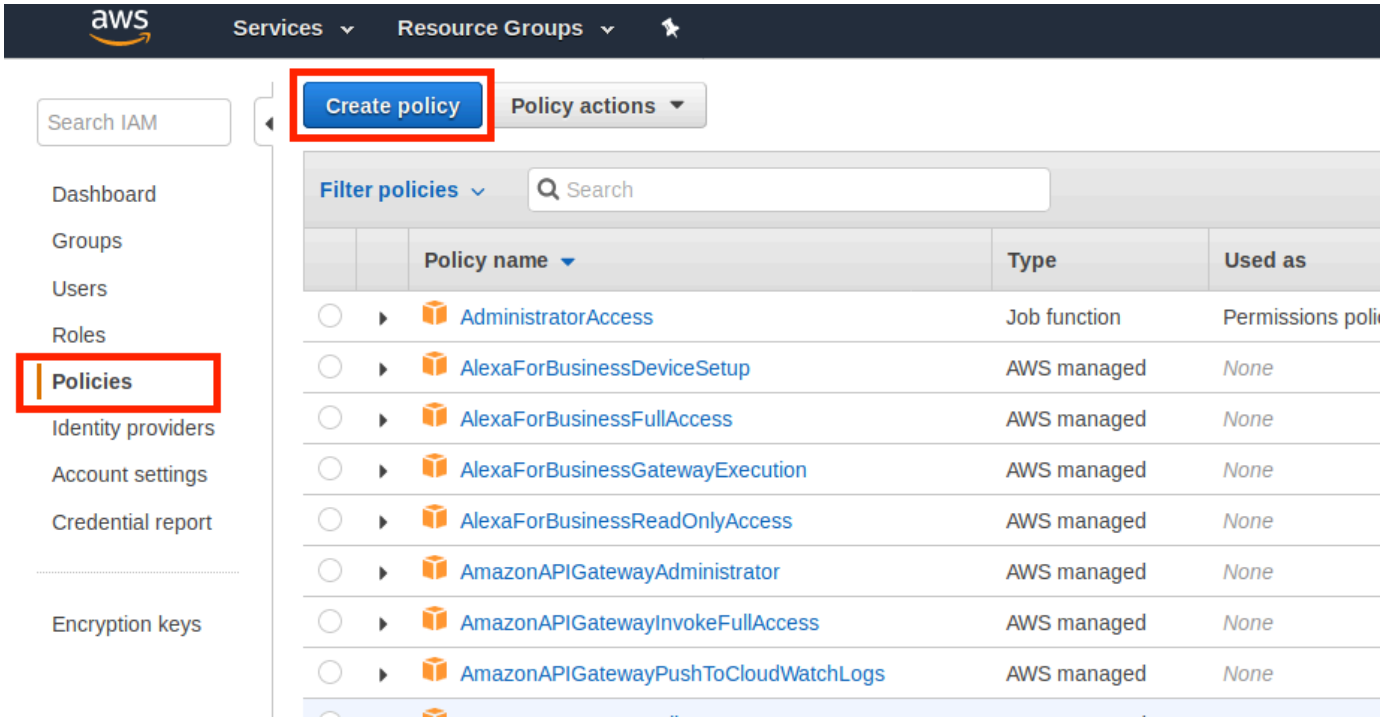
11. Configure o software AWS IoT Greengrass Core para iniciar automaticamente quando o gateway SiteWise Edge for ligado. Consulte a documentação do sistema operacional do seu gateway SiteWise Edge.

Criar um perfil e política do IAM

Você deve criar uma política e uma função AWS Identity and Access Management (IAM) para permitir que o SiteWise Edge Gateway acesse AWS IoT SiteWise em seu nome.

Criar um perfil e política do IAM

1. Navegue até o console do IAM.
2. No painel de navegação, selecione Políticas e, em seguida, Criar política.



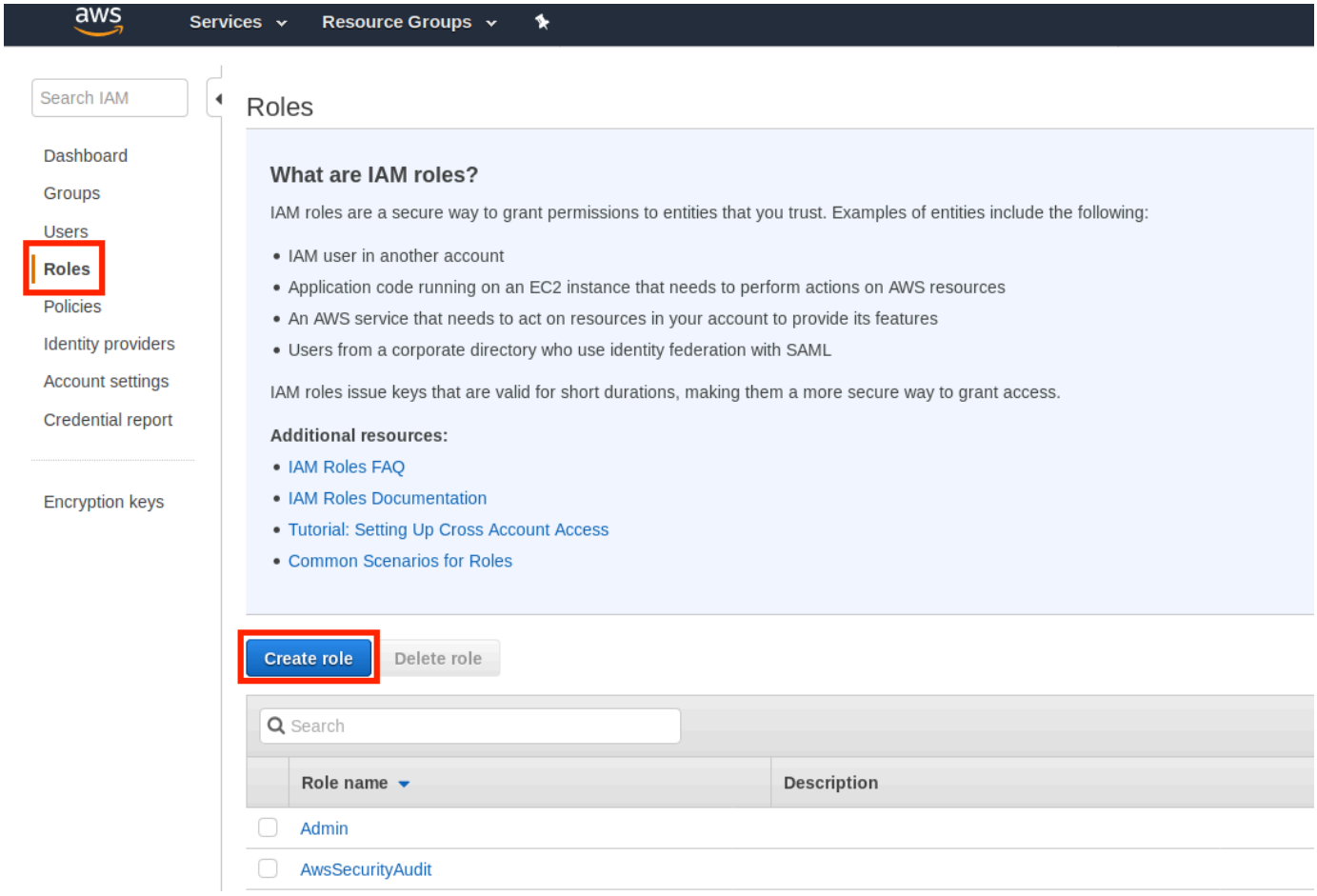
3. Na guia JSON, exclua o conteúdo atual do campo da política e cole nele a política a seguir.

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

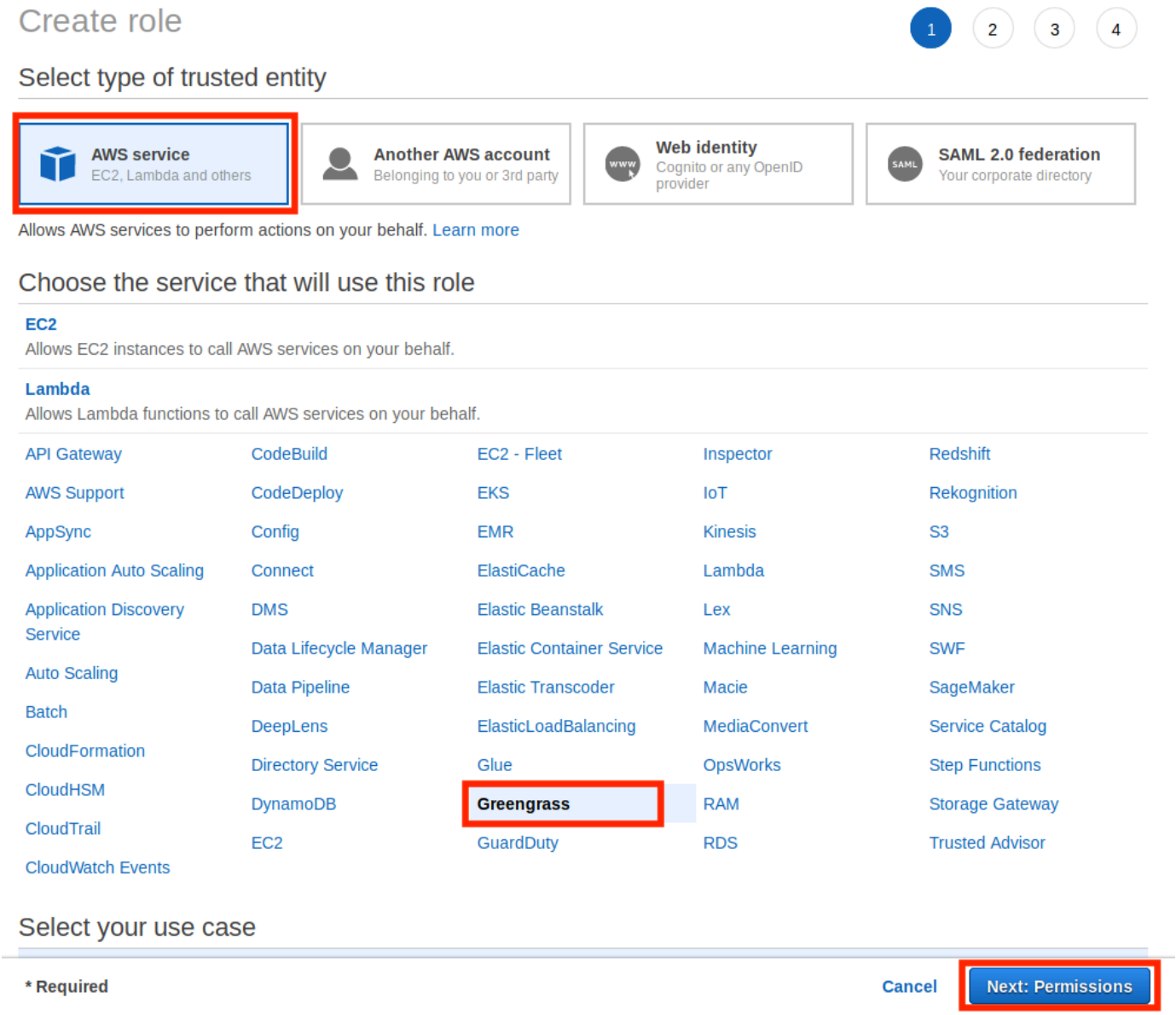
> **Note**
>
> Para melhorar a segurança, você pode especificar um caminho AWS IoT SiteWise de hierarquia de ativos na `Condition` propriedade. O exemplo a seguir é uma política de confiança que especifica um caminho de hierarquia de ativos.
>
> ```
> {
>         "Version": "2012-10-17",
>         "Statement": [
>           {
> ```

```
            "Effect": "Allow",
            "Action": "iotsitewise:BatchPutAssetPropertyValue",
            "Resource": "*",
            "Condition": {
              "StringLike": {
                "iotsitewise:assetHierarchyPath": [
                  "/root node asset ID",
                  "/root node asset ID/*"
                ]
              }
            }
          }
        ]
      }
```

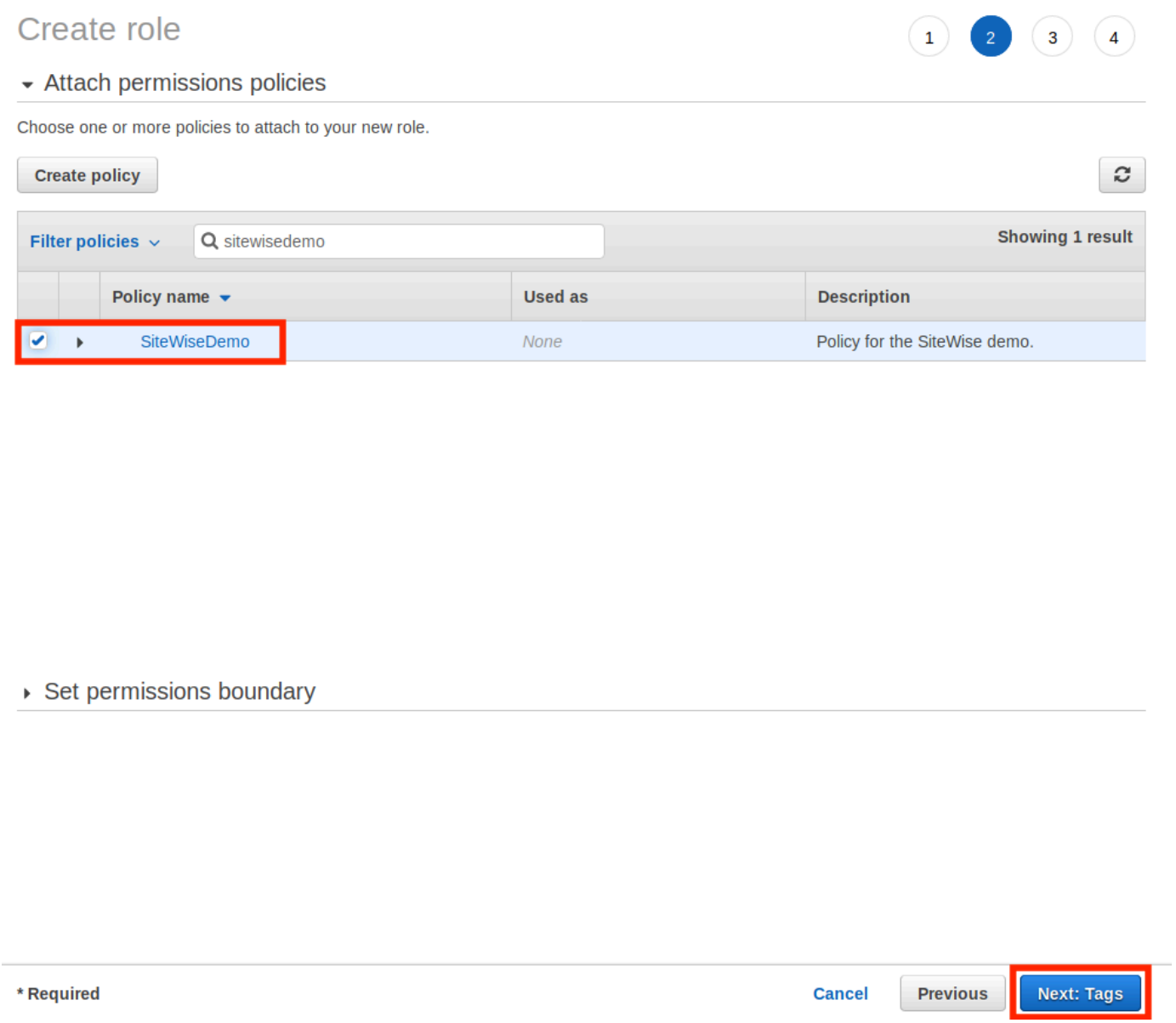
4. Escolha Revisar política.
5. Insira um nome e uma descrição para a política e escolha Create policy (Criar política).
6. No painel de navegação, escolha Perfis e Criar perfil.



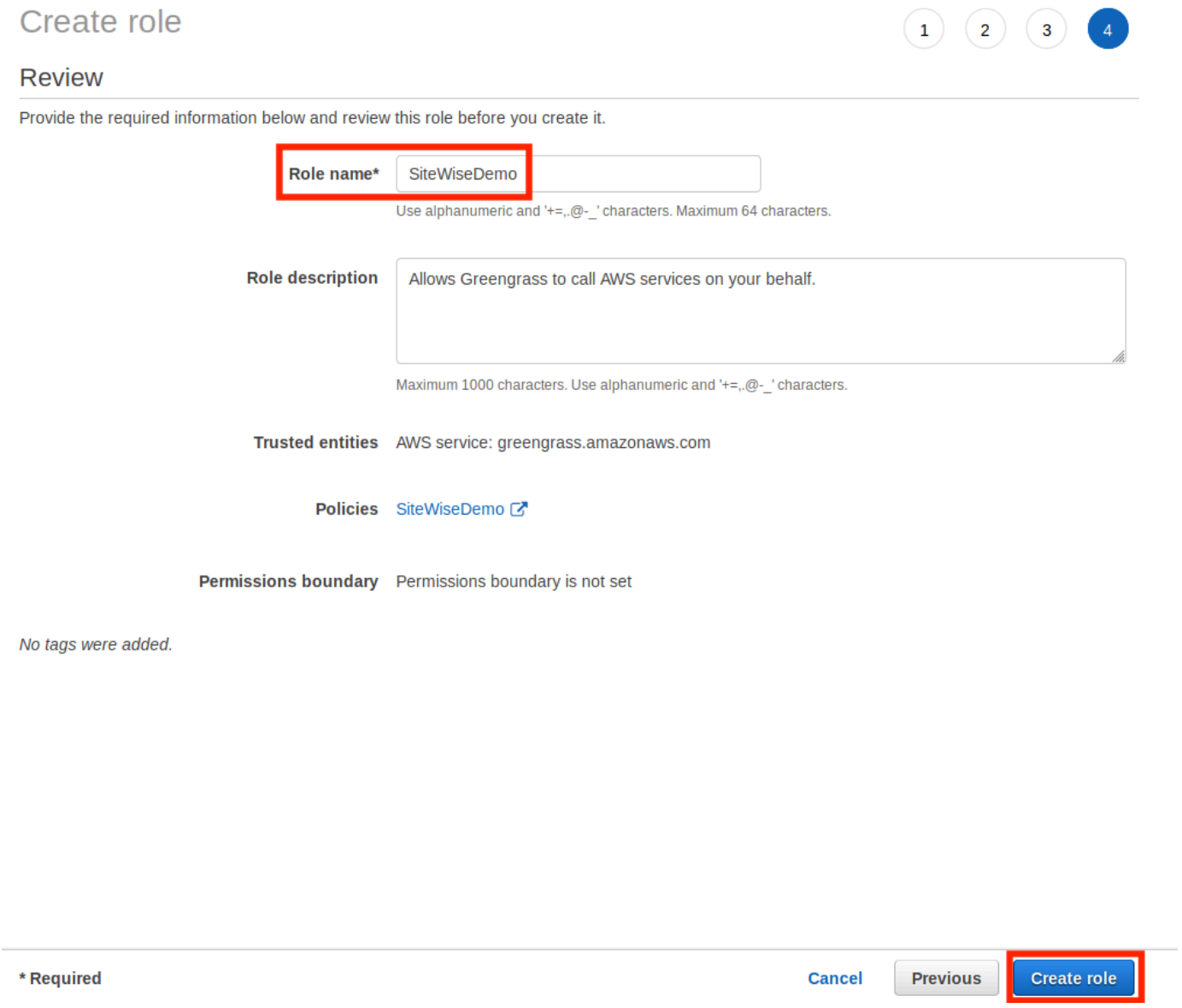
7. Em Select type of trusted entity (Selecionar o tipo de entidade confiável), escolha AWS service (serviço). Em Choose the service that will use the role (Selecionar o serviço que usará a função), selecione Greengrass como o serviço que usará a função e Next: Permissions (Próximo: Permissões).



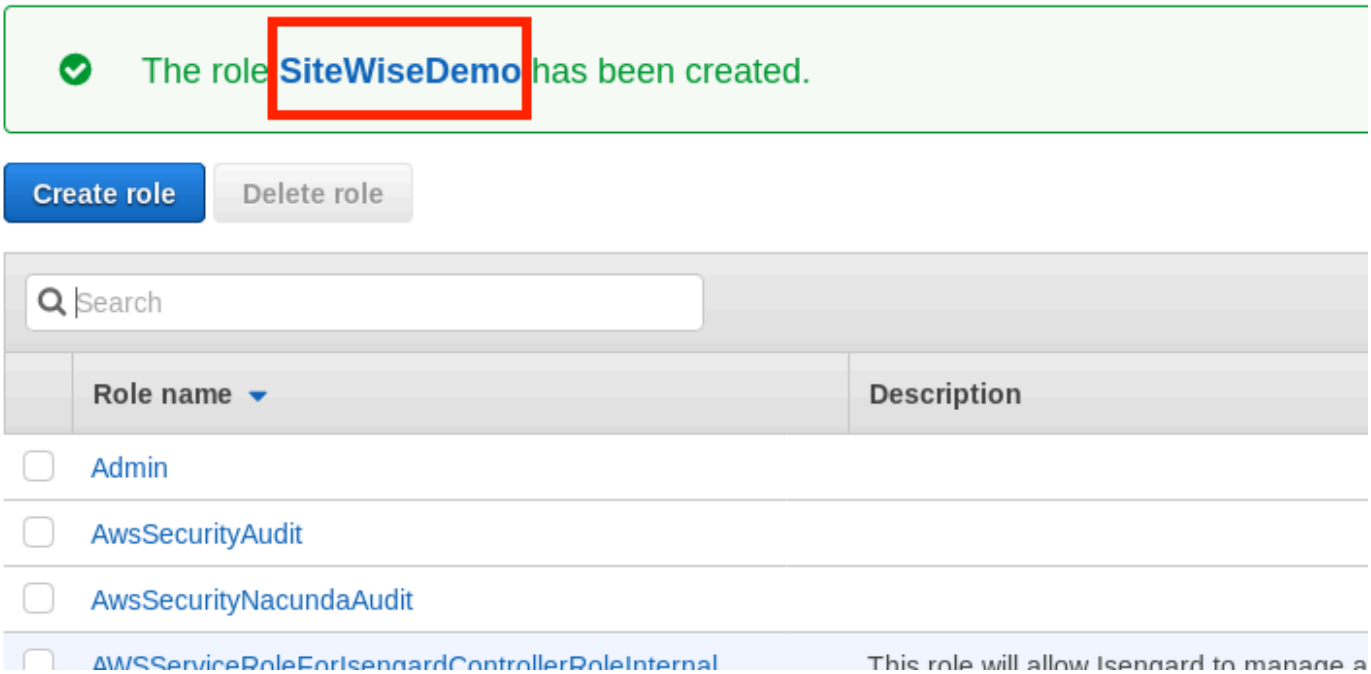
8. Pesquise a política que você criou, marque a caixa de seleção e, em seguida, escolha Próximo: tags.



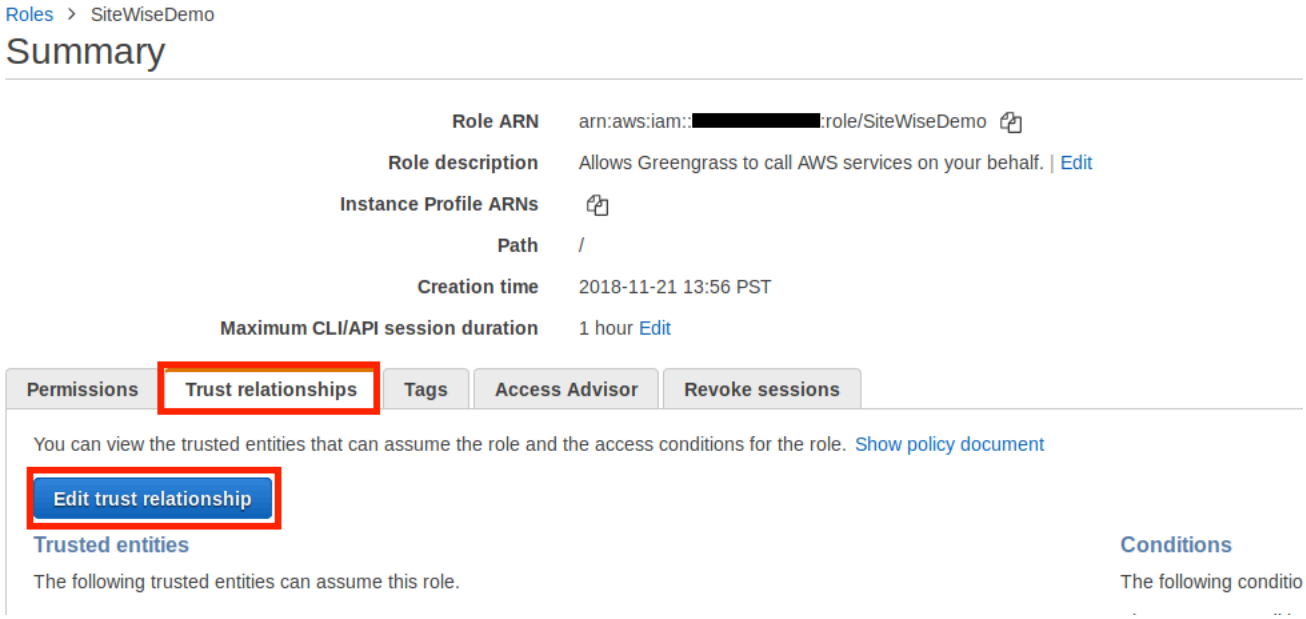
9. (Opcional) Adicione tags à sua função e escolha Next: Review (Próximo: Revisar).
10. Digite um nome e uma descrição para a função e, depois, escolha Create role (Criar função).



11. No banner verde, escolha o link para sua nova função. Você também pode usar o campo de pesquisa para encontrar a função.



12. Escolha a guia Relacionamentos de confiança e, em seguida, selecione Editar relacionamento de confiança.



13. Substitua o conteúdo atual do campo de política pelo seguinte e escolha Update Trust Policy (Atualizar política de confiança).

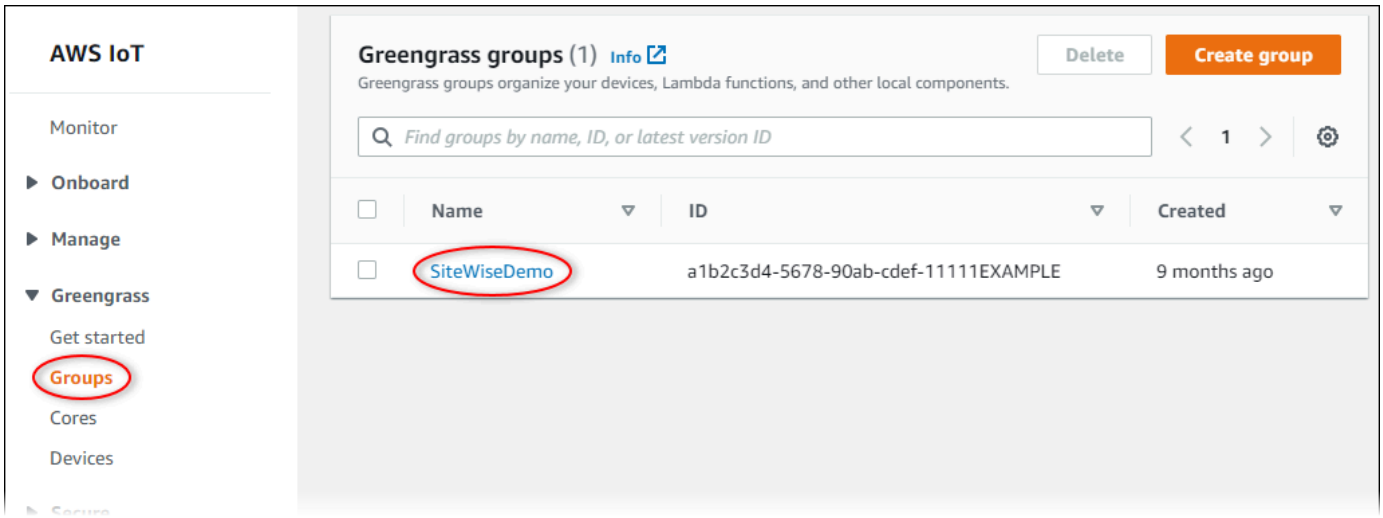
```
{
        "Version": "2012-10-17",
        "Statement": [
```

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

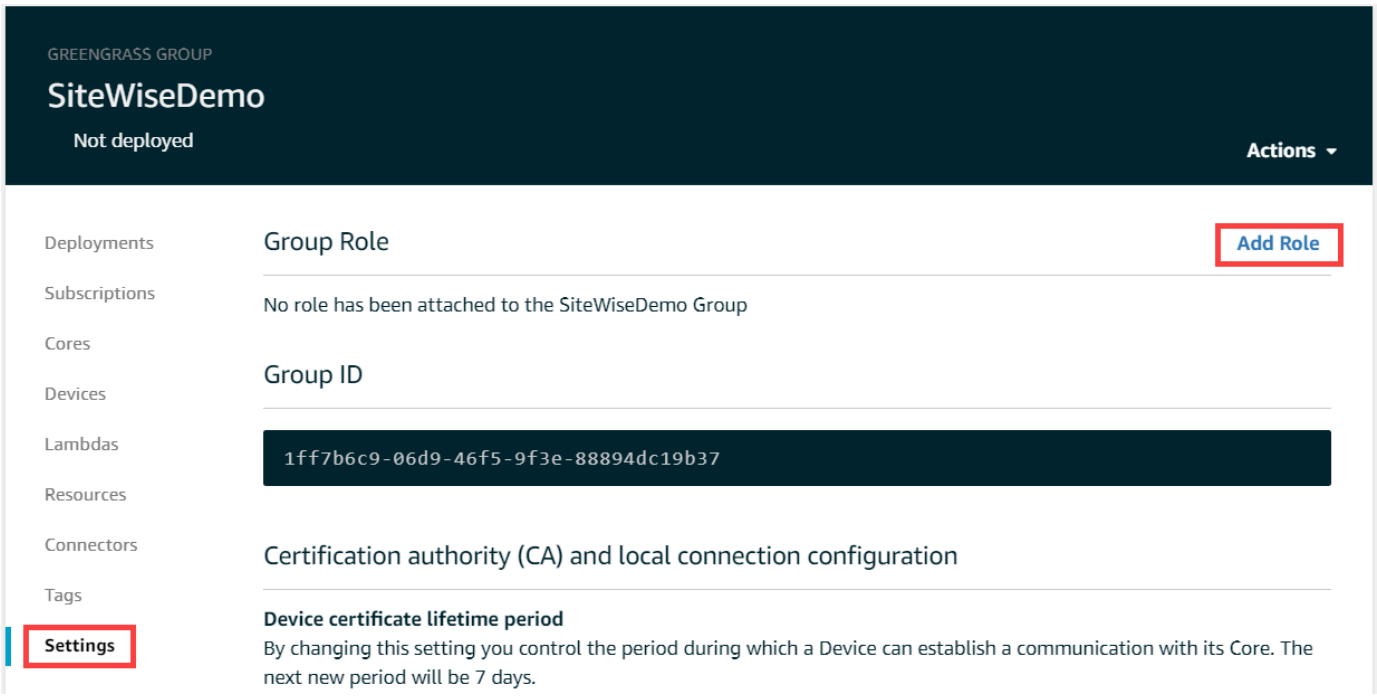
Configurando um grupo AWS IoT Greengrass

Como anexar um perfil do IAM a um grupo e habilitar o gerenciador de fluxo

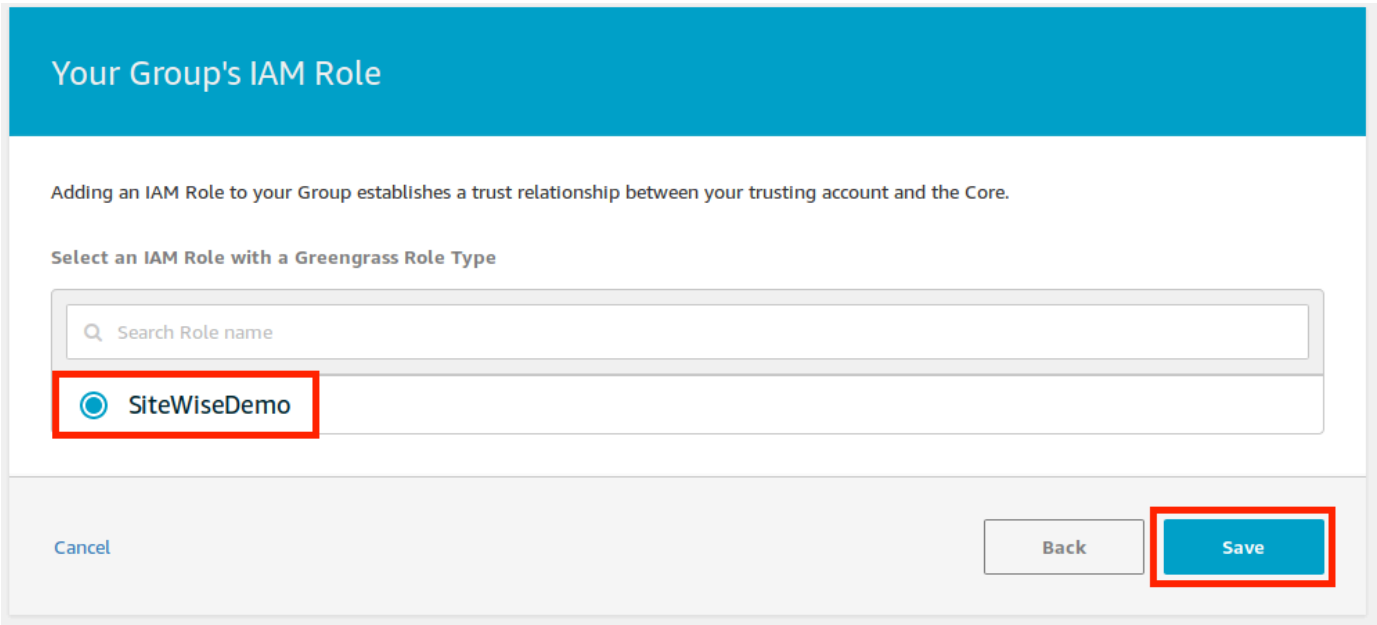
1. Navegue até o console do AWS IoT Greengrass.
2. No painel de navegação à esquerda, em Greengrass, selecione Groups (Grupos) e o grupo que você criou em Configurando o ambiente do SiteWise Edge Gateway.



3. No painel de navegação à esquerda, escolha Configurações. Na seção Group Role (Função do grupo) escolha Add Role (Adicionar função).

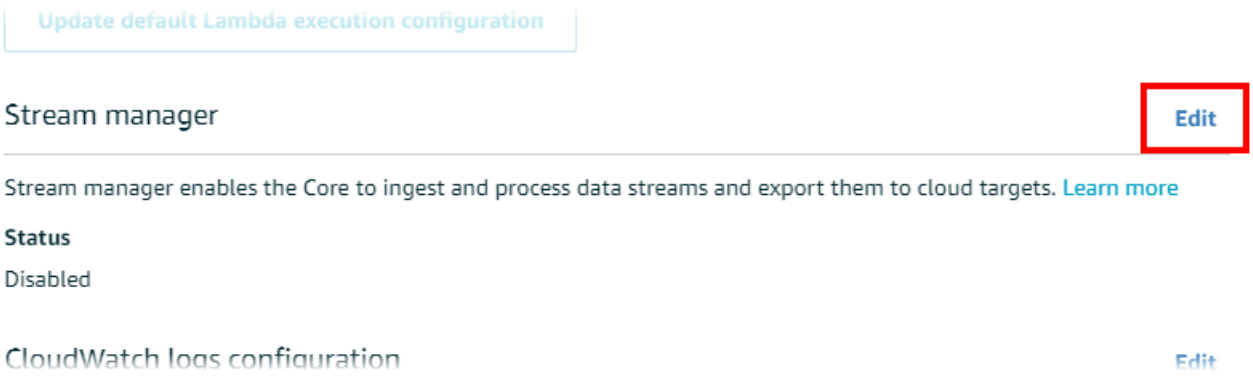


4. Escolha a função criada em Criar um perfil e política do IAM e selecione Save (Salvar).



5. Na página Settings (Configurações), na seção Stream manager (Gerenciador de streaming), escolha Edit (Editar).

   O gerenciador de fluxo é um recurso AWS IoT Greengrass que permite que seu AWS IoT Greengrass Core transmita dados para a AWS nuvem. SiteWise Os gateways Edge exigem que o gerenciador de fluxo esteja ativado. Para obter mais informações, consulte Gerenciar fluxos de dados no AWS IoT Greengrass Core no Guia do AWS IoT Greengrass Version 1 desenvolvedor.



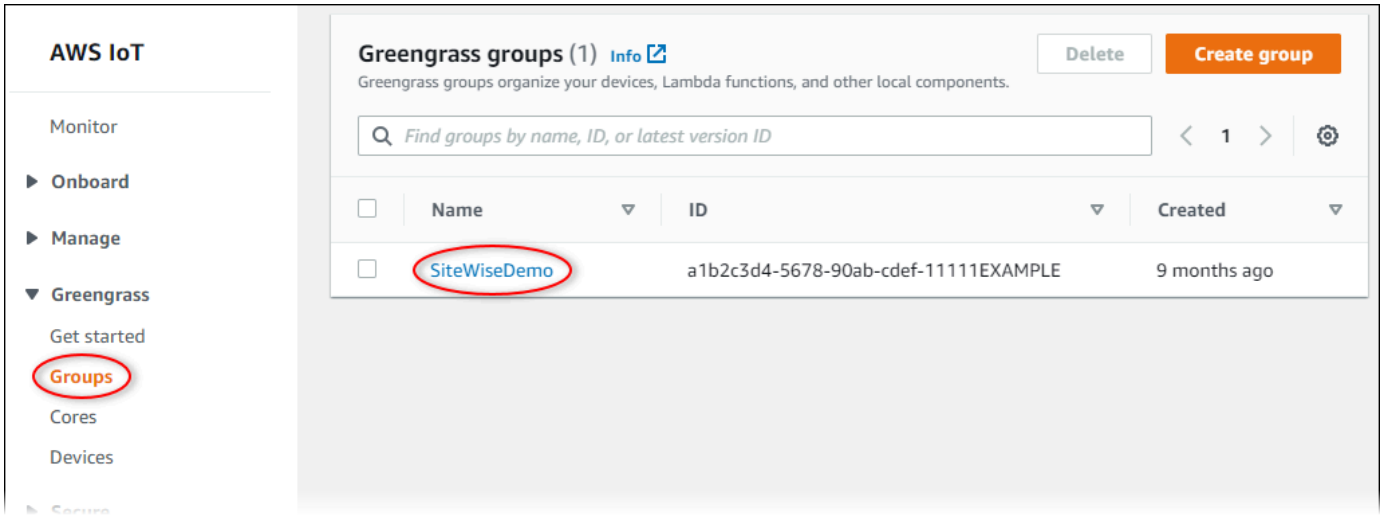
6. Selecione Enable (Habilitar) e Save (Salvar).
7. No canto superior esquerdo, escolha Services (Serviços) para se preparar para a próxima etapa.

Configurando o conector AWS IoT SiteWise

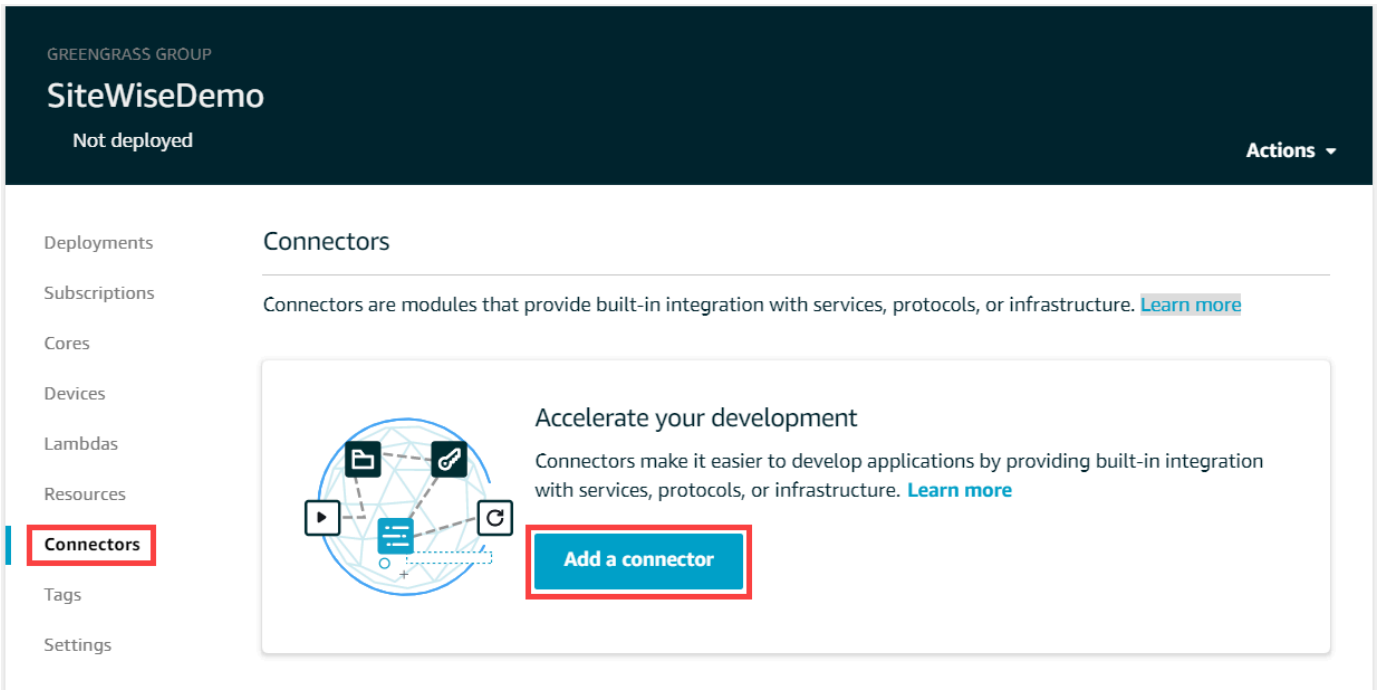
Neste procedimento, você configura o AWS IoT SiteWise conector em seu grupo do Greengrass. Os componentes são módulos pré-construídos que aceleram o ciclo de vida de desenvolvimento para cenários de ponta comuns. Para obter mais informações, consulte Conectores do AWS IoT Greengrass no Guia do desenvolvedor do AWS IoT Greengrass Version 1 .

Para configurar o AWS IoT SiteWise conector

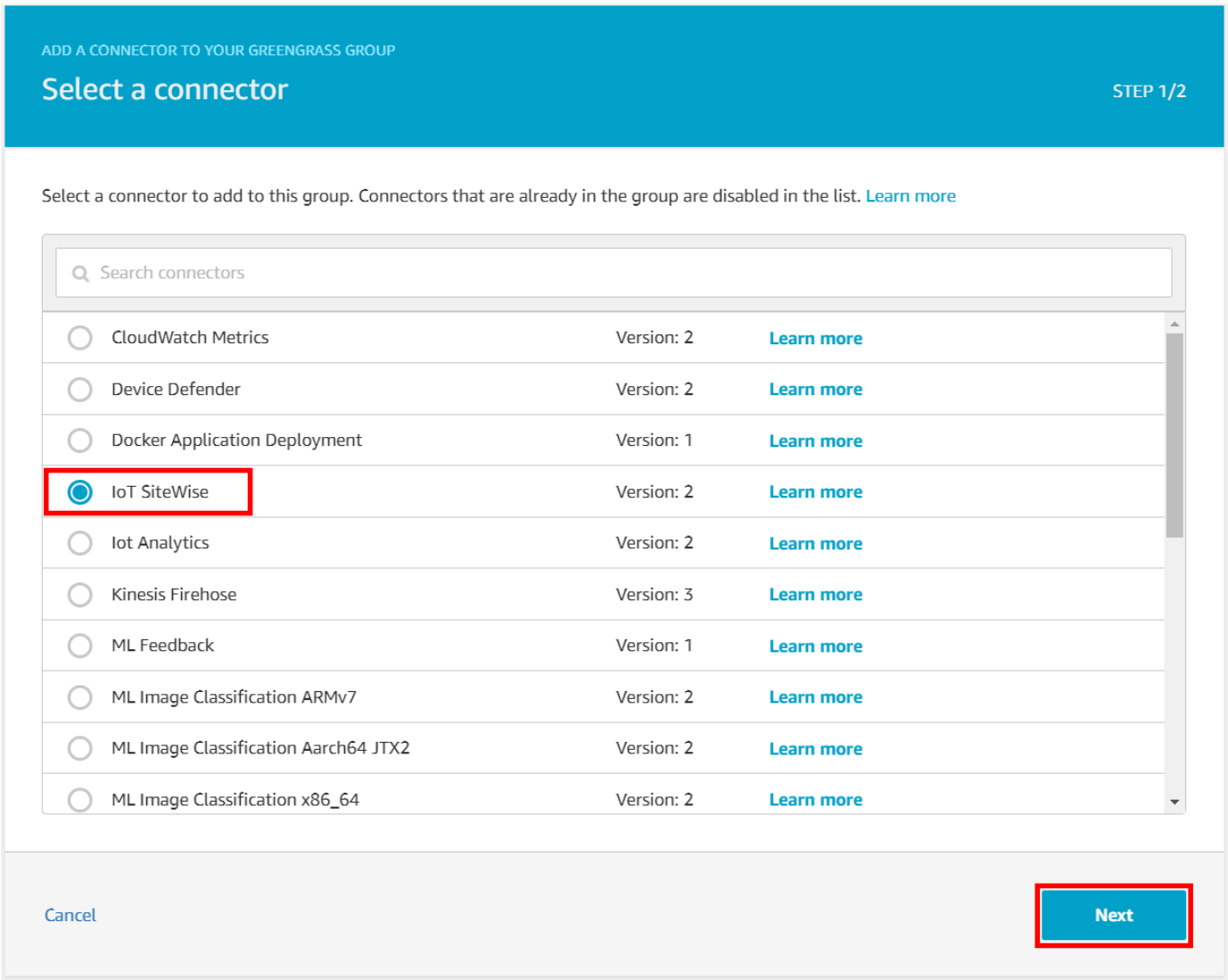
1. Navegue até o console do AWS IoT Greengrass.
2. No painel de navegação à esquerda, em Greengrass, selecione Groups (Grupos) e o grupo que você criou em Configurando o ambiente do SiteWise Edge Gateway.



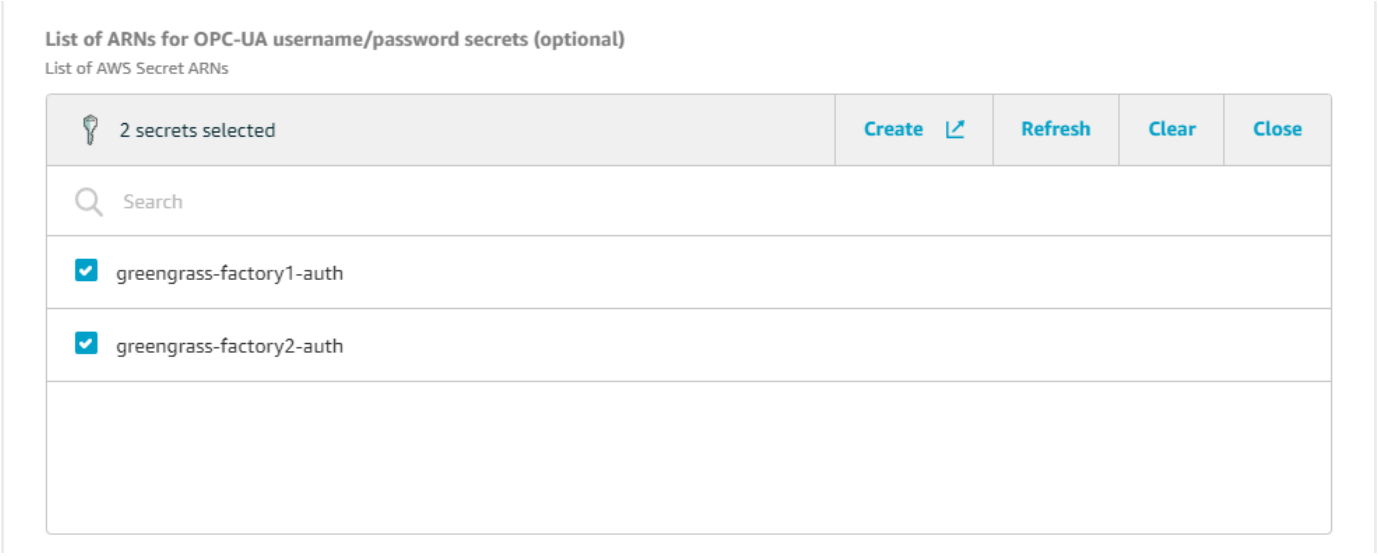
3. Na página de navegação esquerda, escolha Connectors (Conectores). Na página Connectors (Conectores) escolha Add a connector (Adicionar um conector).



4. Escolha IoT na SiteWise lista e escolha Avançar.



5. Se o seu servidor exigir autenticação, você poderá criar AWS Secrets Manager segredos com o nome de usuário e a senha do servidor. Você pode anexar cada segredo ao seu grupo do Greengrass e selecioná-los em Lista de ARNs para segredos de nome de usuário/senha. Para obter mais informações sobre como criar e configurar a função, consulte Configurar a autenticação de origem. Você também pode adicionar segredos ao conector posteriormente.



6. Se você configurar seu gateway SiteWise Edge com um caminho diferente de `/var/sitewise`, insira esse caminho para Caminho de armazenamento local.
7. (Opcional) Insira um tamanho máximo de buffer de disco para o conector. Se o AWS IoT Greengrass núcleo perder a conexão com a AWS nuvem, o conector armazena os dados em cache até que ele possa se conectar com êxito. Se o tamanho do cache exceder o tamanho máximo do buffer de disco, o conector descartará os dados mais antigos da fila.
8. Escolha Adicionar.
9. No canto superior direito, no menu Actions (Ações), escolha Deploy (Implantar).
10. Escolha Automatic detection (Detecção automática) para iniciar a implantação.

    Se a implantação falhar, escolha Deploy (Implantar) novamente. Se continuar a haver falha na implantação, consulte Solução de problemas de implantação do AWS IoT Greengrass.

Adicionando o gateway SiteWise Edge ao AWS IoT SiteWise

Neste procedimento, você adiciona o grupo Greengrass do seu gateway SiteWise Edge a. AWS IoT SiteWise Depois de registrar seu gateway SiteWise Edge com AWS IoT SiteWise, o serviço pode implantar suas configurações de fonte de dados em seu gateway SiteWise Edge.

Para adicionar o gateway SiteWise Edge ao AWS IoT SiteWise

1. Navegue até o console do AWS IoT SiteWise.
2. Escolha Add gateway (Adicionar gateway).
3. Na página Adicionar SiteWise gateway, faça o seguinte:

a. Insira um nome para o gateway SiteWise Edge. Considere incluir a localização do gateway SiteWise Edge no nome para que você possa identificá-lo facilmente.

b. Para o ID de grupo do Greengrass, selecione o grupo do Greengrass criado por você anteriormente.

   Example

c. (Opcional) Em Recursos do Edge, escolha Pacote de processamento de dados. Isso permite a comunicação entre seu gateway SiteWise Edge e quaisquer modelos de ativos e ativos configurados para o Edge. Para ter mais informações, consulte the section called “Habilitar o processamento de dados de borda”.

> **Important**
>
> Se você adicionar o pacote de processamento de dados ao seu gateway SiteWise Edge, deverá configurar e implantar o conector SiteWise Edge em seu AWS IoT Greengrass grupo. Siga as etapas a seguir.

d. Escolha Add gateway (Adicionar gateway).

4. Se você adicionar o pacote de processamento de dados ao seu gateway SiteWise Edge, configure e implante o conector do Processador de AWS IoT SiteWise Dados no seu AWS IoT Greengrass grupo. Siga as etapas the section called “Configurando o conector AWS IoT SiteWise” para configurar o conector do processador de AWS IoT SiteWise dados:

   a. Em Selecionar um conector no AWS IoT Greengrass console, escolha Processador AWS IoT SiteWise de dados.

   b. Em Caminho de armazenamento local, insira o caminho para seu gateway SiteWise Edge.

   c. Escolha Adicionar.

   d. No canto superior direito, no menu Ações, escolha Implantar e, em seguida, escolha Detecção automática para iniciar a implantação.

Após a implantação do gateway SiteWise Edge, você pode adicionar uma fonte para cada equipamento industrial do qual deseja que o gateway SiteWise Edge consuma dados. Para ter mais informações, consulte Configurar fontes de dados.

Você pode visualizar CloudWatch as métricas da Amazon para verificar se seu gateway SiteWise Edge se conecta AWS IoT SiteWise a. Para ter mais informações, consulte AWS IoT Greengrass Version 1 métricas de gateway.

Configurando fontes de dados em gateways AWS IoT Greengrass V1 SiteWise Edge

Depois de configurar um gateway AWS IoT SiteWise Edge, você pode configurar fontes de dados para que seu gateway SiteWise Edge possa ingerir dados de equipamentos industriais locais para AWS IoT SiteWise. Cada fonte representa um servidor local, como um servidor OPC-UA, que seu gateway SiteWise Edge conecta e recupera fluxos de dados industriais. Para obter mais informações sobre como configurar um gateway SiteWise Edge, consulteConfigurando um gateway AWS IoT Greengrass V1 SiteWise Edge.

> **Note**
>
> AWS IoT SiteWise reinicia seu gateway SiteWise Edge sempre que você adiciona ou edita uma fonte. Seu gateway SiteWise Edge não ingere dados durante a reinicialização. O tempo para reiniciar o gateway SiteWise Edge depende do número de tags nas fontes do gateway SiteWise Edge. O tempo de reinicialização pode variar de alguns segundos (para

um gateway SiteWise Edge com poucas tags) a vários minutos (para um gateway SiteWise Edge com muitas tags).

Depois de criar origens, você pode associar os fluxos de dados às propriedades do ativo. Para obter mais informações sobre como criar e usar ativos, consulte Modelagem de ativos industriais e Mapeamento de fluxos de dados industriais para propriedades de ativos.

Você pode visualizar CloudWatch métricas para verificar se uma fonte de dados está conectada AWS IoT SiteWise a. Para ter mais informações, consulte AWS IoT Greengrass Version 1 métricas de gateway.

Atualmente, AWS IoT SiteWise oferece suporte aos seguintes protocolos de fonte de dados:

- OPC-UA — Um protocolo de comunicação machine-to-machine (M2M) para automação industrial.
- Modbus TCP — Um protocolo de comunicação de dados usado para interagir com controladores lógicos programáveis (programmable logic controllers, PLCs).
- EtherNet/IP (EIP) — Um protocolo de rede industrial que adapta o protocolo industrial comum (Common Industrial Protocol, CIP) à Ethernet padrão.

> **Note**
>
> SiteWise Os gateways Edge em execução AWS IoT Greengrass V2 atualmente não suportam fontes Modbus TCP e Ethernet IP.

Tópicos

Configurar uma origem Modbus TCP

Você pode usar o AWS IoT SiteWise console ou um recurso de gateway AWS IoT SiteWise Edge para definir e adicionar uma fonte Modbus TCP ao seu gateway SiteWise Edge. Essa origem representa um servidor Modbus TCP local.

> **Note**
>
> - SiteWise Os gateways Edge em execução AWS IoT Greengrass V2 atualmente não suportam fontes Modbus TCP.
> - Você deve instalar o AWS IoT SiteWise conector para usar uma fonte Modbus TCP.

Você pode usar a fonte Modbus TCP para converter o tipo de dados da sua fonte em um tipo de dados diferente quando recebidos no gateway SiteWise Edge. O tipo de dados de origem determina os tipos de dados que você pode escolher para seus dados de destino. Você também pode optar por trocar bytes usando a origem Modbus TCP. A tabela a seguir fornece mais informações sobre os tipos de dados de origem, os tipos de dados de destino e os modos de troca que são compatíveis.

Para obter mais informações sobre os modos de troca, consulte o artigo Como dados reais (de ponto flutuante) e de 32 bits são codificados em mensagens Modbus RTU sobre codificação de mensagens Modbus.

Tipo de dados de origem	Tipos de dados de destino compatíveis	Modos de troca compatíveis	Versões de conectores compatíveis
ASCII	String	noSwap	2
UTF8	String	noSwap	2
ISO8859	String	noSwap	2
Int16	Inteiro, duplo, string	noSwap	1 e 2
Int32	Inteiro, duplo, string	NoSwap, ByteSwap byteWordSwap, WordSwap	1 e 2

Tipo de dados de origem	Tipos de dados de destino compatíveis	Modos de troca compatíveis	Versões de conectores compatíveis
Float	Duplo, string	NoSwap, ByteSwap byteWordSwap, WordSwap	1 e 2
Booleano	Booleano	noSwap	1 e 2
Hex-dump	String	noSwap	1 e 2

Tópicos

Configurar uma origem Modbus TCP (console)

Para configurar uma origem Modbus TCP

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação à esquerda, escolha Gateways.
3. No gateway SiteWise Edge para o qual você deseja criar uma fonte, escolha Gerenciar e, em seguida, escolha Exibir detalhes.
4. Escolha New source (Nova fonte) no canto superior direito.
5. Para Opções de protocolo, escolha Modbus TCP.
6. Para a Configuração da origem Modbus TCP, insira um Nome para a origem.
7. Em Endereço IP, insira o endereço IP para o servidor da fonte de dados.
8. (Opcional) Insira a Porta e ID da unidade para o servidor de origem.
9. (Opcional) Em Duração mínima entre solicitações, insira o intervalo de tempo entre as solicitações subsequentes enviadas ao seu servidor. Seu gateway SiteWise Edge calcula automaticamente o intervalo mínimo permitido com base no seu dispositivo e no número de registros que você tem.
10. Em Grupos de propriedades, insira um Nome.
11. Para Propriedades:

a. Em Tag, insira um alias de propriedade para seu conjunto de registros. Por exemplo, **`TT-001`**.

b. Em Endereço de registro, insira o endereço de registro que inicia o conjunto de registros.

c. Em Tipo de dados de origem, escolha o tipo de dados Modbus TCP do qual você deseja converter os dados. O padrão é Despejo hexadecimal.

> **Note**
>
> O tipo de dados de origem escolhido determina o tamanho dos dados, tipo de dados de destino e modo de troca que você pode escolher. Para ter mais informações, consulte the section called “Configurar uma origem Modbus TCP”.

d. Em Tamanho dos dados, insira o número de registros a serem lidos ao iniciar pelo endereço do registro. Isso é determinado pelo tipo de dados de origem que você escolhe para essa origem.

e. Em Tipo de dados de destino, escolha o tipo de AWS IoT SiteWise dados para o qual você deseja que seus dados sejam convertidos. O padrão é String. O tipo de destino deve ser compatível com o tipo de dados de origem que você escolher para essa origem. Para ter mais informações, consulte the section called “Configurar uma origem Modbus TCP”.

f. Para o Modo de troca, escolha o modo de troca de dados que você deseja usar para ler dados do seu conjunto de registros. O modo de troca deve ser compatível com o tipo de dados de origem que você escolher para essa origem. Para ter mais informações, consulte the section called “Configurar uma origem Modbus TCP”.

12. Em Taxa de digitalização, atualize a taxa na qual você deseja que o gateway SiteWise Edge leia seus registros. AWS IoT SiteWise calcula automaticamente a taxa de varredura mínima permitida para seu gateway SiteWise Edge.

13. (Opcional) Em Destinos, escolha para onde os dados de origem são enviados. Por padrão, sua fonte envia dados para AWS IoT SiteWise.Você pode usar um AWS IoT Greengrass stream para exportar seus dados para um destino local ou para a AWS nuvem.

> **Note**
>
> Você deve escolher AWS IoT SiteWise como destino para seus dados de origem se quiser processar dados dessa fonte na borda com AWS IoT SiteWise. Para obter mais

informações sobre o processamento de dados na borda, consulte the section called "Habilitar o processamento de dados de borda".

Para enviar seus dados para outro destino:

a. Em Opções de destino, escolha Outros destinos.

b. Para o nome do stream do Greengrass, insira o nome exato do seu AWS IoT Greengrass stream.

> **Note**
>
> Você pode usar um fluxo que você já criou ou criar um novo fluxo de AWS IoT Greengrass para exportar seus dados. Se quiser usar um fluxo existente, insira o nome exato do fluxo ou um novo fluxo será criado.
> Para obter mais informações sobre como trabalhar com AWS IoT Greengrass fluxos, consulte Gerenciar fluxos de dados no guia do AWS IoT Greengrass desenvolvedor.

14. Escolha Add source (Adicionar origem).

AWS IoT SiteWise implanta a configuração do gateway SiteWise Edge em seu AWS IoT Greengrass núcleo. Você não precisa iniciar manualmente uma implantação.

Configurar uma origem Modbus TCP (CLI)

Você pode definir fontes de dados Modbus TCP em um recurso de gateway SiteWise Edge. Você deve definir todas as origens Modbus TCP em uma única configuração de recursos.

> **Note**
>
> Você deve instalar o AWS IoT SiteWise conector para usar uma fonte Modbus TCP.

Esse recurso tem as seguintes versões.

Version (Versão)	Namespace
1	`iotsitewise:modbuscollector:1`

Parâmetros de configuração de recursos Modbus TCP

Ao definir origens Modbus TCP em uma configuração de recursos, especifique as seguintes informações no documento JSON `capabilityConfiguration`:

fontes

Uma lista de estruturas de definição de origem Modbus TCP que contêm as seguintes informações:

name

Um nome exclusivo e amigável para a origem.

measurementDataStreamPrefixo

(Opcional) Uma string que deve preceder todos os fluxos de dados da origem. O gateway SiteWise Edge adiciona esse prefixo a todos os fluxos de dados dessa fonte. Use um prefixo de stream de dados para distinguir entre streams de dados que têm o mesmo nome de origens diferentes. Cada stream de dados deve ter um nome exclusivo na conta.

destino

Uma estrutura de destino que contém as seguintes informações:

tipo

O tipo do destino.

Nome do stream

O nome do AWS IoT Greengrass stream.

streamBufferSize

O tamanho do buffer de fluxo.

endpoint

Uma estrutura de endpoint que contém as seguintes informações:

IPAddress

O endereço IP de origem Modbus TCP.

port

(Opcional) A porta de origem Modbus TCP.

ID da unidade

(Opcional) O unitID. O valor padrão é 1.

minimumInterRequestDuração

A duração mínima entre cada solicitação em milissegundos.

Grupos de propriedades

A lista de grupos de propriedades que definem a tag solicitada pelo protocolo.

name

O nome do grupo de propriedade. Esse deve ser um identificador exclusivo.

tagPathDefinitions

A localização da medição na origem. Por exemplo, a ordem dos bytes e das palavras, o endereço e o tipo de transformação. A estrutura de cada `MeasurementPathDefinition` é definida pelo conector.

Modo de digitalização

Define o comportamento do modo de verificação e os parâmetros configuráveis para a origem.

Configurar uma origem EtherNet/IP (EIP)

Você pode usar o AWS IoT SiteWise console ou um recurso de gateway SiteWise Edge para definir e adicionar uma fonte IP Ethernet ao seu gateway SiteWise Edge. Essa origem representa um servidor Ethernet IP local.

> **Note**
>
> - SiteWise Os gateways Edge em execução AWS IoT Greengrass V2 atualmente não oferecem suporte a fontes IP Ethernet.

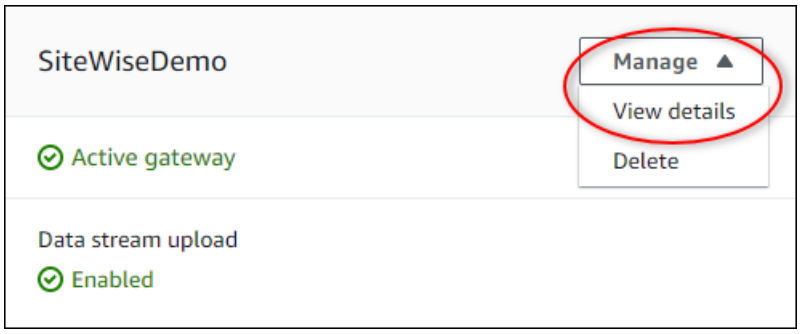
- Você deve instalar o AWS IoT SiteWise conector para usar uma fonte IP Ethernet.

Tópicos

Configurar uma origem Ethernet IP (console)

Configurar uma origem Ethernet IP

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação à esquerda, escolha Gateways.
3. No gateway SiteWise Edge para o qual você deseja criar uma fonte, escolha Gerenciar e, em seguida, escolha Exibir detalhes.



4. Escolha New source (Nova fonte) no canto superior direito.
5. Para Opções de protocolo, escolha Ethernet/IP (EIP).
6. Para a configuração da fonte EtherNet /IP, insira um Nome para a fonte.
7. Em Endereço IP, insira o endereço IP para o servidor da fonte de dados.
8. (Opcional) Insira a Porta para o servidor de origem.
9. Em Duração mínima entre solicitações, insira o intervalo de tempo entre as solicitações subsequentes enviadas ao seu servidor. Seu gateway SiteWise Edge calcula automaticamente o intervalo mínimo permitido com base no seu dispositivo e no número de registros que você tem.
10. Em Grupos de propriedades, insira um Nome.
11. Para Propriedades:

a. Em Tag, insira o alias de propriedade para seu conjunto de registros. Por exemplo, **`boiler.inlet.temperature.value`**.

b. Em Tipo de dados de destino, escolha o tipo de AWS IoT SiteWise dados para o qual você deseja que seus dados sejam convertidos. O padrão é String.

12. Em Taxa de digitalização, atualize a taxa na qual você deseja que o gateway SiteWise Edge leia seus registros. AWS IoT SiteWise calcula automaticamente a taxa de varredura mínima permitida para seu gateway SiteWise Edge.

13. (Opcional) Em Destinos, escolha para onde os dados de origem são enviados. Por padrão, sua fonte envia dados para AWS IoT SiteWise.Você pode usar um AWS IoT Greengrass stream para exportar seus dados para um destino local ou para a AWS nuvem.

> **Note**
>
> Você deve escolher AWS IoT SiteWise como destino para seus dados de origem se quiser processar dados dessa fonte na borda com AWS IoT SiteWise. Para obter mais informações sobre o processamento de dados na borda, consulte the section called “Habilitar o processamento de dados de borda”.

Para enviar seus dados para outro destino:

a. Em Opções de destino, escolha Outros destinos.

b. Para o nome do stream do Greengrass, insira o nome exato do seu AWS IoT Greengrass stream.

> **Note**
>
> Você pode usar um fluxo que você já criou ou criar um novo fluxo de AWS IoT Greengrass para exportar seus dados. Se quiser usar um fluxo existente, insira o nome exato do fluxo ou um novo fluxo será criado.
> Para obter mais informações sobre como trabalhar com AWS IoT Greengrass fluxos, consulte Gerenciar fluxos de dados no guia do AWS IoT Greengrass desenvolvedor.

14. Escolha Add source (Adicionar origem).

AWS IoT SiteWise implanta a configuração do gateway SiteWise Edge em seu AWS IoT Greengrass núcleo. Você não precisa iniciar manualmente uma implantação.

Configurar uma origem Ethernet/IP (CLI)

Você pode definir fontes de dados EIP em um recurso de gateway do SiteWise Edge. Você deve definir todas as origens EIP em uma única configuração de recursos.

> **Note**
>
> Você deve instalar o AWS IoT SiteWise conector para usar uma fonte IP Ethernet.

Esse recurso tem as seguintes versões.

Version (Versão)	Namespace
1	`iotsitewise:eipcollector:1`

Parâmetros de configuração de recursos de EIP

Ao definir as origens EIP em uma configuração de recursos, especifique as seguintes informações no documento JSON `capabilityConfiguration`:

fontes

Uma lista de estruturas de definição de origem EIP que contêm as seguintes informações:

name

Um nome exclusivo e amigável para a origem. Esse nome pode ter até 256 caracteres.

destinationPathPrefix

(Opcional) Uma string que deve preceder todos os fluxos de dados da origem. O gateway SiteWise Edge adiciona esse prefixo a todos os fluxos de dados dessa fonte. Use um prefixo de stream de dados para distinguir entre streams de dados que têm o mesmo nome de origens diferentes. Cada stream de dados deve ter um nome exclusivo na conta.

destino

Uma estrutura de destino que contém as seguintes informações:

tipo

O tipo do destino.

Nome do stream

O nome do AWS IoT Greengrass stream.

streamBufferSize

O tamanho do buffer de fluxo.

endpoint

Uma estrutura de endpoint que contém as seguintes informações:

IPAddress

O endereço IP de origem EIP.

port

(Opcional) A porta de origem EIP. Os valores aceitos são números entre 1 e 65535.

minimumInterRequestDuração

(Opcional) A duração mínima entre cada solicitação em milissegundos.

Grupos de propriedades

A lista de grupos de propriedades que definem a tag solicitada pelo protocolo. Cada origem pode ter um grupo de propriedades.

name

O nome do grupo de propriedade. Esse nome deve ser um identificador exclusivo com um tamanho máximo de 256 caracteres.

tagPathDefinitions

A lista de estruturas que especificam os dados a serem coletados do dispositivo EtherNet/IP e como transformá-los para saída.

tipo

O tipo do `tagPathDefinition`. Por exemplo, `EIPTagPath`.

path

O caminho do `tagPathDefinition`. Cada tag em um caminho pode ter no máximo 40 caracteres e pode começar com uma letra ou um sublinhado. As tags não podem conter sublinhados consecutivos ou finais. O caminho é prefixado com qualquer valor de destinationPathPrefix.

dstDataType

O tipo de dados para gerar os dados da tag. Os valores aceitos são `integer`, `double`, `string` e `boolean`.

Modo de digitalização

Define o comportamento do modo de verificação e os parâmetros configuráveis para a origem.

tipo

O tipo de comportamento do modo de verificação. Os valores aceitos são `POLL`.

taxa

A taxa em milissegundos em que o conector deve ler as tags da origem Ethernet/IP.

Configurar a autenticação de origem

Se os servidores OPC-UA exigirem credenciais de autenticação para conectar-se, você poderá definir um nome de usuário e senha em um segredo para cada origem no AWS Secrets Manager. Em seguida, você adiciona o segredo ao seu grupo Greengrass e ao SiteWise conector de IoT para disponibilizar o segredo no seu gateway Edge. SiteWise Para obter mais informações, consulte Implantar segredos no AWS IoT Greengrass núcleo no Guia do AWS IoT Greengrass Version 1 desenvolvedor.

Depois que um segredo estiver disponível para seu gateway SiteWise Edge, você poderá escolhê-lo ao configurar uma fonte. Em seguida, o gateway SiteWise Edge usa as credenciais de autenticação do segredo quando se conecta à fonte. Para ter mais informações, consulte Configurar fontes de dados.

Tópicos

- Criar segredos de autenticação de origem

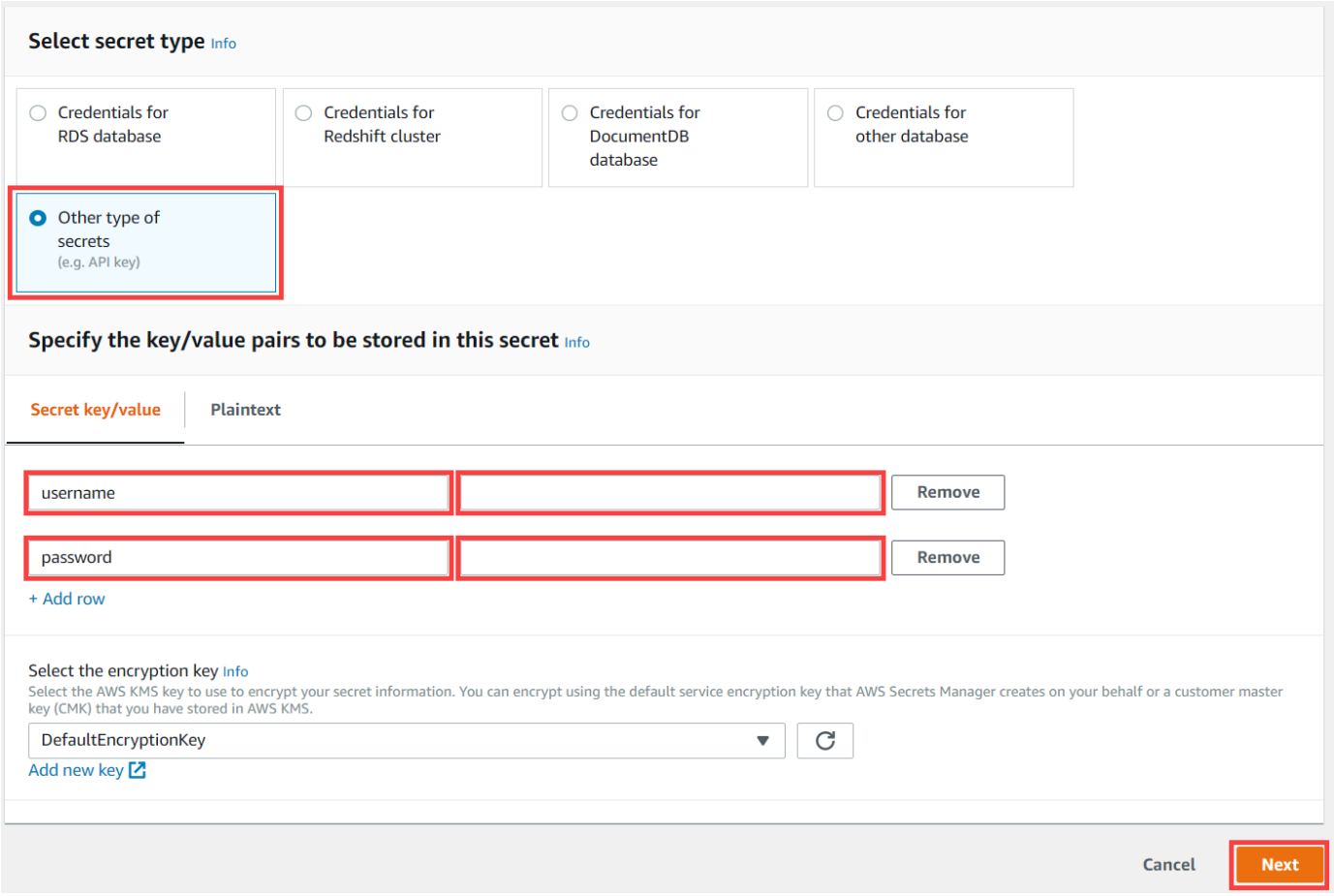
- Adicionar segredos a um grupo do Greengrass
- Adicionando segredos a um conector de IoT SiteWise

Criar segredos de autenticação de origem

Neste procedimento, você cria um segredo de autenticação para sua origem no Secrets Manager. No segredo, defina pares de chave-valor de **`username`** e **`password`** que contenham detalhes da autenticação para sua origem.

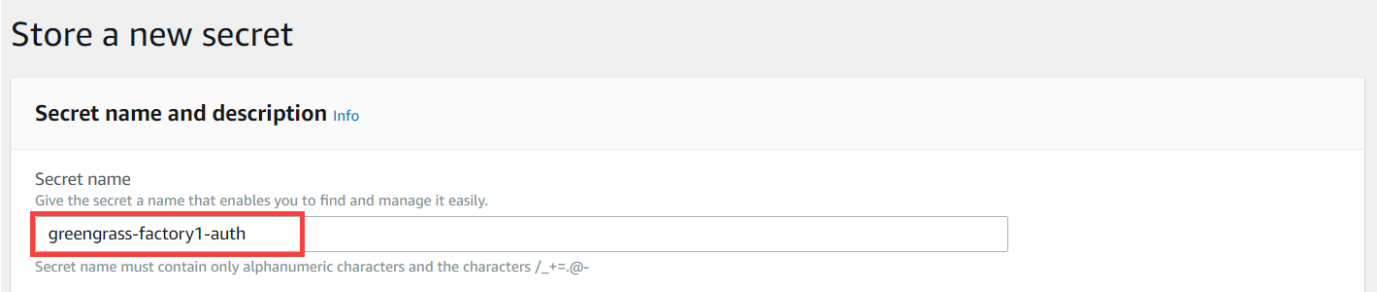
Como criar um segredo de autenticação de origem

1. Navegue até o console do Secrets Manager.
2. Selecione Armazenar um novo segredo.
3. Em Select secret type (Selecionar tipo de segredo), selecione Other type of secrets (Outro tipo de segredos).
4. Insira os pares de chave/valor **`username`** e **`password`** para os valores de autenticação do servidor OPC-UA e escolha Next (Próximo).



5. Insira um Secret name (Nome de segredo) que comece com `greengrass-`, como **`greengrass-factory1-auth`**.

> **Important**
>
> Você deve usar o prefixo `greengrass-` da função de serviço padrão do AWS IoT Greengrass para acessar seus segredos. Se quiser nomear seus segredos sem esse prefixo, você deve conceder permissões AWS IoT Greengrass personalizadas para acessar seus segredos. Para obter mais informações, consulte Permitir AWS IoT Greengrass a obtenção de valores secretos no Guia do AWS IoT Greengrass Version 1 desenvolvedor.



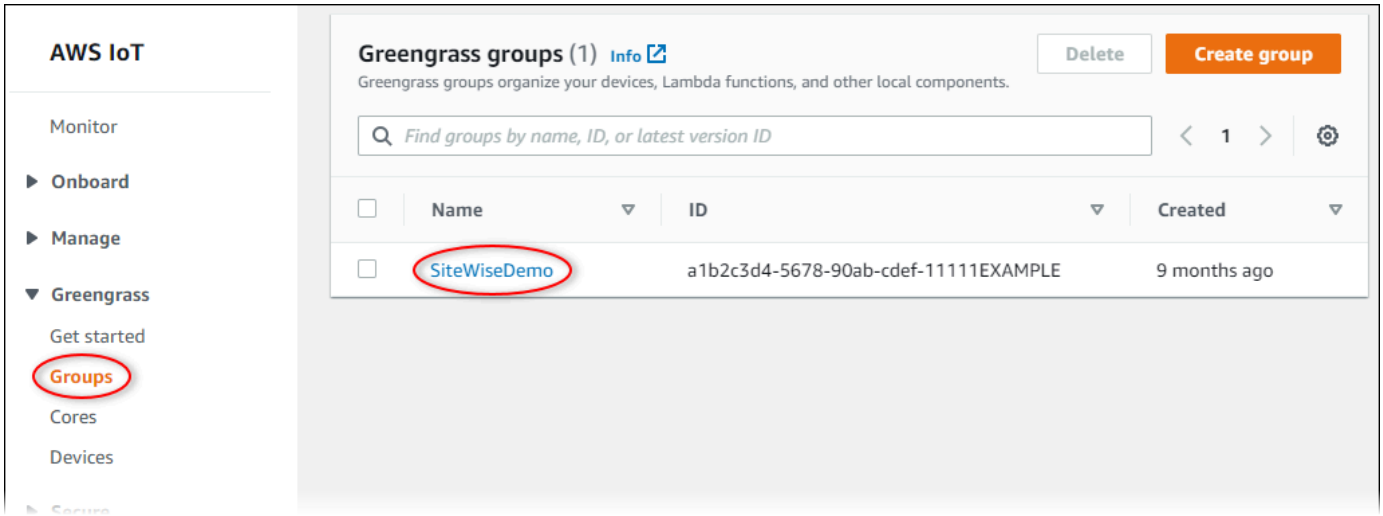
6. Informe uma Description (Descrição) e escolha Next (Próximo).
7. (Opcional) Na página Configure automatic rotation (Configurar mudança automática), configure a mudança automática para seus segredos. Se você configurar a alternância automática, deverá reimplantar seu grupo do Greengrass sempre que um segredo alternar.
8. Na página Configure automatic rotation (Configurar mudança automática escolha Next (Próximo).
9. Revise o novo segredo e escolha Store (Armazenar).

Adicionar segredos a um grupo do Greengrass

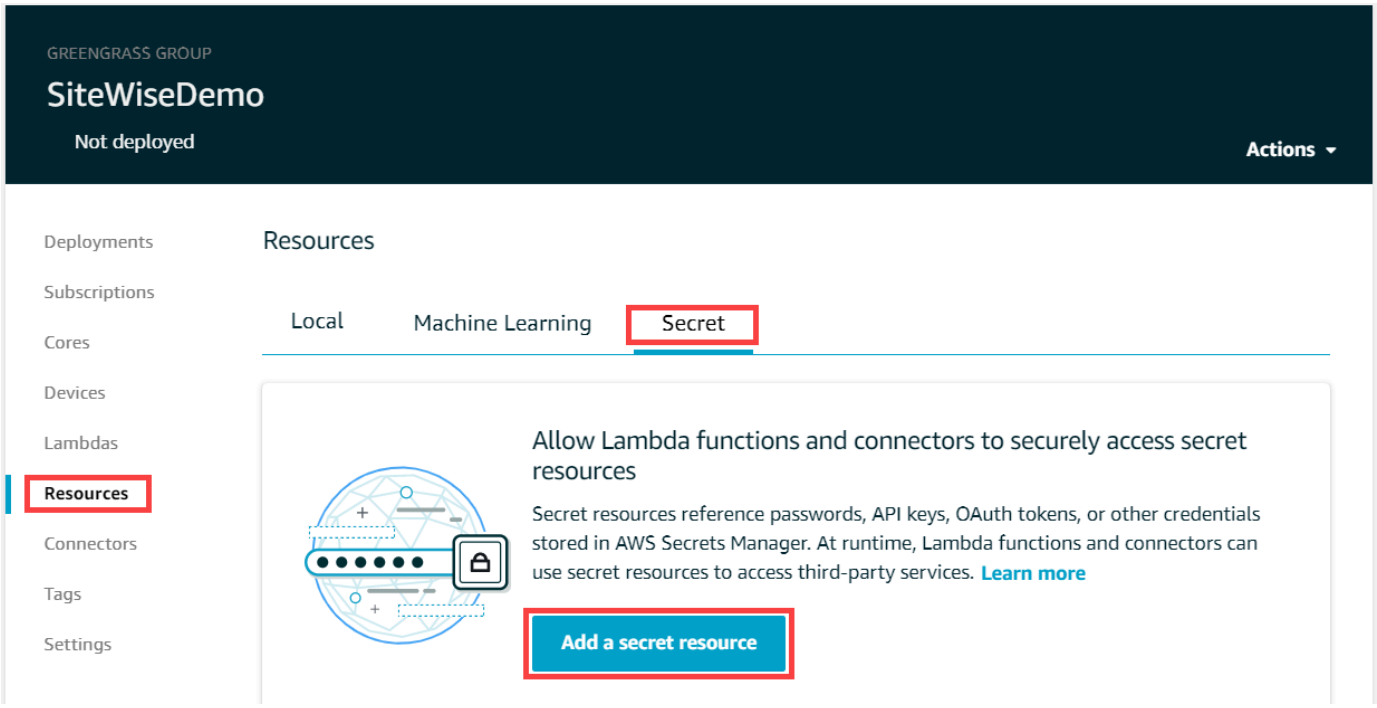
Neste procedimento, você adiciona seus segredos de autenticação de origem ao seu AWS IoT Greengrass grupo para disponibilizá-los ao seu conector de IoT SiteWise .

Para adicionar segredos a um grupo do Greengrass

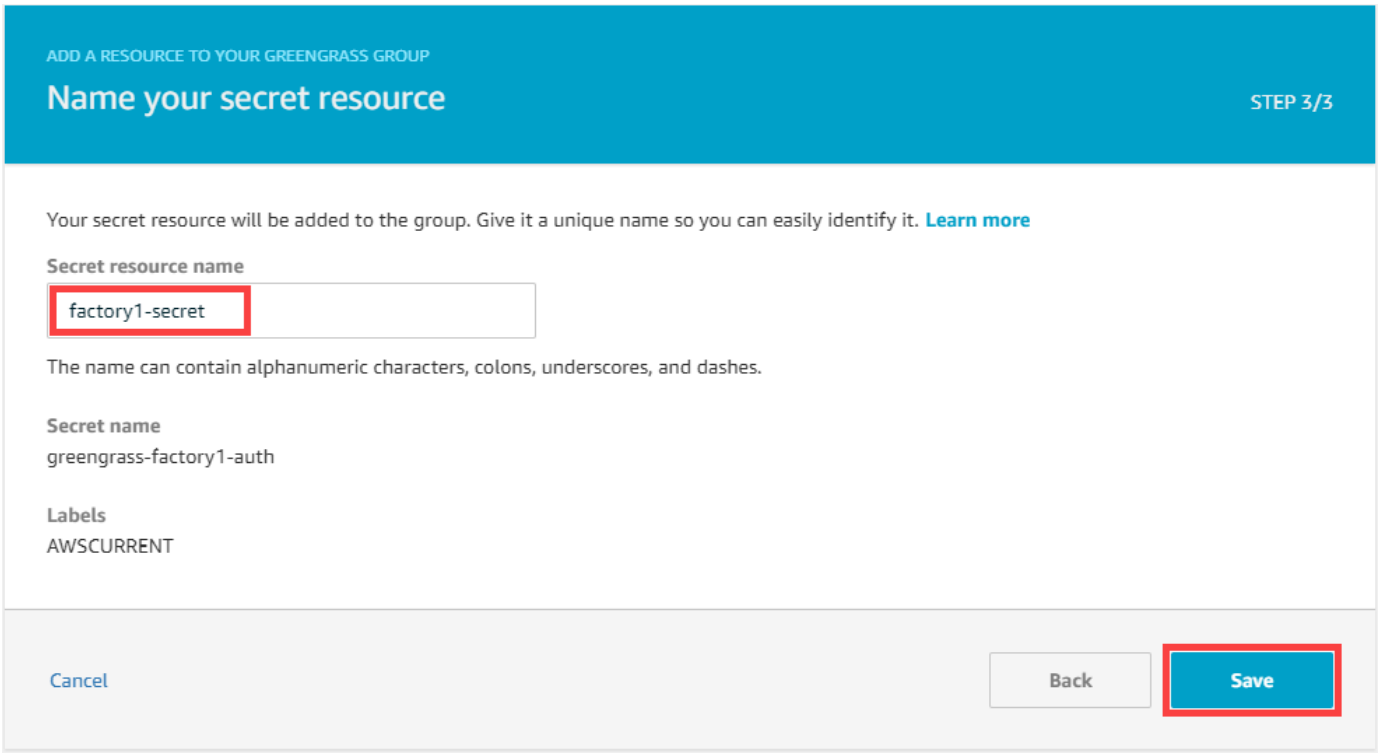
1. Navegue até o console do AWS IoT Greengrass.
2. No painel de navegação, em Greengrass, escolha Grupos e escolha seu grupo.



3. Na página de navegação, escolha Recursos.
4. Na página Resources (Recursos) escolha a guia Secret (Segredo) e escolha Add a secret resource (Adicionar um recurso de segredo).



5. Escolha Select (Selecionar) e escolha seu segredo na lista.
6. Escolha Próximo.
7. Em Secret resource name (Nome do recurso de segredo), insira um nome para o recurso e escolha Save (Salvar).

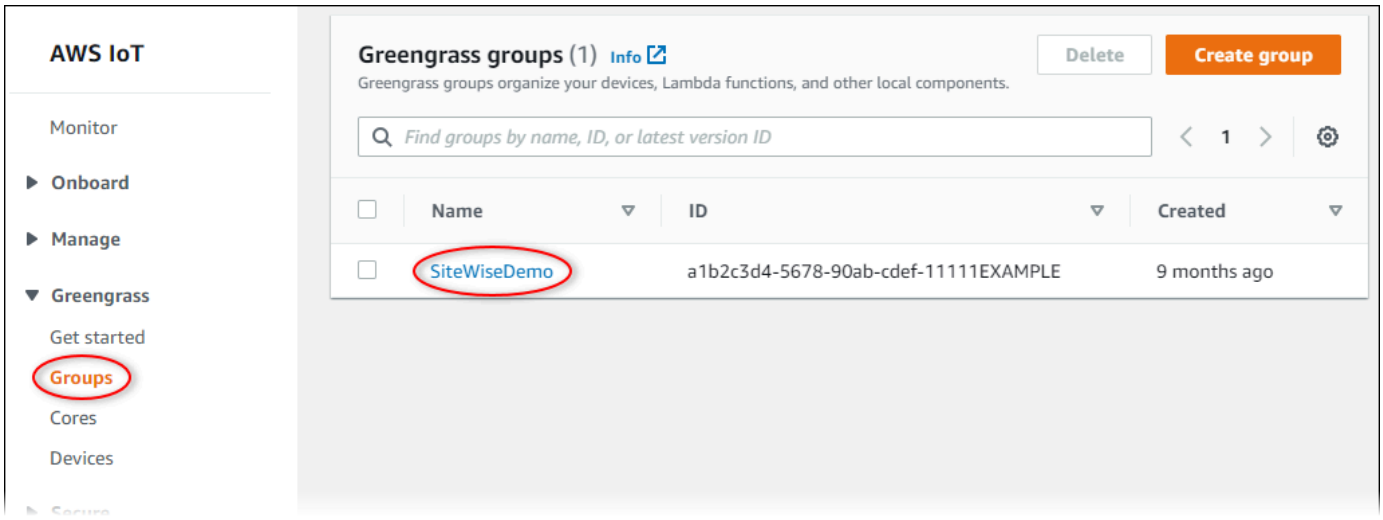


Adicionando segredos a um conector de IoT SiteWise

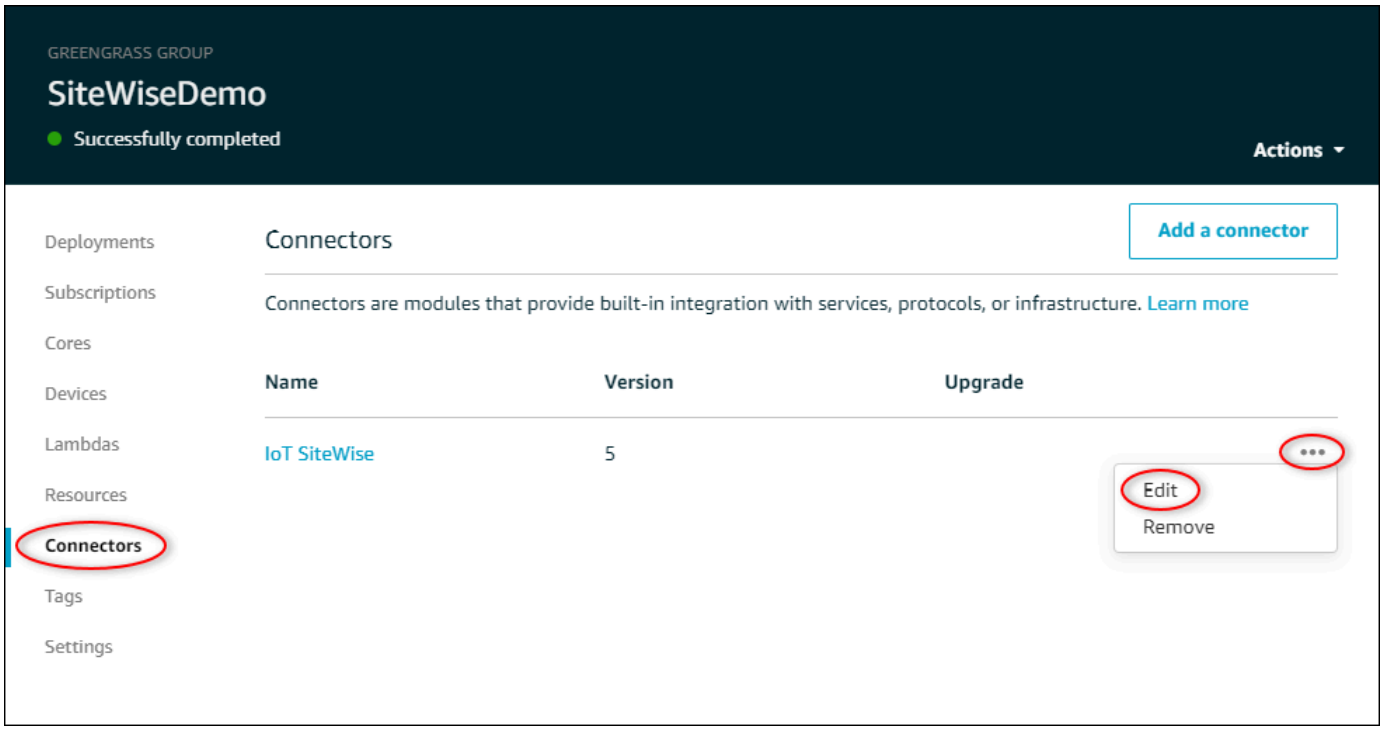
Neste procedimento, você adiciona seus segredos de autenticação de origem ao seu SiteWise conector de IoT para disponibilizá-los AWS IoT SiteWise e para seu gateway SiteWise Edge.

Para adicionar um segredo ao seu conector de IoT SiteWise

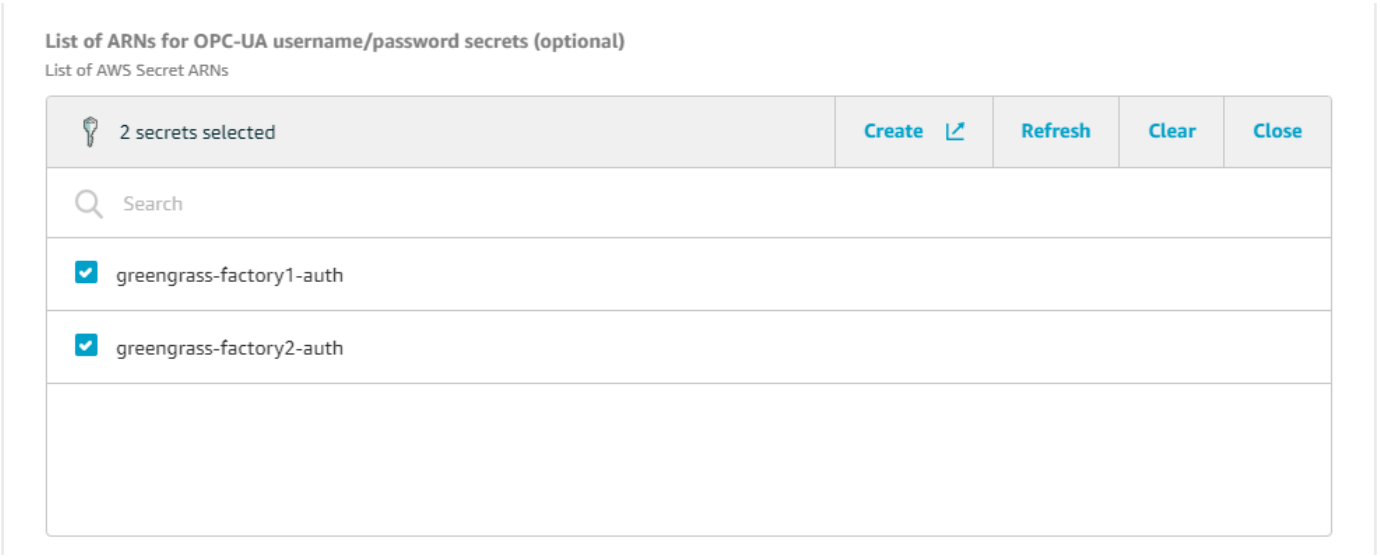
1. Navegue até o console do AWS IoT Greengrass.
2. No painel de navegação, em Greengrass, escolha Grupos e escolha seu grupo.



3. Na página de navegação, escolha Conectores.
4. Escolha o ícone de reticências do SiteWise conector IoT para abrir o menu de opções e, em seguida, escolha Editar.



5. Em Lista de ARNs para segredos de nome de usuário/senha OPC-UA, escolha Selecionar e, em seguida, selecione cada segredo a ser adicionado a esse gateway Edge. SiteWise Se precisar criar segredos, consulte Criar segredos de autenticação de origem.



Se o segredo não aparecer, escolha Refresh (Atualizar). Se o segredo ainda não aparecer, verifique se você adicionou o segredo ao seu grupo do Greengrass.

6. Escolha Salvar.
7. No canto superior direito, no menu Actions (Ações), escolha Deploy (Implantar).
8. Escolha Automatic detection (Detecção automática) para iniciar a implantação.

   Se a implantação falhar, escolha Deploy (Implantar) novamente. Se continuar a haver falha na implantação, consulte Solução de problemas de implantação do AWS IoT Greengrass.

   Após a implantação do grupo, você pode configurar uma origem que usa o novo segredo. Para ter mais informações, consulte Configurar fontes de dados.

Atualizando um conector

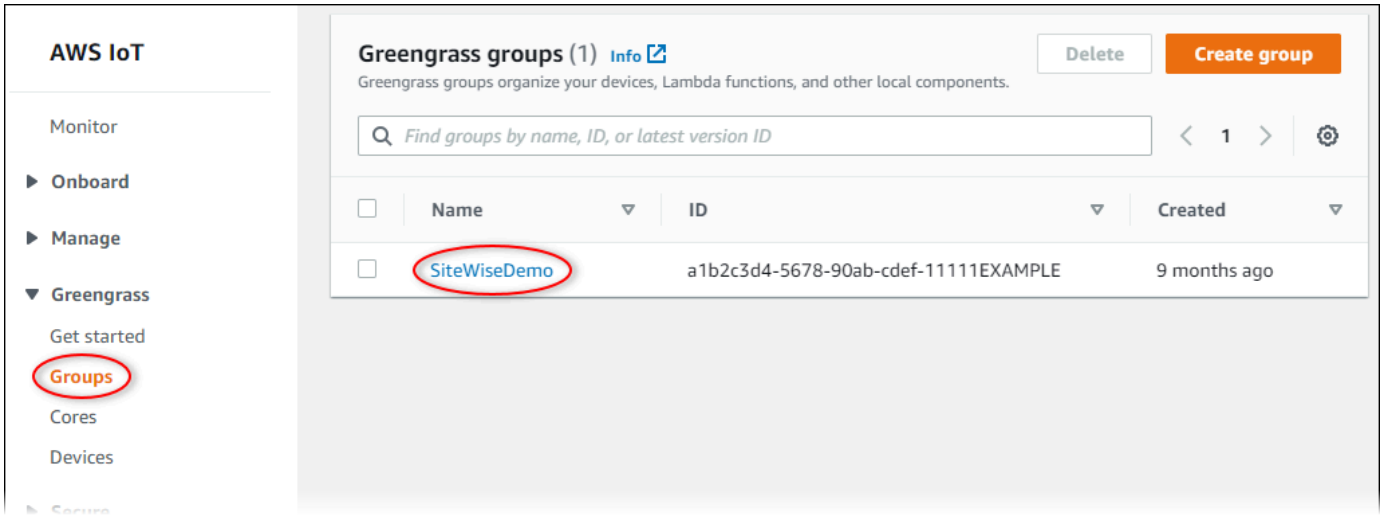
> **Important**
>
> A versão 6 do SiteWise conector IoT introduz novos requisitos: software AWS IoT Greengrass principal v1.10.0 e gerenciador de fluxo. Antes de atualizar seu conector, verifique se seu gateway SiteWise Edge atende a esses requisitos, ou você não conseguirá implantar seu gateway SiteWise Edge.

Você pode atualizar facilmente o conector do gateway SiteWise Edge após o lançamento de uma nova versão do SiteWise conector de IoT.

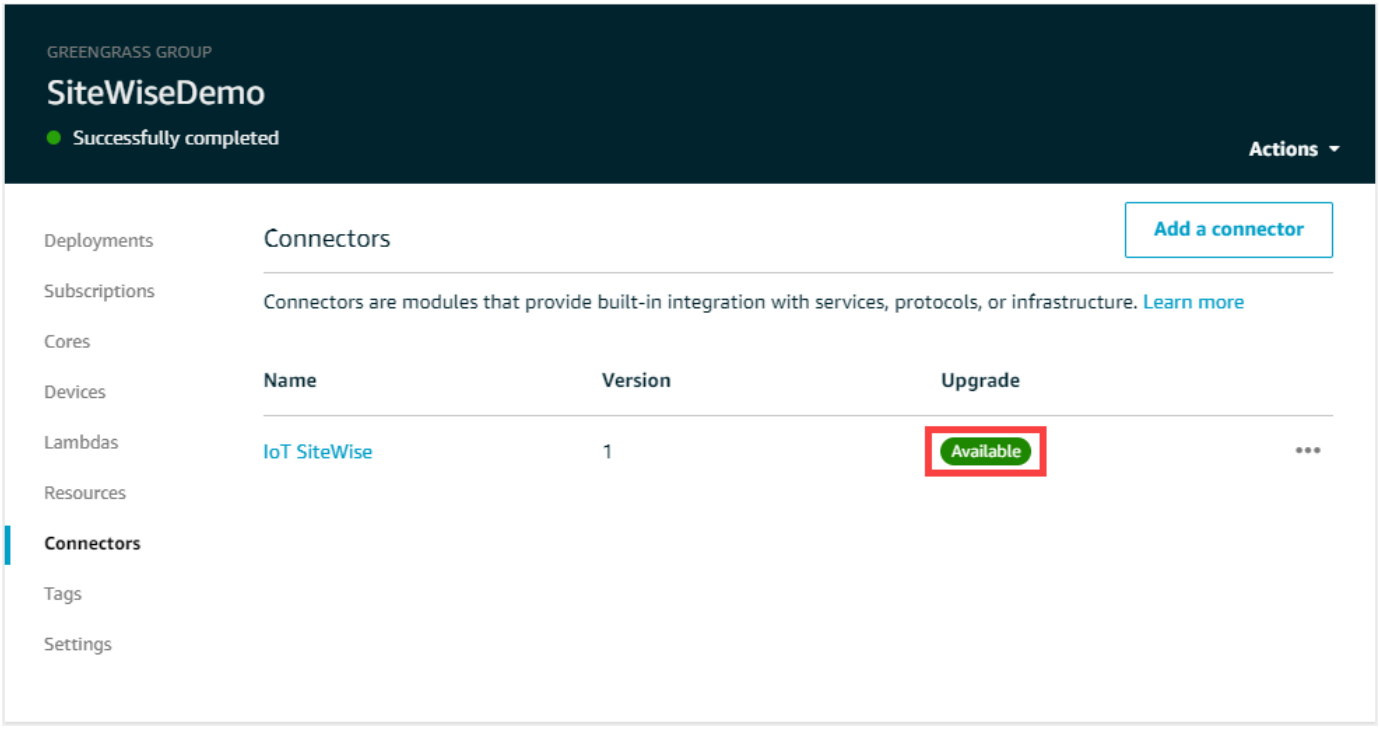
> **Note**
>
> Neste procedimento, você reimplanta seu grupo Greengrass e reinicia SiteWise seu gateway Edge. Seu gateway SiteWise Edge não ingere dados durante a reinicialização. O tempo para reiniciar o gateway SiteWise Edge depende do número de tags nas fontes do gateway SiteWise Edge. O tempo de reinicialização pode variar de alguns segundos (para um gateway SiteWise Edge com poucas tags) a vários minutos (para um gateway SiteWise Edge com muitas tags).

Para atualizar um conector de IoT SiteWise

1. Navegue até o console do AWS IoT Greengrass.
2. No painel de navegação, em Greengrass, escolha Grupos e, em seguida, escolha o grupo que você criou ao configurar SiteWise seu gateway Edge.



3. No painel de navegação, escolha Conectores.
4. Na página Conectores, escolha Disponível ao lado do conector de SiteWiseIoT.



Se você não vir o elemento Available (Disponível), seu conector já está na versão mais recente.

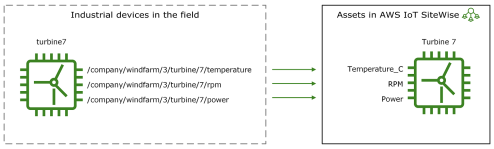
5. Na página Upgrade connector (Atualizar conector), insira os parâmetros do conector e escolha Upgrade (Atualizar).
6. No canto superior direito, no menu Actions (Ações), escolha Deploy (Implantar).
7. Escolha Automatic detection (Detecção automática) para iniciar a implantação.

Se a implantação falhar, escolha Deploy (Implantar) novamente. Se continuar a haver falha na implantação, consulte Solução de problemas de implantação do AWS IoT Greengrass.

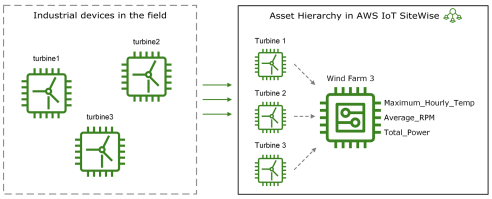
Modelagem de ativos industriais

Você pode criar representações virtuais de sua operação industrial com AWS IoT SiteWise ativos. Um ativo representa um dispositivo, um equipamento ou um processo que carrega um ou mais fluxos de dados para o. Nuvem AWS Por exemplo, um dispositivo do ativo pode ser uma turbina eólica que envia medições de temperatura do ar, velocidade de rotação da hélice e séries temporais de saída de energia para propriedades do ativo no AWS IoT SiteWise.

Cada fluxo de dados corresponde ao apelido de propriedade exclusivo. Por exemplo, o apelido `/company/windfarm/3/turbine/7/temperature` identifica exclusivamente o fluxo de dados de temperatura proveniente da turbina nº 7 no parque eólico nº 3. Você pode configurar AWS IoT SiteWise ativos para transformar dados de medição recebidos usando expressões matemáticas, como converter dados de temperatura de Celsius em Fahrenheit.



Um ativo também pode representar um agrupamento lógico de dispositivos, como um parque eólico inteiro. É possível associar ativos a outros ativos para criar hierarquias que representem operações industriais complexas. Os ativos podem acessar os dados em seus ativos secundários associados. Ao fazer isso, você pode usar AWS IoT SiteWise expressões para calcular métricas agregadas, como a produção líquida de energia de um parque eólico.



Você deve criar todos os ativos a partir de um modelo de ativos. Os modelos de ativos são estruturas declarativas que padronizam o formato de seus ativos. Os modelos de ativos impõem informações consistentes em vários ativos do mesmo tipo para que você possa processar dados em ativos que representam grupos de dispositivos. No diagrama anterior, você usa o mesmo modelo de ativo para todas as três turbinas porque todas as turbinas compartilham um conjunto comum de propriedades.

Você também pode criar modelos de componentes. Um modelo de componente é um tipo especial de modelo de ativo que você pode incluir em modelos de ativos ou outros modelos de componentes.

Você pode usar modelos de componentes para definir subconjuntos reutilizáveis comuns, como sensores, motores e assim por diante, que você compartilha em vários modelos de ativos.

Depois que definir os modelos de ativo, você poderá criar seus ativos industriais. Para criar um ativo, selecione um modelo de ativo do `ACTIVE` para criar um ativo a partir desse modelo. Depois, preencha as informações específicas do ativo, como apelidos e atributos do fluxo de dados. No diagrama anterior, você cria três ativos de turbina de um modelo de ativo e associa apelidos do fluxo de dados, como `/company/windfarm/3/turbine/7/temperature`, para cada turbina.

Você também pode atualizar e excluir ativos, modelos de ativos e modelos de componentes existentes. Ao atualizar um modelo de ativo, cada ativo baseado nesse modelo de ativo reflete todas as alterações feitas no modelo subjacente. Quando você atualiza um modelo de componente, isso se aplica a cada ativo com base em cada modelo de ativo que faz referência ao modelo de componente.

Seus modelos de ativos podem ser muito complexos, por exemplo, ao modelar um equipamento complicado que tem muitos subcomponentes. Para ajudar a manter esses modelos de ativos organizados e sustentáveis, você pode usar modelos compostos personalizados para agrupar propriedades relacionadas ou reutilizar componentes compartilhados. Para ter mais informações, consulte Modelos compostos personalizados (componentes).

Tópicos

Estados de ativos e modelos

Quando você cria, atualiza ou exclui um ativo, um modelo de ativo ou um modelo de componente, as alterações demoram para se propagar. AWS IoT SiteWise resolve essas operações de forma assíncrona e atualiza o status de cada recurso. Cada ativo, modelo de ativo e modelo de componente tem um campo de status que contém o estado do recurso e qualquer mensagem de erro, se aplicável. O estado pode ser um dos seguintes valores:

- `ACTIVE`— O recurso está ativo. Esse é o único estado em que você pode consultar e interagir com ativos, modelos de ativos e modelos de componentes.
- `CREATING`— O recurso está sendo criado.
- `UPDATING`— O recurso está sendo atualizado.
- `DELETING`— O recurso está sendo excluído.
- `PROPAGATING`— (Somente modelos de ativos e modelos de componentes) As mudanças estão se propagando para todos os recursos dependentes (do modelo do ativo para os ativos ou do modelo do componente para os modelos do ativo).
- `FAILED`— O recurso falhou na validação durante uma operação de criação ou atualização, possivelmente devido a uma referência circular em uma expressão. Você pode excluir recursos que estão no `FAILED` estado.

Algumas das operações de criação, atualização e exclusão AWS IoT SiteWise `ACTIVE` implementam um ativo, modelo de ativo ou modelo de componente em um estado diferente do estado em que a operação é resolvida. Para consultar ou interagir com um recurso depois de realizar uma dessas operações, você deve esperar até que o estado mude para`ACTIVE`. Caso contrário, suas solicitações falharão.

Tópicos

Verificar o status de um ativo

Você pode usar o AWS IoT SiteWise console ou a API para verificar o status de um ativo.

Tópicos

Verificar o status de um ativo (console)

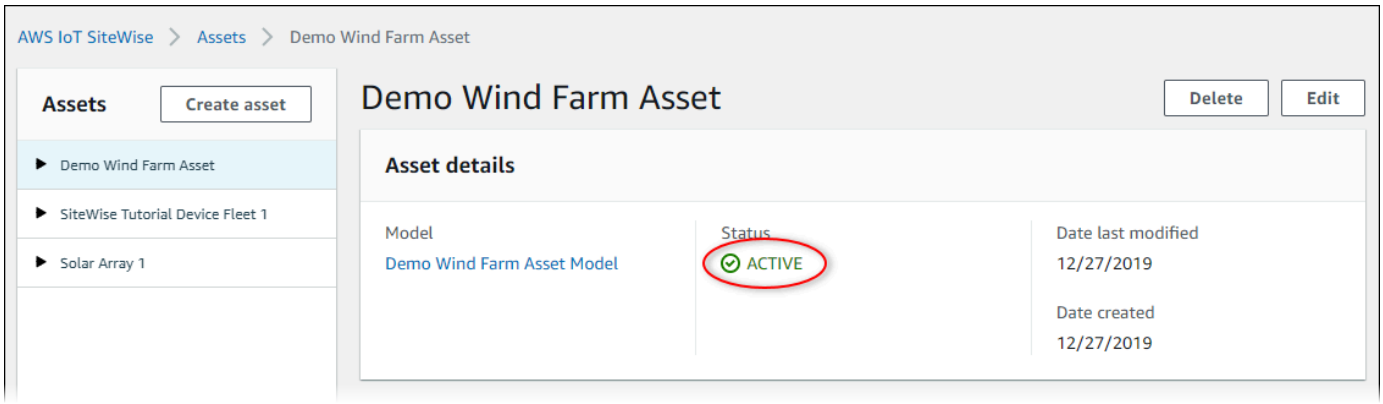
Use o procedimento a seguir para verificar o status de um ativo no console do AWS IoT SiteWise .

Como verificar o status de um ativo (console)

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Ativos.
3. Escolha o ativo a ser verificado.

> **Tip**
>
> Você pode escolher o ícone de seta para expandir uma hierarquia de ativos para localizar seu ativo.

4. Localize Status no painel Detalhes do ativo .



Verificando o status de um ativo (AWS CLI)

Você pode usar o AWS Command Line Interface (AWS CLI) para verificar o status de um ativo.

Para verificar o status de um ativo, use a DescribeAssetoperação com o `assetId` parâmetro.

Para verificar o status de um ativo (AWS CLI)

- Execute o comando a seguir para descrever o ativo. Substitua *asset-id* pelo ID do ativo ou ID externo. A ID externa é uma ID definida pelo usuário. Para obter mais informações, consulte Referenciando objetos com IDs externos no Guia de Usuário AWS IoT SiteWise .

```
aws iotsitewise describe-asset --asset-id asset-id
```

A operação retorna uma resposta que contém os detalhes do ativo. A resposta contém um `assetStatus` objeto que tem a seguinte estrutura:

```
{
    ...
    "assetStatus": {
      "state": "String",
      "error": {
         "code": "String",
         "message": "String"
      }
    }
  }
```

O estado do ativo está em `assetStatus.state` no objeto JSON.

Verificando o status de um modelo de ativo ou modelo de componente

Você pode usar o AWS IoT SiteWise console ou a API para verificar o status de um modelo de ativo ou modelo de componente.

Tópicos

- Verificando o status de um modelo de ativo ou modelo de componente (console)
- Verificando o status de um modelo de ativo ou modelo de componente (AWS CLI)

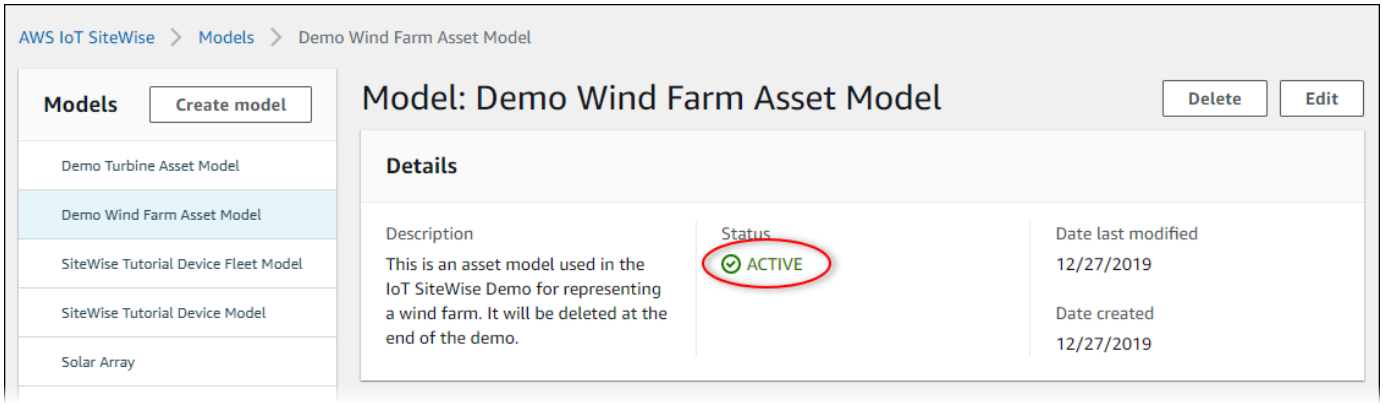
Verificando o status de um modelo de ativo ou modelo de componente (console)

Use o procedimento a seguir para verificar o status de um modelo de ativo ou modelo de componente no AWS IoT SiteWise console.

> **Tip**
>
> Os modelos de ativos e os modelos de componentes estão listados em Modelos no painel de navegação. O painel Detalhes do modelo de ativo ou modelo de componente selecionado indica de que tipo ele é.

Para verificar o status de um modelo de ativo ou modelo de componente (console)

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Modelos.
3. Escolha o modelo a ser verificado.
4. Localize Status no painel Detalhes.



Verificando o status de um modelo de ativo ou modelo de componente (AWS CLI)

Você pode usar o AWS CLI para verificar o status de um modelo de ativo ou modelo de componente.

Para verificar o status de um modelo de ativo ou modelo de componente, use a operação DescribeAssetModelo com o `assetModelId` parâmetro.

> **Tip**
>
> O AWS CLI define modelos de componentes como um tipo de modelo de ativo. Portanto, você usa a mesma operação de DescribeAssetmodelo para os dois tipos de modelo. O `assetModelType` campo na resposta indica se é um `ASSET_MODEL` ou um`COMPONENT_MODEL`.

Para verificar o status de um modelo de ativo ou modelo de componente (AWS CLI)

- Execute o comando a seguir para descrever o modelo. Substitua *asset-model-id pelo ID* ou pelo ID externo do modelo do ativo ou do modelo do componente. A ID externa é uma ID definida pelo usuário. Para obter mais informações, consulte Referenciando objetos com IDs externos no Guia de Usuário AWS IoT SiteWise .

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

  A operação retorna uma resposta que contém os detalhes do modelo. A resposta contém um objeto `assetModelStatus` com a seguinte estrutura:

  ```
  {
      ...
      "assetModelStatus": {
        "state": "String",
        "error": {
           "code": "String",
           "message": "String"
        }
      }
    }
  ```

  O estado do modelo está `assetModelStatus.state` no objeto JSON.

Modelos compostos personalizados (componentes)

Quando você está modelando um ativo industrial especialmente complexo, como uma peça de maquinário complicada que tem muitas peças, pode ser um desafio manter seus modelos de ativos organizados e sustentáveis.

Nesses casos, você pode adicionar modelos compostos personalizados, ou componentes, se estiver usando o console, aos seus modelos de ativos e modelos de componentes existentes. Isso ajuda você a se manter organizado agrupando propriedades relacionadas e reutilizando definições de subcomponentes.

Há dois tipos de modelos compostos personalizados:

- Os modelos compostos personalizados em linha definem um conjunto de propriedades agrupadas que se aplicam ao modelo de ativo ou ao modelo de componente ao qual o modelo composto personalizado pertence. Você os usa para agrupar propriedades relacionadas. Eles consistem em um nome, uma descrição e um conjunto de propriedades do modelo de ativos. Eles não são reutilizáveis.
- Modelos compostos personalizados baseados em modelos de componentes fazem referência a um modelo de componente que você deseja incluir em seu modelo de ativo ou modelo de componente. Você os usa para incluir submontagens padrão em seu modelo. Eles consistem em um nome, uma descrição e o ID do modelo de componente ao qual ele faz referência. Eles não têm propriedades próprias; o modelo de componente referenciado fornece suas propriedades associadas a qualquer ativo criado.

As seções a seguir ilustram como usar modelos compostos personalizados em seus designs.

Tópicos

Modelos compostos personalizados em linha

Modelos compostos personalizados em linha fornecem uma maneira de organizar seu modelo de ativos agrupando propriedades relacionadas.

Por exemplo, suponha que você queira modelar um ativo robótico. O robô inclui um servomotor, uma fonte de alimentação e uma bateria. Cada uma dessas partes constituintes tem suas próprias propriedades que você deseja incluir no modelo. Você pode definir um modelo de ativo chamado `robot_model` que tenha propriedades como as seguintes.

- `robot_model`
  - `servo_status` (inteiro)
  - `servo_position` (duplo)
  - `powersupply_status` (inteiro)
  - `powersupply_temperature` (duplo)

- `battery_status` (inteiro)
- `battery_charge` (duplo)

No entanto, em alguns casos, pode haver muitos subconjuntos ou os próprios subconjuntos podem ter muitas propriedades. Nesses casos, pode haver tantas propriedades que se torne difícil referenciá-las e mantê-las em uma única lista simples na raiz do modelo, como no exemplo anterior.

Para lidar com essas situações, você pode usar um modelo composto personalizado embutido para agrupar propriedades. Um modelo composto personalizado em linha é um modelo composto personalizado que define suas próprias propriedades. Por exemplo, você pode modelar seu robô da seguinte forma.

- `robot_model`
  - `servo`
    - `status`(inteiro)
    - `position`(duplo)
  - `powersupply`
    - `status`(inteiro)
    - `temperature` (duplo)
  - `battery`
    - `status`(inteiro)
    - `charge`(duplo)

No exemplo anterior,, `servopowersupply`, e `battery` estão os nomes dos modelos compostos personalizados em linha definidos no `robot_model` modelo de ativo. Cada um desses modelos compostos então define suas próprias propriedades.

> **Note**
>
> Nesse caso, cada modelo composto personalizado define suas próprias propriedades, de forma que todas as propriedades façam parte do próprio modelo de ativo (`robot_model`nesse caso). Essas propriedades não são compartilhadas com nenhum outro modelo de ativo ou modelo de componente. Por exemplo, se você criasse algum outro modelo de ativo que também tivesse um modelo composto personalizado em linha

chamado`servo`, fazer uma alteração `servo` no interior não `robot_model` afetaria a definição do outro modelo de `servo` ativo.
Se você quiser implementar esse compartilhamento (por exemplo, ter apenas uma definição para um servo, que todos os seus modelos de ativos possam compartilhar), crie um modelo de componente para ele e, em seguida, crie modelos compostos baseados em modelos de componentes que façam referência a ele. Consulte a seção a seguir para obter detalhes.

Para obter informações sobre como criar modelos compostos personalizados em linha, consulte. Criação de modelos compostos personalizados (componentes)

C: omponent-model-based modelos compostos personalizados

Você pode criar um modelo de componente AWS IoT SiteWise para definir uma submontagem padrão reutilizável. Depois de criar um modelo de componente, você pode adicionar referências a ele em seus outros modelos de ativos e modelos de componentes. Você faz isso adicionando um modelo composto component-model-based personalizado a qualquer modelo em que queira referenciar o componente. Você pode adicionar referências ao seu componente de vários modelos ou várias vezes no mesmo modelo.

Dessa forma, você pode evitar a duplicação das mesmas definições nos modelos. Isso também simplifica a manutenção de seus modelos, porque todas as alterações feitas em um modelo de componente serão refletidas em todos os modelos de ativos que o utilizam.

Por exemplo, suponha que sua instalação industrial tenha muitos tipos de equipamentos que usam o mesmo tipo de servomotor. Alguns deles têm muitos servomotores em um único equipamento. Você cria um modelo de ativo para cada tipo de equipamento, mas não quer duplicar a definição de `servo` cada vez. Você deseja modelá-lo apenas uma vez e usá-lo em seus vários modelos de ativos. Se, posteriormente, você fizer uma alteração na definição de`servo`, ela será atualizada em todos os seus modelos e ativos.

Para modelar o robô do exemplo anterior dessa forma, você pode definir servomotores, fontes de alimentação e baterias como modelos de componentes, desta forma.

- `servo_component_model`
  - `status`(inteiro)
  - `position`(duplo)

- powersupply_component_model
  - status(inteiro)
  - temperature (duplo)

- battery__component_model
  - status(inteiro)
  - charge(duplo)

Você poderia então definir modelos de ativosrobot_model, como os que fazem referência a esses componentes. Vários modelos de ativos podem referenciar o mesmo modelo de componente. Você também pode referenciar o mesmo modelo de componente várias vezes em um modelo de ativo, como se seu robô tivesse vários servomotores.

- robot_model
  - servo1(referência:servo_component_model)
  - servo2(referência:servo_component_model)
  - servo3(referência:servo_component_model)
  - powersupply (referência:powersupply_component_model)
  - battery(referência:battery_component_model)

Para obter informações sobre como criar modelos de componentes, consulteCriação de modelos de componentes.

Para obter informações sobre como referenciar seus modelos de componentes em outros modelos, consulteCriação de modelos compostos personalizados (componentes).

Usando caminhos para referenciar propriedades personalizadas do modelo composto

Ao criar uma propriedade em um modelo de ativo, modelo de componente ou modelo composto personalizado, você pode referenciá-la a partir de outras propriedades que usam seu valor, como transformações e métricas.

AWS IoT SiteWise fornece maneiras diferentes para você referenciar sua propriedade. A maneira mais simples geralmente é usar o ID da propriedade. No entanto, se a propriedade que você deseja referenciar estiver em um modelo composto personalizado, talvez seja mais útil referenciá-la por caminho.

Um caminho é uma sequência ordenada de segmentos de caminho que especifica uma propriedade em termos de sua posição entre os modelos compostos aninhados em um modelo de ativo e modelo composto.

Obtendo caminhos imobiliários

Você pode obter o caminho de uma propriedade no `path` campo de sua AssetModelpropriedade.

Por exemplo, suponha que você tenha um modelo de ativo `robot_model` que contém um modelo composto personalizado`servo`, que tem uma propriedade`position`. Se você chamar DescribeAssetModelCompositeModel on`servo`, a `position` propriedade listará um `path` campo parecido com este:

```
"path": [
    {
       "id": "asset model ID",
       "name": "robot_model"
    },
    {
       "id": "composite model ID",
       "name": "servo"
    },
    {
       "id": "property ID",
       "name": "position"
    }
]
```

Usando caminhos de propriedades

Você pode usar um caminho de propriedade ao definir uma propriedade que faz referência a outras propriedades, como uma transformação ou métrica.

Uma propriedade usa uma variável para referenciar outra propriedade. Para obter mais informações sobre como trabalhar com variáveis, consulteUsando variáveis em expressões de fórmulas.

Ao definir uma variável para referenciar uma propriedade, você pode usar o ID da propriedade ou seu caminho.

Para definir uma variável que usa o caminho da propriedade referenciada, especifique o `propertyPath` campo de seu valor.

Por exemplo, para definir um modelo de ativo que tenha uma métrica que faça referência a uma propriedade usando um caminho, você pode passar uma carga útil como essa para CreateAssetModel:

```
{
    ...
    "assetModelProperties": [
        {
            ...
            "type": {
                "metric": {
                    ...
                    "variables": [
                        {
                            "name": "variable name",
                            "value": {
                                "propertyPath": [
                                    path segments
                                ]
                            }
                        }
                    ],
                    ...
                }
            },
            ...
        },
        ...
    ],
    ...
}
```

Trabalhando com IDs de objetos

AWS IoT SiteWise define vários tipos de objetos persistentes, como ativos, modelos de ativos, propriedades e hierarquias. Todos esses objetos têm identificadores exclusivos que você pode usar para recuperá-los, atualizá-los e excluí-los.

AWS IoT SiteWise tem opções diferentes para os clientes criarem identidades. AWS IoT SiteWise gera um para você por padrão no momento da criação do objeto. Os usuários também podem fornecer seus próprios IDs para seus objetos.

Tópicos

Trabalhando com UUIDs de objetos

Cada objeto persistente AWS IoT SiteWise tem um UUID para identificá-lo. Por exemplo, modelos de ativos têm uma ID de modelo de ativo, ativos têm uma ID de ativo e assim por diante. Essa ID é atribuída no momento em que você cria o objeto e permanece inalterada durante a vida útil do objeto.

Quando você cria um novo objeto, AWS IoT SiteWise gera um ID exclusivo para você por padrão. Você também pode fornecer seu próprio ID no momento da criação no formato UUID.

> **Note**
>
> Os UUIDs devem ser globalmente exclusivos na AWS região em que foram criados e para o mesmo tipo de objeto. Quando AWS IoT SiteWise gera automaticamente um ID para você, ele é sempre exclusivo. Se você escolher seu próprio documento de identidade, verifique se ele é exclusivo.

Por exemplo, se você criar um novo modelo de ativo chamando CreateAssetModel, poderá fornecer seu próprio UUID no `assetModelId` campo opcional da solicitação.

Por outro lado, se você omitir `assetModelId` da solicitação, AWS IoT SiteWise gera um UUID para o novo modelo de ativo.

Usando IDs externos

Para definir seu próprio ID em algum formato diferente do UUID, você pode atribuir um ID externo. Por exemplo, você pode fazer isso se reutilizar um ID que está usando em um sistema que não está AWS, ou para ser mais legível por humanos. Os IDs externos têm um formato mais flexível. Você pode usá-los para referenciar seus objetos em operações de AWS IoT SiteWise API em que, de outra forma, usaria o UUID.

Assim como os UUIDs, cada ID externa deve ser exclusiva dentro de seu contexto. Por exemplo, você não pode ter dois modelos de ativos com a mesma ID externa. Além disso, como os UUIDs, um objeto só pode ter um ID externo em sua vida útil, que não pode mudar.

Diferenças entre IDs externos e UUIDs

Os IDs externos diferem dos UUIDs das seguintes maneiras:

- Cada objeto tem um UUID, mas os IDs externos são opcionais.
- AWS IoT SiteWise nunca gera IDs externos. Você mesmo os fornece.
- Se o objeto ainda não tiver uma, você poderá atribuir uma ID externa a qualquer momento.

Formato de IDs externos

Uma ID externa válida tem as seguintes propriedades:

- Tem entre 2 e 128 caracteres.
- O primeiro e o último caracteres devem ser alfanuméricos (A-Z, a-z, 0-9).
- Caracteres diferentes do primeiro e do último devem ser alfanuméricos, ou então um dos seguintes: `_-.:`

Por exemplo, uma ID externa deve estar em conformidade com a seguinte expressão regular:

```
[a-zA-Z0-9][a-zA-Z0-9_\-.:]*[a-zA-Z0-9]+
```

Referenciando objetos com IDs externos

Em muitos lugares em que você pode referenciar um objeto usando seu UUID, você pode usar seu ID externo em vez disso, se ele tiver um. Para fazer isso, anexe o ID externo à string. `externalId:`

Por exemplo, suponha que você tenha um modelo de ativo cujo UUID (ID do modelo de ativo) seja`a1b2c3d4-5678-90ab-cdef-11111EXAMPLE`, que também tenha o ID externo. `myExternalId` Ligue para a DescribeAssetModel para obter detalhes sobre isso. Você pode usar qualquer um dos seguintes como o valor de`assetModelId`:

- Com o ID do modelo de ativo (UUID) em si: `a1b2c3d4-5678-90ab-cdef-11111EXAMPLE`
- Com o 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**
>
> O `externalId:` prefixo não é, por si só, parte do ID externo. Você só precisa fornecer o prefixo ao fornecer um ID externo a uma operação de API que aceite UUIDs ou IDs externos. Por exemplo, forneça o prefixo ao consultar ou atualizar um objeto existente.
> Ao definir uma ID externa para um objeto, como ao criar um modelo de ativo, não inclua o prefixo.

Você pode usar IDs externos no lugar dos UUIDs dessa forma para muitas operações de API em AWS IoT SiteWise, mas não em todas. Por exemplo, o GetAssetPropertyValue, deve usar UUIDs; ele não suporta o uso de ID externo.

Para determinar se uma operação de API específica é compatível com esse uso, consulte a Referência da API.

Criação de modelos de ativos e modelos de componentes

AWS IoT SiteWise modelos de ativos e modelos de componentes impulsionam a padronização de seus dados industriais. Um modelo de ativo ou modelo de componente contém um nome, descrição, propriedades do ativo e (opcionalmente) modelos compostos personalizados que agrupam propriedades ou que fazem referência a modelos de componentes para submontagens.

- Você usa um modelo de ativo para criar ativos. Além dos recursos listados acima, um modelo de ativo também pode conter definições de hierarquia que definem relacionamentos entre ativos.

- Um modelo de componente representa uma submontagem dentro de um modelo de ativo ou outro modelo de componente. Ao criar um modelo de componente, você pode adicionar referências a ele em modelos de ativos e em outros modelos de componentes. No entanto, você não pode criar ativos diretamente dos modelos de componentes.

Depois de criar um modelo de ativo ou modelo de componente, você pode criar modelos compostos personalizados para agrupar propriedades ou referenciar modelos de componentes existentes.

Para obter detalhes sobre como criar modelos de ativos e modelos de componentes, consulte as seções a seguir.

Tópicos

Criar modelos de ativo

AWS IoT SiteWise modelos de ativos impulsionam a padronização de seus dados industriais. Um modelo de ativo contém um nome, uma descrição, propriedades do ativo e definições da hierarquia de ativos. Por exemplo, você pode definir um modelo de turbina eólica com temperatura, rotações por minuto (RPM) e propriedades de energia. Depois, você define um modelo de parque eólico com uma propriedade de saída de energia útil e uma definição de hierarquia de turbinas eólicas.

> **Note**
>
> - Recomendamos modelar sua operação começando com os nós de nível mais baixo. Por exemplo, crie seu modelo de turbina eólica antes de criar seu modelo de parque eólico. As definições de hierarquia de ativos contêm referências a modelos de ativos existentes. Com essa abordagem, você pode definir hierarquias de ativos conforme cria seus modelos.
> - Os modelos de ativos não podem conter outros modelos de ativos. Se você precisar definir um modelo que possa ser referenciado como uma submontagem em outro modelo, crie um modelo de componente -> em vez disso. Para ter mais informações, consulte Criação de modelos de componentes.

As seções a seguir descrevem como usar o AWS IoT SiteWise console ou a API para criar modelos de ativos. As seções a seguir também descrevem os diferentes tipos de propriedades e hierarquias de ativos que você pode usar para criar modelos.

Tópicos

Criar um modelo de ativo (console)

Você pode usar o AWS IoT SiteWise console para criar um modelo de ativo. O AWS IoT SiteWise console fornece vários recursos, como preenchimento automático de fórmulas, que podem ajudá-lo a definir modelos de ativos válidos.

Como criar um modelo de ativo (console)

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Modelos.
3. Escolha Criar modelo.
4. Na página Criar modelo, faça o seguinte:

    a. Insira um Nome para o modelo de ativo, como **`Wind Turbine`** ou **`Wind Turbine Model`**. Esse nome deve ser exclusivo em todos os modelos de sua conta nesta região.

    b. (Opcional) Adicione uma ID externa para o modelo. Esse é um ID definido pelo usuário. Para obter mais informações, consulte Referenciando objetos com IDs externos no Guia de Usuário AWS IoT SiteWise .

    c. (Opcional) Adicione Definições de medição ao modelo. As medições representam fluxos de dados do seu equipamento. Para ter mais informações, consulte Definindo fluxos de dados do equipamento (medições).

    d. (Opcional) Adicione Definições de transformação ao modelo. As transformações são fórmulas que mapeiam dados de um formulário para outro. Para ter mais informações, consulte Transformando dados (transformações).

    e. (Opcional) Adicione Definições de métrica ao modelo. Métricas são fórmulas que agregam dados em intervalos de tempo. As métricas podem inserir dados de entrada de ativos

associados, para que você possa calcular valores que representem sua operação ou um subconjunto de sua operação. Para ter mais informações, consulte Agregando dados de propriedades e outros ativos (métricas).

f. (Opcional) Adicione Definições de hierarquia ao modelo. Hierarquias são relacionamentos entre ativos. Para ter mais informações, consulte Definindo hierarquias de modelos de ativos.

g. (Opcional) Adicione tags ao modelo de ativo. Para ter mais informações, consulte Marcando seus recursos AWS IoT SiteWise.

h. Escolha Criar modelo.

Quando você cria um modelo de ativo, o AWS IoT SiteWise console navega até a página do novo modelo. Nessa página, você pode ver o Status do modelo que, inicialmente, é CRIANDO. Essa página é atualizada automaticamente, para que você possa aguardar a atualização do status do modelo.

> **Note**
>
> O processo de criação do modelo de ativo pode levar alguns minutos para modelos complexos. Depois que o status do modelo de ativo for ATIVADO, você poderá usá-lo para criar ativos. Para ter mais informações, consulte Estados de ativos e modelos.

5. (Opcional) Depois de criar seu modelo de ativo, você pode configurá-lo para a borda. Para obter mais informações sobre o SiteWise Edge, consulteHabilitar o processamento de dados de borda.

   a. Na página do modelo, escolha Configurar para Edge.

   b. Na página de configuração do modelo, escolha a configuração de borda para seu modelo. Isso controla onde é AWS IoT SiteWise possível calcular e armazenar propriedades associadas a esse modelo de ativo. Para obter mais informações sobre como configurar seu modelo para a borda, consulte the section called “Configurar o recurso de borda”.

   c. Para Configuração de borda personalizada, escolha o local que você deseja AWS IoT SiteWise calcular e armazenar cada uma das propriedades do seu modelo de ativo.

> **Note**
>
> As transformações e métricas associadas devem ser configuradas para o mesmo local. Para obter mais informações sobre como configurar seu modelo para a borda, consulte the section called “Configurar o recurso de borda”.

d. Selecione Save (Salvar). Na página do modelo, sua configuração do Edge agora deve estar Configurada.

Criação de um modelo de ativo (AWS CLI)

Você pode usar o AWS Command Line Interface (AWS CLI) para criar um modelo de ativo.

Use a operação CreateAssetModelo para criar um modelo de ativo com propriedades e hierarquias. Essa operação espera uma carga útil com a seguinte estrutura.

```
{
  "assetModelType": "ASSET_MODEL",
  "assetModelName": "String",
  "assetModelDescription": "String",
  "assetModelProperties": Array of AssetModelProperty,
  "assetModelHierarchies": Array of AssetModelHierarchyDefinition
}
```

Para criar um modelo de ativo (AWS CLI)

1. Crie um arquivo chamado `asset-model-payload.json` e copie o objeto JSON a seguir no arquivo.

```
{
  "assetModelType": "ASSET_MODEL",
  "assetModelName": "",
  "assetModelDescription": "",
  "assetModelProperties": [

  ],
  "assetModelHierarchies": [

  ],
  "assetModelCompositeModels": [
```

```
  ]
}
```

2. Use seu editor de texto JSON preferido para editar o arquivo `asset-model-payload.json` para o seguinte:

   a. Insira um nome (`assetModelName`) para o modelo de ativo, como **`Wind Turbine`** ou **`Wind Turbine Model`**. Nesse caso, esse nome deve ser exclusivo em todos os modelos de ativos e modelos de componentes da sua conta Região da AWS.

   b. (Opcional) Insira uma ID externa (`assetModelExternalId`) para o modelo de ativo. Esse é um ID definido pelo usuário. Para obter mais informações, consulte Referenciando objetos com IDs externos no Guia de Usuário AWS IoT SiteWise .

   c. (Opcional) Insira uma descrição (`assetModelDescription`) para o modelo de ativo ou remova o par de chave-valor `assetModelDescription`.

   d. (Opcional) Defina as propriedades do ativo (`assetModelProperties`) para o modelo. Para ter mais informações, consulte Definir propriedades de dados.

   e. (Opcional) Defina hierarquias de ativos (`assetModelHierarchies`) para o modelo. Para ter mais informações, consulte Definindo hierarquias de modelos de ativos.

   f. (Opcional) Defina alarmes para o modelo. Os alarmes monitoram outras propriedades para que você possa identificar quando equipamentos ou processos requerem atenção. Cada definição de alarme é um modelo composto (`assetModelCompositeModels`) que padroniza o conjunto de propriedades usado pelo alarme. Para obter mais informações, consulte Monitorar dados com alarmes e Definir alarmes em modelos de ativos.

   g. (Opcional) Adicione tags (`tags`) ao modelo de ativo. Para ter mais informações, consulte Marcando seus recursos AWS IoT SiteWise.

3. Execute o seguinte comando para criar um modelo de ativo usando a definição no arquivo JSON.

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

   A operação retorna uma resposta que contém o `assetModelId` ao qual você faz referência ao criar um ativo. A resposta também contém o estado do modelo (`assetModelStatus.state`) que, inicialmente, é `CREATING`. O status do modelo de ativo é `CREATING` até que as alterações sejam propagadas.

> **Note**
>
> O processo de criação do modelo de ativo pode levar alguns minutos para modelos complexos. Para verificar o status atual do seu modelo de ativo, use a operação DescribeAssetModelo especificando o. `assetModelId` Depois que o status do modelo de ativo for `ACTIVE`, você poderá usá-lo para criar ativos. Para ter mais informações, consulte Estados de ativos e modelos.

4. (Opcional) Crie modelos compostos personalizados para seu modelo de ativo. Com modelos compostos personalizados, você pode agrupar propriedades dentro do modelo ou incluir uma submontagem fazendo referência a um modelo de componente. Para ter mais informações, consulte Criação de modelos compostos personalizados (componentes).

Exemplos de modelos de ativos

Esta seção contém exemplos de definições de modelos de ativos que você pode usar para criar modelos de ativos com os AWS IoT SiteWise SDKs AWS CLI e. Esses modelos de ativos representam uma turbina eólica e um parque eólico. Os ativos da turbina eólica ingerem dados brutos do sensor e calculam valores como potência e velocidade média do vento. Os ativos do parque eólico calculam valores como a potência total de todas as turbinas eólicas do parque eólico.

Tópicos

- Modelo de ativo de turbina eólica
- Modelo de ativo de parque eólico

Modelo de ativo de turbina eólica

O modelo de ativo a seguir representa uma turbina em um parque eólico. A turbina eólica ingere dados do sensor para calcular valores como potência e velocidade média do vento.

> **Note**
>
> Este modelo de exemplo se assemelha ao modelo de turbina eólica da AWS IoT SiteWise demonstração. Para ter mais informações, consulte Usando a AWS IoT SiteWise demonstração.

```
{
  "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 ativo de parque eólico

O modelo de ativo a seguir representa um parque eólico que é composto por várias turbinas eólicas. Esse modelo de ativos define uma hierarquia para o modelo de turbina eólica. Isso permite que o parque eólico calcule valores (como potência média) a partir dos dados de todas as turbinas eólicas do parque eólico.

> **Note**
>
> Esse modelo de exemplo se assemelha ao modelo de parque eólico da AWS IoT SiteWise demonstração. Para ter mais informações, consulte Usando a AWS IoT SiteWise demonstração.

Esse modelo de ativo depende do Modelo de ativo de turbina eólica. Substitua os valores de `childAssetModelId` e `propertyId` por aqueles de um modelo de ativo de turbina eólica existente.

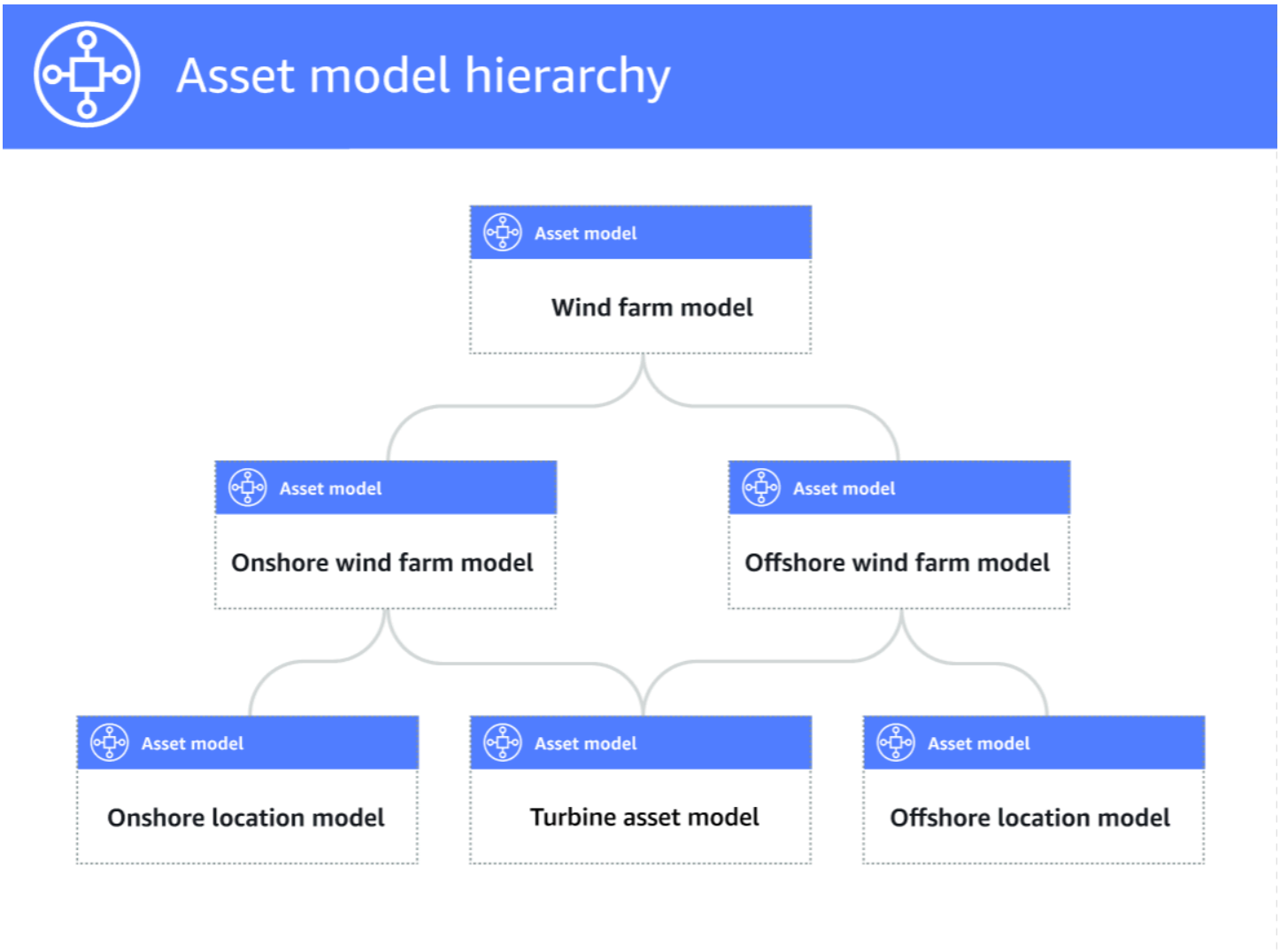
```
{
  "assetModelName": "Wind Farm Asset Model",
```

```
  "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"
    }
  ]
}
```

Definindo hierarquias de modelos de ativos

Você pode definir hierarquias de modelos de ativos para criar associações lógicas entre os modelos de ativos em sua operação industrial. Por exemplo, você pode definir um parque eólico composto de parques eólicos terrestres e de deslocamento. Um parque eólico terrestre contém uma turbina e uma localização em terra. Um parque eólico offshore contém uma turbina e uma localização em deslocamento.



Quando um modelo de ativo filho é associado a um modelo de ativo pai por meio de uma hierarquia, as métricas modelo do ativo pai podem receber dados de entrada das métricas do modelo do ativo filho. Você pode usar hierarquias e métricas de modelo de ativos para calcular estatísticas que forneçam informações sobre sua operação ou sobre um subconjunto da operação. Para ter mais informações, consulte Agregando dados de propriedades e outros ativos (métricas).

Cada hierarquia define uma relação entre um modelo de ativo pai (e um modelo de ativo filho. Em um modelo de ativo pai, você pode definir várias hierarquias para o mesmo modelo de ativo filho. Por exemplo, se você tiver dois tipos diferentes de turbinas em seus parques eólicos, onde todas as turbinas eólicas forem representadas pelo mesmo modelo de ativo, você poderá definir uma hierarquia para cada tipo. Em seguida, você pode definir métricas no modelo de parque eólico para calcular estatísticas independentes e combinadas para cada tipo de turbina eólica.

Um modelo de ativo pai pode ser associado a vários modelos de ativos filho. Por exemplo, se você tem um parque eólico terrestre e um parque eólico remoto representados por dois modelos de ativos diferentes, você pode associar esses modelos de ativos ao mesmo modelo de ativo pai do parque eólico.

Um modelo de ativo filho pode ser associado a vários modelos de ativos filho. Por exemplo, se você tiver dois tipos diferentes de parques eólicos, onde todas as turbinas eólicas são representadas pelo mesmo modelo de ativo, você pode associar o modelo de ativo de turbina eólica a diferentes modelos de ativos de parques eólicos.

> **Note**
>
> Quando você define uma hierarquia de modelo de ativos, o modelo de ativo filho deve ser `ACTIVE` ou ter uma versão `ACTIVE` anterior. Para ter mais informações, consulte Estados de ativos e modelos.

Depois de definir modelos de ativos hierárquicos e criar ativos, você pode associar os ativos para concluir o relacionamento pai-filho. Para obter mais informações, consulte Criação de ativos e Associar e desassociar ativos.

Tópicos

- Definir hierarquias de modelos de ativos (console)
- Definindo hierarquias de ativos ()AWS CLI

Definir hierarquias de modelos de ativos (console)

Ao definir uma hierarquia para um modelo de ativo no AWS IoT SiteWise console, você especifica os seguintes parâmetros:

- Nome da hierarquia — nome da hierarquia, como **`Wind Turbines`**.

- Modelo de hierarquia — modelo de ativo filho.
- ID externa da hierarquia (opcional) — Essa é uma ID definida pelo usuário. Para obter mais informações, consulte Referenciando objetos com IDs externos no Guia de Usuário AWS IoT SiteWise .

Para ter mais informações, consulte Criar um modelo de ativo (console).

Definindo hierarquias de ativos ()AWS CLI

Ao definir uma hierarquia para um modelo de ativo com a AWS IoT SiteWise API, você especifica os seguintes parâmetros:

- `name` — nome da hierarquia, como **`Wind Turbines`**.
- `childAssetModelId`— O ID ou o ID externo do modelo de ativo secundário para a hierarquia. Você pode usar a operação ListAssetModelos para encontrar a ID de um modelo de ativo existente.

Example Exemplo de definição de hierarquia

O exemplo a seguir demonstra uma hierarquia de ativos que representa o relacionamento de um parque eólico com as turbinas eólicas. Esse objeto é um exemplo de AssetModelhierarquia. Para ter mais informações, consulte Criação de um modelo de ativo (AWS CLI).

```
{
  ...
  "assetModelHierarchies": [
    {
      "name": "Wind Turbines",
      "childAssetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE"
    },
  ]
}
```

Criação de modelos de componentes

Use modelos de AWS IoT SiteWise componentes para definir submontagens que você pode referenciar a partir de modelos de ativos ou outros modelos de componentes. Dessa forma, você pode reutilizar a definição do componente em vários outros modelos ou várias vezes no mesmo modelo.

O processo de definição de um modelo de componente é muito semelhante à definição de um modelo de ativo. Assim como um modelo de ativo, um modelo de componente tem nome, descrição e propriedades de ativos. No entanto, os modelos de componentes não podem incluir definições de hierarquia de ativos, pois os modelos de componentes em si não podem ser usados para criar ativos diretamente. Os modelos de componentes também não podem definir alarmes.

Por exemplo, você pode definir um componente para um servomotor com propriedades de temperatura do motor, temperatura do codificador e resistência de isolamento. Em seguida, você pode definir um modelo de ativo para equipamentos que contenham servomotores, como uma máquina CNC.

> **Note**
>
> - Recomendamos modelar sua operação começando com os nós de nível mais baixo. Por exemplo, crie seu componente de servomotor antes de criar o modelo de ativos de sua máquina CNC. Os modelos de ativos contêm referências aos modelos de componentes existentes.
> - Você não pode criar um ativo diretamente de um modelo de componente. Para criar um ativo que usa seu componente, você deve criar um modelo de ativo para seu ativo. Em seguida, você cria um modelo composto personalizado para ele que faz referência ao seu componente. Para obter mais informações sobre a criação de modelos de ativos, consulte Criar modelos de ativo Para obter mais informações sobre a criação de modelos compostos personalizados, consulteCriação de modelos compostos personalizados (componentes).

As seções a seguir descrevem como usar a AWS IoT SiteWise API para criar modelos de componentes.

Tópicos

- Criando um modelo de componente (AWS CLI)
- Exemplo de modelo de componente

Criando um modelo de componente (AWS CLI)

Você pode usar o AWS Command Line Interface (AWS CLI) para criar um modelo de componente.

Use a operação CreateAssetModel para criar um modelo de componente com propriedades. Essa operação espera uma carga útil com a seguinte estrutura:

```
{
  "assetModelType": "COMPONENT_MODEL",
  "assetModelName": "String",
  "assetModelDescription": "String",
  "assetModelProperties": Array of AssetModelProperty,
}
```

Para criar um modelo de componente (AWS CLI)

1. Crie um arquivo chamado `component-model-payload.json` e, em seguida, copie o seguinte objeto JSON no arquivo:

   ```
   {
     "assetModelType": "COMPONENT_MODEL",
     "assetModelName": "",
     "assetModelDescription": "",
     "assetModelProperties": [

     ]
   }
   ```

2. Use seu editor de texto JSON preferido para editar o arquivo `component-model-payload.json` para o seguinte:

   a. Insira um nome (`assetModelName`) para o modelo do componente, como **`Servo Motor`** ou**`Servo Motor Model`**. Nesse caso, esse nome deve ser exclusivo em todos os modelos de ativos e modelos de componentes da sua conta Região da AWS.

   b. (Opcional) Insira uma ID externa (`assetModelExternalId`) para o modelo do componente. Esse é um ID definido pelo usuário. Para obter mais informações, consulte Referenciando objetos com IDs externos no Guia de Usuário AWS IoT SiteWise .

   c. (Opcional) Insira uma descrição (`assetModelDescription`) para o modelo de ativo ou remova o par de chave-valor `assetModelDescription`.

   d. (Opcional) Defina as propriedades do ativo (`assetModelProperties`) para o modelo do componente. Para ter mais informações, consulte Definir propriedades de dados.

   e. (Opcional) Adicione tags (`tags`) ao modelo de ativo. Para ter mais informações, consulte Marcando seus recursos AWS IoT SiteWise.

3. Execute o comando a seguir para criar um modelo de componente a partir da definição no arquivo JSON.

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

A operação retorna uma resposta que contém a `assetModelId` que você se refere ao adicionar uma referência ao seu modelo de componente em um modelo de ativo ou outro modelo de componente. A resposta também contém o estado do modelo (`assetModelStatus.state`) que, inicialmente, é `CREATING`. O status do modelo do componente é `CREATING` até que as alterações se propaguem.

> **Note**
>
> O processo de criação do modelo de componente pode levar alguns minutos para modelos complexos. Para verificar o status atual do seu modelo de componente, use a operação DescribeAssetModelo especificando o. `assetModelId` Depois que o status do modelo de componente for`ACTIVE`, você poderá adicionar referências ao seu modelo de componente em modelos de ativos ou outros modelos de componentes. Para ter mais informações, consulte Estados de ativos e modelos.

4. (Opcional) Crie modelos compostos personalizados para seu modelo de componente. Com modelos compostos personalizados, você pode agrupar propriedades dentro do modelo ou incluir uma submontagem fazendo referência a outro modelo de componente. Para ter mais informações, consulte Criação de modelos compostos personalizados (componentes).

Exemplo de modelo de componente

Esta seção contém um exemplo de definição de modelo de componente que você pode usar para criar um modelo de componente com os AWS IoT SiteWise SDKs AWS CLI e. Este modelo de componente representa um servomotor que pode ser usado em outro equipamento, como uma máquina CNC.

Tópicos

- Modelo de componente de servomotor

Modelo de componente de servomotor

O modelo de componente a seguir representa um servomotor que pode ser usado em equipamentos como máquinas CNC. O servomotor fornece várias medidas, como temperaturas e resistência elétrica. Essas medições estão disponíveis como propriedades em ativos criados a partir de modelos de ativos que fazem referência ao modelo de componentes do 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"
        }
    ]
}
```

Definir propriedades de dados

As propriedades do ativo são as estruturas em cada ativo que contêm dados do mesmo. As propriedades do ativo podem ser qualquer de um dos seguintes tipos:

- Atributos – propriedades geralmente estáticas de um ativo, como fabricante do dispositivo ou região geográfica. Para ter mais informações, consulte Definindo dados estáticos (atributos).
- Medições – fluxos de dados brutos do sensor de um dispositivo de um ativo, como valores de velocidade de rotação com time stamp ou valores de temperatura com time stamp em Celsius. Uma medição é definida por um apelido de fluxo de dados. Para ter mais informações, consulte Definindo fluxos de dados do equipamento (medições).

- Transformações – valores transformados de séries temporais de um ativo, como valores de temperatura com time stamp em Fahrenheit. Uma transformação é definida por uma expressão e as variáveis a serem consumidas com essa expressão. Para ter mais informações, consulte Transformando dados (transformações).
- Métricas – dados de um ativo agregados em um intervalo de tempo especificado, como a temperatura média por hora. Uma métrica é definida por um intervalo de tempo, uma expressão e as variáveis a serem consumidas com essa expressão. As expressões métricas podem inserir as propriedades métricas dos ativos associados, para que você possa calcular métricas que representem sua operação ou um subconjunto de sua operação. Para ter mais informações, consulte Agregando dados de propriedades e outros ativos (métricas).

Para ter mais informações, consulte Criar modelos de ativo.

Para obter um exemplo de como usar medições, transformações e métricas para calcular a Eficácia Geral do Equipamento (OEE), consulte Calculando o OEE em AWS IoT SiteWise.

Tópicos

- Definindo dados estáticos (atributos)
- Definindo fluxos de dados do equipamento (medições)
- Transformando dados (transformações)
- Agregando dados de propriedades e outros ativos (métricas)
- Usando expressões de fórmula

Definindo dados estáticos (atributos)

Os Ativos dos atributos representam informações geralmente estáticas, como o fabricante do dispositivo ou a localização geográfica. Cada ativo criado a partir de um modelo de ativo contém os atributos desse modelo.

Tópicos

- Definir atributos (console)
- Definindo atributos (AWS CLI)

Definir atributos (console)

Ao definir um atributo para um modelo de ativo no AWS IoT SiteWise console, você especifica os seguintes parâmetros:

- Nome — o nome da propriedade.
- Valor padrão – (opcional) o valor predefinido para este atributo. Os ativos criados a partir do modelo têm esse valor para o atributo. Para obter mais informações sobre como substituir o valor predefinido em um ativo criado a partir de um modelo, consulte Atualizar valores de atributo.
- Tipo de dado — o tipo de dado da propriedade, que é um dos seguintes:
  - String – uma string com até 1024 bytes.
  - Número inteiro – um número inteiro assinado de 32 bits com intervalo [-2.147.483.648, 2.147.483.647].
  - Duplo – um número de ponto flutuante com intervalo [-10^100, 10^100] e precisão dupla IEEE 754.
  - Booleano — `true` ou `false`.
- ID externa — (Opcional) Essa é uma ID definida pelo usuário. Para obter mais informações, consulte Referenciando objetos com IDs externos no Guia de Usuário AWS IoT SiteWise .

Para ter mais informações, consulte Criar um modelo de ativo (console).

Definindo atributos (AWS CLI)

Ao definir um atributo para um modelo de ativo com a AWS IoT SiteWise API, você especifica os seguintes parâmetros:

- `name` – o nome da propriedade.
- `defaultValue` – (opcional) o valor padrão para este atributo. Os ativos criados a partir do modelo têm esse valor para o atributo. Para obter mais informações sobre como substituir o valor predefinido em um ativo criado a partir de um modelo, consulte Atualizar valores de atributo.
- `dataType`— o tipo de dado da propriedade, que é um dos seguintes:
  - `STRING` – uma string com até 1024 bytes.
  - `INTEGER` – um número inteiro assinado de 32 bits com intervalo [-2.147.483.648, 2.147.483.647].
  - `DOUBLE` – um número de ponto flutuante com intervalo [-10^100, 10^100] e precisão dupla IEEE 754.

  - `BOOLEAN` – `true` ou `false`.
- `externalId`— (Opcional) Essa é uma ID definida pelo usuário. Para obter mais informações, consulte Referenciando objetos com IDs externos no Guia de Usuário AWS IoT SiteWise .

Example Exemplo de definição de atributo

O exemplo a seguir demonstra um atributo que representa o número de um modelo de ativo com um valor padrão. Esse objeto é um exemplo de uma AssetModelpropriedade que contém um atributo. Você pode especificar esse objeto como parte da carga de solicitação de CreateAssetmodelo para criar uma propriedade de atributo. Para ter mais informações, consulte Criação de um modelo de ativo (AWS CLI).

```
{
...
"assetModelProperties": [
{
  "name": "Model number",
  "dataType": "STRING",
  "type": {
    "attribute": {
      "defaultValue": "BLT123"
    }
  }
}
],
...
}
```

Definindo fluxos de dados do equipamento (medições)

Uma medição representa o fluxo de dados brutos do sensor de um dispositivo, como valores de temperatura com time stamp ou valores de rotação com time stamp por minuto (RPM).

Tópicos

- Definindo medições (console)
- Definindo medidas (AWS CLI)

Definindo medições (console)

Ao definir uma medida para um modelo de ativo no AWS IoT SiteWise console, você especifica os seguintes parâmetros:

- Nome — o nome da propriedade.
- Unidade – (opcional) unidade científica da propriedade, como mm ou Celsius.
- Tipo de dado — o tipo de dado da propriedade, que é um dos seguintes:
  - String – uma string com até 1024 bytes.
  - Número inteiro – um número inteiro assinado de 32 bits com intervalo [-2.147.483.648, 2.147.483.647].
  - Duplo – um número de ponto flutuante com intervalo [-10^100, 10^100] e precisão dupla IEEE 754.
  - Booleano — `true` ou `false`.
- ID externa — (Opcional) Essa é uma ID definida pelo usuário. Para obter mais informações, consulte Referenciando objetos com IDs externos no Guia de Usuário AWS IoT SiteWise .

Para ter mais informações, consulte Criar um modelo de ativo (console).

Definindo medidas (AWS CLI)

Ao definir uma medida para um modelo de ativo com a AWS IoT SiteWise API, você especifica os seguintes parâmetros:

- `name` – o nome da propriedade.
- `dataType`— o tipo de dado da propriedade, que é um dos seguintes:
  - `STRING` – uma string com até 1024 bytes.
  - `INTEGER` – um número inteiro assinado de 32 bits com intervalo [-2.147.483.648, 2.147.483.647].
  - `DOUBLE` – um número de ponto flutuante com intervalo [-10^100, 10^100] e precisão dupla IEEE 754.
  - `BOOLEAN` – `true` ou `false`.
- `unit` – (opcional) unidade científica da propriedade, como mm ou Celsius.
- `externalId`— (Opcional) Essa é uma ID definida pelo usuário. Para obter mais informações, consulte Referenciando objetos com IDs externos no Guia de Usuário AWS IoT SiteWise .

Example Exemplo de definição de medição

O exemplo a seguir demonstra uma medição que representa as leituras do sensor de temperatura de um ativo. Esse objeto é um exemplo de uma AssetModelpropriedade que contém uma medida. Você pode especificar esse objeto como parte da carga de solicitação de CreateAssetmodelo para criar uma propriedade de medição. Para ter mais informações, consulte Criação de um modelo de ativo (AWS CLI).

A Medição é uma estrutura vazia ao definir um modelo de ativo, já que, posteriormente, você irá configurar cada ativo para uso de fluxos de dados de dispositivo exclusivos. Para obter mais informações sobre como conectar a propriedade de medição de um ativo ao fluxo de dados do sensor de um dispositivo, consulte o Mapeamento de fluxos de dados industriais para propriedades de ativos.

```
{
      ...
      "assetModelProperties": [
      {
          "name": "Temperature C",
          "dataType": "DOUBLE",
          "type": {
              "measurement": {}
          },
          "unit": "Celsius"
      }
  ],
      ...
}
```

Transformando dados (transformações)

As Transformações são expressões matemáticas que mapeiam pontos de dados de propriedades de um ativo de um formulário a outro. Uma expressão de transformação consiste em variáveis de propriedade de ativos, literais, operadores e funções. Os pontos de dados transformados mantêm uma one-to-one relação com os pontos de dados de entrada. AWS IoT SiteWise calcula um novo ponto de dados transformado sempre que qualquer uma das propriedades de entrada recebe um novo ponto de dados.

Por exemplo, se o seu ativo tiver um fluxo de medição de temperatura chamado `Temperature_C` com unidades em Celsius, você poderá converter cada ponto de dados em Fahrenheit com a fórmula

`Temperature_F = 9/5 * Temperature_C + 32`. Cada vez que AWS IoT SiteWise recebe um ponto de dados no fluxo de `Temperature_C` medição, o `Temperature_F` valor correspondente é calculado em alguns segundos e está disponível como `Temperature_F` propriedade.

Caso sua transformação contiver mais de uma variável, o ponto de dados que chegar primeiro iniciará o cálculo imediatamente. Considere um exemplo onde um fabricante de peças usa uma transformação para monitorar a qualidade do produto. Usando um padrão diferente com base no tipo de peça, o fabricante usa as seguintes medidas para representar o processo:

- `Part_Number` - uma sequência de caracteres que identifica o tipo de peça.
- `Good_Count` - um número inteiro que aumenta em um se a peça atender ao padrão.
- `Bad_Count` - um número inteiro que aumenta em um se a peça não atender ao padrão.

O fabricante também cria uma transformação, `Quality_Monitor`, igual a `if(eq(Part_Number, "BLT123") and (Bad_Count / (Good_Count + Bad_Count) > 0.1), "Caution", "Normal")`.

Essa transformação monitora a porcentagem de peças defeituosas produzidas para um tipo específico de peça. Se o número da peça for BLT123 e a porcentagem de peças defeituosas exceder 10 por cento (0,1), a transformação será retornada `"Caution"`. Caso contrário, a transformação retornará `"Normal"`.

> **Note**
>
> - Se `Part_Number` receber um novo ponto de dados antes de outras medições, a `Quality_Monitor` transformação usa o novo valor `Part_Number` e os valores `Bad_Count` e `Good_Count` mais recentes. Para evitar erros, reinicie `Good_Count` e `Bad_Count` antes da próxima execução de fabricação.
> - Use métricas se quiser avaliar expressões somente depois que todas as variáveis receberem novos pontos de dados.

Tópicos

- Definir transformações (console)
- Definindo transformações ()AWS CLI

Definir transformações (console)

Ao definir uma transformação para um modelo de ativo no AWS IoT SiteWise console, você especifica os seguintes parâmetros:

- Nome — o nome da propriedade.
- Unidade – (opcional) unidade científica da propriedade, como mm ou Celsius.
- Tipo de dado — tipo de dado da transformação, que pode ser Duplo ou String.
- ID externa — (Opcional) Essa é uma ID definida pelo usuário. Para obter mais informações, consulte Referenciando objetos com IDs externos no Guia de Usuário AWS IoT SiteWise .
- Fórmula — a expressão de transformação. As expressões de transformação não podem usar funções de agregação ou funções temporais. Para abrir o recurso de preenchimento automático, comece a digitar ou pressione a tecla de seta para baixo. Para ter mais informações, consulte Usando expressões de fórmula.

> **Important**
>
> As transformações só podem inserir propriedades de número inteiro, duplo, Booleano, ou tipo string. Os Booleanos são convertidos em `0` (falso) e `1` (verdadeiro).
> As transformações devem inserir uma ou mais propriedades que não sejam atributo e qualquer número de propriedades de atributo. O AWS IoT SiteWise calcula um novo ponto de dados transformado cada vez que a propriedade de entrada que não for de atributo receber um novo ponto de dados. Novos valores de atributos não iniciam atualizações de transformação. A mesma taxa de solicitação para operações de API de dados de propriedades de ativos se aplica aos resultados de computação de transformação.
> As expressões de fórmula só podem produzir valores duplos ou de string. Expressões aninhadas podem gerar outros tipos de dados, como strings, mas a fórmula como um todo deve ser avaliada como um número ou string. Você pode usar a função jp para converter uma string em um número. O valor Booleano deve ser 1 (verdadeiro) ou 0 (falso). Para ter mais informações, consulte Valores indefinidos, infinitos e excedidos.

Para ter mais informações, consulte Criar um modelo de ativo (console).

Definindo transformações ()AWS CLI

Ao definir uma transformação para um modelo de ativo com a AWS IoT SiteWise API, você especifica os seguintes parâmetros:

- `name` – o nome da propriedade.
- `unit` – (opcional) unidade científica da propriedade, como mm ou Celsius.
- `dataType` – tipo de dados da transformação, que deve ser `DOUBLE` ou`STRING`.
- `externalId`— (Opcional) Essa é uma ID definida pelo usuário. Para obter mais informações, consulte Referenciando objetos com IDs externos no Guia de Usuário AWS IoT SiteWise .
- `expression` – expressão de transformação. As expressões de transformação não podem usar funções de agregação ou funções temporais. Para ter mais informações, consulte Usando expressões de fórmula.
- `variables` – lista de variáveis que define as outras propriedades do seu ativo a serem usadas na expressão. Cada estrutura variável contém um nome simples para uso na expressão e uma estrutura de `value` que identifica qual propriedade deve ser vinculada a essa variável. A estrutura `value` contém as seguintes informações:
  - `propertyId` – a ID da propriedade da qual deseja extrair valores. Você pode usar o nome da propriedade em vez de seu ID.

> **Important**
>
> As transformações só podem inserir propriedades de número inteiro, duplo, Booleano, ou tipo string. Os Booleanos são convertidos em `0` (falso) e `1` (verdadeiro).
> As transformações devem inserir uma ou mais propriedades que não sejam atributo e qualquer número de propriedades de atributo. O AWS IoT SiteWise calcula um novo ponto de dados transformado cada vez que a propriedade de entrada que não for de atributo receber um novo ponto de dados. Novos valores de atributos não iniciam atualizações de transformação. A mesma taxa de solicitação para operações de API de dados de propriedades de ativos se aplica aos resultados de computação de transformação.
> As expressões de fórmula só podem produzir valores duplos ou de string. Expressões aninhadas podem gerar outros tipos de dados, como strings, mas a fórmula como um todo deve ser avaliada como um número ou string. Você pode usar a função jp para converter uma string em um número. O valor Booleano deve ser 1 (verdadeiro) ou 0 (falso). Para ter mais informações, consulte Valores indefinidos, infinitos e excedidos.

Example definição de transformação

O exemplo a seguir demonstra uma propriedade de transformação que converte dados de medição de temperatura de um ativo de Celsius para Fahrenheit. Esse objeto é um exemplo de uma

AssetModelpropriedade que contém uma transformação. Você pode especificar esse objeto como parte da carga de solicitação de CreateAssetmodelo para criar uma propriedade de transformação. Para ter mais informações, consulte Criação de um modelo de ativo (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 definição de transformação que contém três variáveis

O exemplo a seguir demonstra uma propriedade de transformação que retorna uma mensagem de aviso (`"Caution"`) se mais de 10% das partes do BLT123 não atenderem ao padrão. Caso contrário, ela retornará uma mensagem de informação (`"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"
                }
            }
        ]
    }
}
}
...
}
```

Agregando dados de propriedades e outros ativos (métricas)

As métricas são expressões matemáticas que usam funções agregadas para processar todos os pontos de dados de entrada e produzir um único ponto de dados por intervalo de tempo especificado. Por exemplo, uma métrica pode calcular a temperatura média por hora a partir de um fluxo de dados de temperatura.

As métricas podem inserir dados de entrada de ativos associados, para que você possa calcular estatísticas que forneçam informações sobre sua operação ou sobre um subconjunto da sua operação. Por exemplo, uma métrica pode calcular a temperatura média horária em todas as

turbinas eólicas em um parque eólico. Para obter mais informações sobre como definir associações entre ativos, consulte Definindo hierarquias de modelos de ativos.

As métricas também podem inserir dados de entrada de outras propriedades sem agregar dados a cada intervalo de tempo. Se você especificar um atributo em uma fórmula, AWS IoT SiteWise usa o valor mais recente desse atributo ao computar a fórmula. Se você especificar uma métrica em uma fórmula, AWS IoT SiteWise usa o último valor para o intervalo de tempo durante o qual ela calcula a fórmula. Isso significa que você pode definir métricas como `OEE = Availability * Quality * Performance`, onde `Availability`, `Quality` e `Performance` são todas as outras métricas no mesmo modelo de ativos.

AWS IoT SiteWise também calcula automaticamente um conjunto de métricas básicas de agregação para todas as propriedades do ativo. Para reduzir os custos de computação, você pode usar esses agregados em vez de definir métricas personalizadas para cálculos básicos. Para ter mais informações, consulte Consultando agregados de propriedades de ativos.

Tópicos

- Definir métricas (console)
- Definindo métricas (AWS CLI)

Definir métricas (console)

Ao definir uma métrica para um modelo de ativo no AWS IoT SiteWise console, você especifica os seguintes parâmetros:

- Nome — o nome da propriedade.
- Tipo de dado — tipo de dado da transformação, que pode ser Duplo ou String.
- ID externa — (Opcional) Essa é uma ID definida pelo usuário. Para obter mais informações, consulte Referenciando objetos com IDs externos no Guia de Usuário AWS IoT SiteWise .
- Fórmula — a expressão métrica. As expressões métricas podem usar funções de agregação para inserir dados de entrada de uma propriedade para todos os ativos associados em uma hierarquia. Comece digitando ou pressionando a seta para baixo para abrir o recurso de preenchimento automático. Para ter mais informações, consulte Usando expressões de fórmula.

> **Important**
>
> Métricas só podem inserir propriedades do tipo inteiro, duplo, Booleano ou string. Os Booleanos são convertidos em `0` (falso) e `1` (verdadeiro).

Se você definir quaisquer variáveis de entrada de métrica na expressão de uma métrica, essas entradas deverão ter o mesmo intervalo de tempo que a métrica de saída.
As expressões de fórmula só podem produzir valores duplos ou de string. Expressões aninhadas podem gerar outros tipos de dados, como strings, mas a fórmula como um todo deve ser avaliada como um número ou string. Você pode usar a função jp para converter uma string em um número. O valor Booleano deve ser 1 (verdadeiro) ou 0 (falso). Para ter mais informações, consulte Valores indefinidos, infinitos e excedidos.

- Intervalo de tempo – tempo de intervalo métrico. AWS IoT SiteWise é compatível com a seguinte janela em cascata de intervalos de tempo, onde cada intervalo começa quando o anterior termina:
  - 1 minuto – 1 minuto, calculado no final de cada minuto (00:00:00, 00:01:00, 00:02:00 e assim por diante).
  - 5 minutos – 5 minutos, calculados no final de cada cinco minutos a partir da hora (00:00:00, 00:05:00, 00:10:00 e assim por diante).
  - 15 minutos – 15 minutos, calculados no final de cada quinze minutos a partir da hora (00:00:00, 00:15:00, 00:30:00 e assim por diante).
  - 1 hora – 1 hora (60 minutos), calculada no final de cada hora em UTC (00:00:00, 01:00:00, 02:00:00 e assim por diante).
  - 1 dia – 1 dia (24 horas), calculado no final de cada dia em UTC (00:00:00 segunda-feira, 00:00:00 terça-feira e assim por diante).
  - 1 semana – 1 semana (7 dias), calculada no final de cada domingo em UTC (a cada 00:00:00 segunda-feira).
  - Intervalo personalizado — você pode inserir qualquer intervalo de tempo entre um minuto e uma semana.
- Data de deslocamento — (opcional) data de referência a partir da qual agregar dados.
- Tempo de deslocamento — (opcional) horário de referência a partir do qual agregar dados. O horário de deslocamento deve ser entre 00:00:00 e 23:59:59.
- Fuso horário de deslocamento — (opcional) fuso horário do deslocamento. Se não for especificado, o fuso horário de compensação padrão é Horário Universal Coordenado (UTC).

Fusos horários suportados:

- (UTC+ 00:00) Tempo Universal Coordenado
- (UTC+ 01:00) Hora Central Europeia
- (UTC+ 02:00) Leste Europeu

- (UTC+ 03:00) Hora da África Oriental
- (UTC+ 04:00) Hora do Oriente Próximo
- (UTC+ 05:00) Horário de Lahore, no Paquistão
- (UTC+ 05:30) Horário padrão da Índia
- (UTC+ 06:00) Horário padrão de Bangladesh
- (UTC+ 07:00) Horário padrão do Vietnã
- (UTC+ 08:00) Hora China Taipei
- (UTC+ 09:00) Horário Padrão do Japão
- (UTC+ 09:30) Hora Central da Austrália
- (UTC+ 10:00) Horário do Leste da Austrália
- (UTC+ 11:00) Horário Padrão de Salomão
- (UTC+ 12:00) Horário Padrão da Nova Zelândia
- (UTC- 11:00) Horário das Ilhas Midway
- (UTC- 10:00) Horário padrão do Havaí
- (UTC- 09:00) Horário padrão do Alasca
- (UTC- 08:00) Hora padrão do Pacífico
- (UTC- 07:00) Horário padrão de Phoenix
- (UTC- 06:00) Horário Padrão Central
- (UTC- 05:00) Horário Padrão do Leste
- (UTC- 04:00) Horário de Porto Rico e Ilhas Virgens dos EUA
- (UTC- 03:00) Horário Padrão da Argentina
- (UTC- 02:00) Hora da Geórgia do Sul
- (UTC- 01:00) Horário da África Central

Example intervalo de tempo personalizado com um deslocamento (console)

O exemplo a seguir mostra como definir um intervalo de 12 horas com um deslocamento em 20 de fevereiro de 2021, às 18:30:30 (PST).

Para definir um intervalo personalizado com um deslocamento

1. Em Intervalo de tempo, escolha Intervalo personalizado.

2. Para Intervalo de tempo, execute uma das opções a seguir:

   - Insira **`12`** e escolha horas.
   - Insira **`720`** e escolha minutos.
   - Insira **`43200`** e escolha segundos.

   > **Important**
   >
   > O intervalo de tempo deve ser um número inteiro, independente da unidade.

3. Em Data de deslocamento, escolha 20/02/2021.
4. Em Tempo de deslocamento, insira **`18:30:30`**.
5. Em Fuso horário de deslocamento, escolha (UTC- 08:00) Horário Padrão do Pacífico.

Se você criar a métrica em 1º de julho de 2021, antes ou às 18h30 (PST), obterá o primeiro resultado da agregação em 1º de julho de 2021, às 18h30 (PST). O segundo resultado da agregação é em 2 de julho de 2021, às 06h30 (PST), e assim por diante.

Definindo métricas (AWS CLI)

Ao definir uma métrica para um modelo de ativo com a AWS IoT SiteWise API, você especifica os seguintes parâmetros:

- `name` – o nome da propriedade.
- `dataType` — tipo de dados da métrica, que pode ser `DOUBLE` ou `STRING`.
- `externalId`— (Opcional) Essa é uma ID definida pelo usuário. Para obter mais informações, consulte Referenciando objetos com IDs externos no Guia de Usuário AWS IoT SiteWise .
- `expression` — a expressão métrica. As expressões métricas podem usar funções de agregação para inserir dados de entrada de uma propriedade para todos os ativos associados em uma hierarquia. Para ter mais informações, consulte Usando expressões de fórmula.
- `window` — intervalo de tempo e deslocamento da janela de queda da métrica, onde cada intervalo começa quando o anterior termina:
  - `interval` – intervalo de tempo da janela em cascata. O intervalo de tempo deve estar entre um minuto e uma semana.
  - `offsets` – deslocamento da janela em cascata.

Para obter mais informações, consulte TumblingWindowa Referência AWS IoT SiteWise da API.

Example intervalo de tempo personalizado com um deslocamento (AWS CLI)

O exemplo a seguir mostra como definir um intervalo de 12 horas com um deslocamento em 20 de fevereiro de 2021, às 18:30:30 (PST).

```
{
    "window": {
        "tumbling": {
            "interval": "12h",
            "offset": " 2021-07-23T18:30:30-08"
        }
    }
}
```

Se você criar a métrica em 1º de julho de 2021, antes ou às 18h30 (PST), obterá o primeiro resultado da agregação em 1º de julho de 2021, às 18h30 (PST). O segundo resultado da agregação é em 2 de julho de 2021, às 06h30 (PST), e assim por diante.

- `variables` – uma lista de que define as outras propriedades de seu ativo ou ativos filho a serem usados na expressão. Cada estrutura variável contém um nome simples para uso na expressão e uma estrutura `value`, que identifica qual propriedade deve ser vinculada à variável. A estrutura `value` contém as seguintes informações:
  - `propertyId` – ID da propriedade da qual deseja extrair valores. Você pode usar o nome da propriedade em vez da ID se a propriedade for definida no modelo atual (em vez de definida em um modelo de uma hierarquia).
  - `hierarchyId` – (opcional) ID da hierarquia da qual consultar ativos filhos para a propriedade. Você pode usar o nome da definição de hierarquia em vez da ID. Se você omitir esse valor, AWS IoT SiteWise localizará a propriedade no modelo atual.

> **Important**
>
> Métricas só podem inserir propriedades do tipo inteiro, duplo, Booleano ou string. Os Booleanos são convertidos em `0` (falso) e `1` (verdadeiro).
> Se você definir quaisquer variáveis de entrada de métrica na expressão de uma métrica, essas entradas deverão ter o mesmo intervalo de tempo que a métrica de saída.

As expressões de fórmula só podem produzir valores duplos ou de string. Expressões aninhadas podem gerar outros tipos de dados, como strings, mas a fórmula como um todo deve ser avaliada como um número ou string. Você pode usar a função jp para converter uma string em um número. O valor Booleano deve ser 1 (verdadeiro) ou 0 (falso). Para ter mais informações, consulte Valores indefinidos, infinitos e excedidos.

- `unit` – (opcional) unidade científica da propriedade, como mm ou Celsius.

Example Exemplo de definição de métrica

O exemplo a seguir demonstra uma propriedade de métrica que agrega dados de medição de temperatura de um ativo para calcular a temperatura máxima por hora em Fahrenheit. Esse objeto é um exemplo de uma AssetModelpropriedade que contém uma métrica. Você pode especificar esse objeto como parte da carga de solicitação de CreateAssetmodelo para criar uma propriedade métrica. Para ter mais informações, consulte Criação de um modelo de ativo (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 Exemplo de definição de métrica que insere dados de entrada de ativos associados

O exemplo a seguir demonstra uma propriedade métrica que agrega múltiplos dados de potência média de turbinas eólicas para calcular a potência média total de um parque eólico. Esse objeto é um exemplo de uma AssetModelpropriedade que contém uma métrica. Você pode especificar esse objeto como parte da carga de solicitação de CreateAssetmodelo para criar uma propriedade 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"
      }
```

```
    ],
    ...
}
```

Usando expressões de fórmula

Com expressões de fórmula, você pode definir as funções matemáticas para transformar e agregar seus dados industriais brutos a fim de obter insights sobre sua operação. As expressões de fórmula combinam literais, operadores, funções e variáveis para processar dados. Para obter mais informações sobre como definir propriedades que usam expressões de fórmula, consulte Transformando dados (transformações) e Agregando dados de propriedades e outros ativos (métricas). Transformações e métricas são propriedades da fórmula.

Tópicos

- Usando variáveis em expressões de fórmulas
- Usando literais em expressões de fórmula
- Usando operadores em expressões de fórmula
- Usando constantes em expressões de fórmulas
- Usando funções em expressões de fórmulas
- Tutoriais de expressão de fórmulas

Usando variáveis em expressões de fórmulas

As variáveis representam propriedades AWS IoT SiteWise de ativos em expressões de fórmulas. Use variáveis para inserir valores de outras propriedades do ativo em suas expressões, para que você possa processar dados de propriedades constantes (atributos), fluxos de dados brutos (medidas) e outras propriedades da fórmula.

As variáveis podem representar propriedades de ativos do mesmo modelo de ativo ou de modelos de ativos filho associados. Somente fórmulas métricas podem inserir variáveis de modelos de ativos filho.

Você identifica variáveis por nomes diferentes no console e na API.

- AWS IoT SiteWise console — Use nomes de propriedades de ativos como variáveis em suas expressões.
- AWS IoT SiteWise API (AWS CLI, AWS SDKs) — Defina variáveis com a ExpressionVariableestrutura, o que requer um nome de variável e uma referência a uma

propriedade do ativo. O nome da variável pode conter letras minúsculas, números e sublinhados (_). Em seguida, use nomes de variáveis para referenciar propriedades de ativos em suas expressões.

Os nomes de variáveis diferenciam minúsculas de maiúsculas.

Para obter mais informações, consulte Definindo transformações e Definindo de métricas.

Usando variáveis para referenciar propriedades

O valor de uma variável define a propriedade à qual ela faz referência. AWS IoT SiteWise fornece maneiras diferentes de fazer isso.

- Por ID da propriedade: você pode especificar a ID exclusiva da propriedade (UUID) para identificá-la.
- Por nome: se a propriedade estiver no mesmo modelo de ativo, você poderá especificar seu nome no campo ID da propriedade.
- Por caminho: o valor de uma variável pode se referir a uma propriedade por seu caminho. Para ter mais informações, consulte Usando caminhos para referenciar propriedades personalizadas do modelo composto.

> **Note**
>
> As variáveis não são suportadas pelo AWS IoT SiteWise console. Eles são usados pela AWS IoT SiteWise API, incluindo o AWS Command Line Interface AWS CLI) e os AWS SDKs.

Uma variável que você recebe em uma resposta AWS IoT SiteWise inclui informações completas sobre o valor, incluindo a ID e o caminho.

No entanto, ao passar uma variável para AWS IoT SiteWise (por exemplo, em uma chamada de “criar” ou “atualizar”), você só precisa especificar uma delas. Por exemplo, se você especificar o caminho, não precisará fornecer o ID.

Usando literais em expressões de fórmula

Você pode definir literais numéricos e de strings em expressões de fórmula.

•

Números

Use números e notação científica para definir números inteiros e duplos. Você pode usar a notação E para expressar números com notação científica.

Exemplos: `1`, `2.0`, `.9`, `-23.1`, `7.89e3`, `3.4E-5`

- Strings

  Use os caracteres `'` (aspas) e `"` (aspas duplas) para definir strings de caracteres. O tipo de cotação para o início e fim deve corresponder. Para escapar de uma citação que corresponda a que você usa para declarar uma string, inclua o caractere de aspa duas vezes. Esse é o único caractere de escape em AWS IoT SiteWise strings.

  Exemplos: `'active'`, `"inactive"`, `'{"temp": 52}'`, `"{""temp"": ""high""}"`

Usando operadores em expressões de fórmula

Você pode usar os seguintes operadores matemáticos comuns em suas expressões:

Operador	Descrição
+	Se ambos os operandos forem números, esse operador adiciona os operandos esquerdo e direito. Se um dos operandos for uma string, esse operador concatena os operandos esquerdo e direito como strings. Por exemplo, a expressão `1 + 2 + " is three"` é avaliada como `"3 is three"`. A string concatenada pode conter até 1024 caracteres. Se a string exceder 1024 caracteres, AWS IoT SiteWise não produzirá um ponto de dados para esse cálculo.
-	Subtrai o operando direito do operando esquerdo.

Operador	Descrição
	Você só pode usar esse operador com operandos numéricos.
`/`	Divide o operando esquerdo pelo operando direito. Você só pode usar esse operador com operandos numéricos.
`*`	Multiplica os operandos esquerdo e direito. Você só pode usar esse operador com operandos numéricos.
`^`	Eleva o operando esquerdo à potência do operando direito (exponenciação). Você só pode usar esse operador com operandos numéricos.
`%`	Gera o restante da divisão do operando esquerdo pelo operando direito. O resultado tem o mesmo sinal que o operando esquerdo. Esse comportamento é diferente do operador de módulo. Você só pode usar esse operador com operandos numéricos.
`x < y`	Retorna 1 se `x` for menor que `y`, caso contrário, `0`.
`x > y`	Retorna 1 se `x` for maior que `y`, caso contrário, `0`.
`x <= y`	Retorna 1 se `x` for menor ou igual a `y`, caso contrário, `0`.

Operador	Descrição
`x >= y`	Retorna 1 se x for maior ou igual a y, caso contrário, `0`.
`x == y`	Retorna 1 se x for igual a y, caso contrário, `0`.
`x != y`	Retorna 1 se x não for igual a y, caso contrário, `0`.
`!x`	Retorna 1 se x for avaliado como `0` (falso), caso contrário, `0`. x é avaliado como falso se: • x for um operando numérico avaliado para `0`. • x for avaliado como uma string vazia. • x for avaliado como uma matriz vazia. • x for avaliado para `None`.
`x and y`	Retorna `0` se x for avaliado como `0` (false). Caso contrário, retorna um resultado avaliado de y. x ou y são avaliados como falsos se: • x ou y forem um operando numérico avaliado para `0`. • x ou y forem avaliados como uma string vazia. • x ou y forem avaliados como uma matriz vazia. • x ou y forem avaliados como `None`.

Operador	Descrição
`x or y`	Retorna `1` se `x` for avaliado como `1` (verdadeiro). Caso contrário, retorna um resultado avaliado de `y`. `x` ou `y` são avaliados como falsos se: • `x` ou `y` forem um operando numérico avaliado para `0`. • `x` ou `y` forem avaliados como uma string vazia. • `x` ou `y` forem avaliados como uma matriz vazia. • `x` ou `y` forem avaliados como `None`.
`not x`	Retorna `1` se `x` for avaliado como `0` (falso), caso contrário, `0`. `x` é avaliado como falso se: • `x` for um operando numérico avaliado para `0`. • `x` for avaliado como uma string vazia. • `x` for avaliado como uma matriz vazia. • `x` for avaliado para `None`.

`[]`
 	
`s[index]`
	Retorna o caractere em um índice `index` da string `s`. Isso é equivalente à sintaxe do índice em Python.
	
	Example Exemplos
	
	• `"Hello!"[1]` Retorna `e`.
	• `"Hello!"[-2]` Retorna `o`.

Operador	Descrição

`[]`
 	
`s[start:end:step]`
	Retorna uma fatia da string `s`. Isso é equivalente à fatia da sintaxe do índice em Python. Esse operador tem os seguintes argumentos:
	
	• `start` — (opcional) índice inicial inclusivo da fatia. Padronizado como `0`.
	• `end` — (opcional) índice final exclusivo da fatia. O padrão é o comprimento da string.
	• `step` — (opcional) número a ser incrementado para cada etapa na fatia. Por exemplo, você pode especificar 2 para retornar uma fatia com todos os outros caracteres, ou especificar `-1` para reverter a fatia. Padronizado como 1.
	
	Você pode omitir o argumento `step` para usar seu valor padrão. Por exemplo, `s[1:4:1]` equivale a `s[1:4]`.
	
	Os argumentos devem ser números inteiros ou a constante nenhum. Se você especificar`none`, AWS IoT SiteWise usa o valor padrão para esse argumento.
	
	Example Exemplos
	
	• `"Hello!"[1:4]` Retorna `"ell"`.
	• `"Hello!"[:2]` Retorna `"He"`.
	• `"Hello!"[3:]` Retorna `"lo!"`.
	• `"Hello!"[:-4]` Retorna `"He"`.
	• `"Hello!"[::2]` Retorna `"Hlo"`.
	• `"Hello!"[::-1]` Retorna `"!olleH"`.

Usando constantes em expressões de fórmulas

Você pode usar as seguintes constantes matemáticas comuns em suas expressões. Todas as constantes diferenciam letras maiúsculas de minúsculas.

> **Note**
>
> Se você definir uma variável com o mesmo nome de uma constante, a variável substituirá a constante.

Constante	Descrição
`pi`	O número pi (π): `3.141592653589793`
`e`	O número e: `2.718281828459045`
`true`	Equivalente ao número 1. Em AWS IoT SiteWise, os booleanos se convertem em seus equivalentes numéricos.
`false`	Equivalente ao número 0. Em AWS IoT SiteWise, os booleanos se convertem em seus equivalentes numéricos.
`none`	Equivalente a nenhum valor. Você pode usar essa constante para não produzir nada como resultado de uma expressão condicional.

Usando funções em expressões de fórmulas

Você pode usar as seguintes funções para operar com dados em suas expressões de fórmula.

As transformações e métricas oferecem suporte a diferentes funções. A tabela a seguir indica quais tipos de funções suportam cada tipo de propriedade da fórmula.

> **Note**
>
> Você pode incluir no máximo 10 funções em uma expressão de fórmula.

Tipo de função	Transformações	Metrics
Usando funções comuns em expressões de fórmulas	 Sim	 Sim
Usando funções de comparação em expressões de fórmulas	 Sim	 Sim
Usando funções condicionais em expressões de fórmulas	 Sim	 Sim
Usando funções de string em expressões de fórmula	 Sim	 Sim
Usando funções de agregação em expressões de fórmulas	 Não	 Sim
Usando funções temporais em expressões de fórmula	 Sim	 Sim

Tipo de função	Transformações	Metrics
Usando funções de data e hora em expressões de fórmula	 Sim	 Sim

Sintaxe de funções

Você pode usar a seguinte sintaxe para criar funções:

Sintaxe regular

Com a sintaxe regular, o nome da função é seguido por parênteses com zero ou mais argumentos.

`function_name``(`*`argument1, argument2, argument3, ...`*`)`. Por exemplo, funções com a sintaxe regular podem ser parecidas com `log(x)` e `contains(s, substring)`.

Sintaxe uniforme de chamada de função (UFCS)

UFCS permite que você chame funções usando a sintaxe para chamadas de métodos na programação orientada a objetos. Com UFCS, o primeiro argumento é seguido por ponto (`.`), o nome da função e os argumentos restantes (caso haja algum) entre parênteses.

`argument1``.`*`function_name`*`(`*`argument2, argument3, ...`*`)`. Por exemplo, funções com UFCS podem ser parecidas com `x.log()` e `s.contains(substring)`.

Você também pode usar o UFCS para encadear funções subsequentes. AWS IoT SiteWise usa o resultado da avaliação da função atual como o primeiro argumento para a próxima função.

Por exemplo, você pode usar `message.jp('$.status').lower().contains('fail')`, em vez de `contains(lower(jp(message, '$.status')),'fail')`.

Para obter mais informações, visite o website D Programming Language.

> **Note**
>
> Você pode usar o UFCS para todas as AWS IoT SiteWise funções.

AWS IoT SiteWise as funções não diferenciam maiúsculas de minúsculas. Por exemplo, você pode usar `lower(s)` e `Lower(s)` de forma intercambiável.

Usando funções comuns em expressões de fórmulas

Em transformações e métricas, você pode usar as seguintes funções para calcular funções matemáticas comuns em transformações e métricas:

Função	Descrição
`abs(x)`	Retorna o valor absoluto de `x`.
`acos(x)`	Retorna o arco cosseno de `x`.
`asin(x)`	Retorna o arco seno de `x`.
`atan(x)`	Retorna o arco tangente de `x`.
`cbrt(x)`	Retorna a raiz cúbica de `x`.
`ceil(x)`	Retorna o inteiro mais próximo maior que `x`.
`cos(x)`	Retorna o cosseno de `x`.
`cosh(x)`	Retorna o cosseno hiperbólico de `x`.
`cot(x)`	Retorna o co-tangente de `x`.
`exp(x)`	Retorna `e` à potência de `x`.
`expm1(x)`	Retorna `exp(x) - 1`. Use essa função para calcular com mais precisão `exp(x) - 1` para valores pequenos de `x`.
`floor(x)`	Retorna o inteiro mais próximo menor que `x`.
`log(x)`	Retorna o $\log_e$ (base `e`) de `x`.
`log10(x)`	Retorna o $\log_{10}$ (base `10`) de `x`.

Função	Descrição
`log1p(x)`	Retorna `log(1 + x)`. Use essa função para calcular com mais precisão `log(1 + x)` para valores pequenos de `x`.
`log2(x)`	Retorna o $\log_2$ (base 2) de `x`.
`pow(x, y)`	Retorna `x` à potência de `y`. Isso é equivalente a `x ^ y`.
`signum(x)`	Retorna o sinal de `x` (`-1` para entradas negativas, `0` para entradas zero, `+1` para entradas positivas).
`sin(x)`	Retorna o seno de `x`.
`sinh(x)`	Retorna o seno hiperbólico de `x`.
`sqrt(x)`	Retorna a raiz quadrada de `x`.
`tan(x)`	Retorna a tangente de `x`.
`tanh(x)`	Retorna a tangente hiperbólica de `x`.

Usando funções de comparação em expressões de fórmulas

Em transformações e métricas, você pode usar as seguintes funções de comparação para comparar dois valores e a saída `1` (verdadeiro) ou `0` (falso). AWS IoT SiteWise compara cadeias de caracteres por ordem lexicográfica.

Função	Descrição
`gt(x, y)`	Retorna `1` se `x` for maior que `y`, caso contrário `0` (`x > y`). Essa função não retorna um valor se `x` e `y` forem tipos incompatíveis, como um número e uma string.

Função	Descrição
`gte(x, y)`	Retorna `1` se `x` for maior ou igual a `y`, caso contrário `0` (`x ≥ y`). AWS IoT SiteWise considera os argumentos iguais se estiverem dentro de uma tolerância relativa de`1E-9`. Isso se comporta de forma semelhante à função isclose em Python. Essa função não retorna um valor se `x` e `y` forem tipos incompatíveis, como um número e uma string.
`eq(x, y)`	Retorna `1` se `x` for igual a `y`, caso contrário `0` (`x == y`). AWS IoT SiteWise considera os argumentos iguais se estiverem dentro de uma tolerância relativa de`1E-9`. Isso se comporta de forma semelhante à função isclose em Python. Essa função não retorna um valor se `x` e `y` forem tipos incompatíveis, como um número e uma string.
`lt(x, y)`	Retorna `1` se `x` for menor que `y`, caso contrário `0` (`x < y`). Essa função não retorna um valor se `x` e `y` forem tipos incompatíveis, como um número e uma string.

Função	Descrição
`lte(x, y)`	Retorna `1` se `x` for menor ou igual a `y`, caso contrário `0` (`x ≤ y`). AWS IoT SiteWise considera os argumentos iguais se estiverem dentro de uma tolerância relativa de`1E-9`. Isso se comporta de forma semelhante à função isclose em Python. Essa função não retorna um valor se `x` e `y` forem tipos incompatíveis, como um número e uma string.
`isnan(x)`	Retorna `1` se `x` for igual a `NaN`, caso contrário, `0`. Essa função não retorna um valor se `x` for uma string.

Usando funções condicionais em expressões de fórmulas

Em transformações e métricas, você pode usar a função a seguir para verificar uma condição e retornar resultados diferentes, independentemente de a condição ser avaliada como verdadeira ou falsa.

Função	Descrição
`if(condition, result_if_true, result_if_false)`	Avalia `condition` e retorna `result_if_true` se a condição for avaliada como verdadeira ou `result_if_false` se a condição for avaliada como `false`. `condition` deve ser um número. Essa função considera `0` uma string vazia como `false` e todo o resto (inclusive `NaN`) como `true`. Os Booleanos são convertidos em `0` (falso) e `1` (verdadeiro).

Função	Descrição
	Você pode retornar a constante nula dessa função para descartar a saída de uma condição específica. Isso significa que você pode filtrar pontos de dados que não atendam a uma condição. Para ter mais informações, consulte Como filtrar pontos de dados. Example Exemplos • `if(0, x, y)` retorna a variável `y`. • `if(5, x, y)` retorna a variável `x`. • `if(gt(temp, 300), x, y)` retorna a variável `x` se a variável `temp` for maior que `300`. • `if(gt(temp, 300), temp, none)` retorna a variável `temp` se for maior ou igual a `300`, ou `none` (sem valor), se `temp` for menor que `300`. Recomendamos que você use UFCS para funções condicionais aninhadas onde um ou mais argumentos forem funções condicion ais. Você pode usar `if(condition, result_if_true)` para avaliar uma condição e `elif(condition, result_if_true, result_if_false)` para avaliar condições adicionais. Por exemplo, você pode usar `if(condition1, result1_if_true).elif(condition2, result2_if_true, result2_if_false)` , em vez de `if(condition1, result1_if_true, if(condition2, result2_if_true, result2_if_false))` .

Função	Descrição
	Você também pode encadear funções condicionais intermediárias adicionais. Por exemplo, você pode usar `if(condition1, result1_if_true).elif(condition2, result2_if_true).elif(condition3, result3_if_true, result3_if_false)` em vez de aninhar várias instruções `if`, como `if(condition1, result1_if_true, if(condition2, result2_if_true, if(condition3, result3_if_true result3_if_false)))` . **Important** Você deve usar `elif(condition, result_if_true, result_if_false)` com UFCS.

Usando funções de string em expressões de fórmula

Em transformações e métricas, você pode usar as seguintes funções para operar em cadeias de caracteres: Para ter mais informações, consulte Usando cadeias de caracteres em fórmulas.

Important

As expressões de fórmula só podem produzir valores duplos ou de string. Expressões aninhadas podem gerar outros tipos de dados, como strings, mas a fórmula como um todo deve ser avaliada como um número ou string. Você pode usar a função jp para converter uma string em um número. O valor Booleano deve ser 1 (verdadeiro) ou 0 (falso). Para ter mais informações, consulte Valores indefinidos, infinitos e excedidos.

Função	Descrição
`len(s)`	Retorna o tamanho da string `s`.
`find(s, substring)`	Retorna o índice da string `substring` na string `s`.
`contains(s, substring)`	Retorna `1` se a string `s` contiver a string `substring`, caso contrário, `0`.
`upper(s)`	Retorna a string `s` em maiúsculas.
`lower(s)`	Retorna a string `s` em minúsculas.
`jp(s, json_path)`	Avalia a string `s` com a JsonPathexpressão `json_path` e retorna o resultado. Use essa função para fazer o seguinte: • Extrair um valor, matriz ou objeto de uma estrutura JSON serializada. • Converter uma string em um número. Por exemplo, a fórmula `jp('111', '$')` retorna `111` como um número. Para extrair um valor de string de uma estrutura JSON e retorná-lo como um número, você deve usar várias funções aninhadas `jp`. A função externa `jp` extrai a string da estrutura JSON e a função internajp converte a string em um número. A string `json_path` deve conter uma literal de string. Isso significa que `json_path` não pode ser uma expressão avaliada como uma string.

Função	Descrição
	Example Exemplos • `jp('{"status":"active","value":15}', '$.value')` Retorna 15. • `jp('{"measurement":{"reading":25,"confidence":0.95}}', '$.measurement.reading')` Retorna 25. • `jp('[2,8,23]', '$[2]')` Retorna 23. • `jp('{"values":[3,6,7]}', '$.values[1]')` Retorna 6. • `jp('111', '$')` Retorna 111. • `jp(jp('{"measurement":{"reading":25,"confidence":"0.95"}}', '$.measurement.confidence'), '$')` Retorna `0.95`.
`join(s0, s1, s2, s3, ...)`	Retorna uma string concatenada com um delimitador. Essa função usa a primeira string de entrada como delimitador e une as demais strings de entrada. Isso se comporta de forma semelhante à função join (CharSequence delimiter, CharSequence... elements) em Java. Example Exemplos: • `join("-", "aa", "bb", "cc")` retorna `aa-bb-cc`

Função	Descrição
`format(expression: "format")` ou `format("format", expression)`	Retorna uma string no formato especificado. Essa função valia `expression` como um valor e, em seguida, retorna o valor no formato especificado. Isso se comporta de forma semelhante a função format(String format, Object... args) em Java. Para obter mais informações sobre os formatos suportados, consulte Conversões em Formatador de Classe na Plataforma Java, Especificação de API Standard Edition 7. Example Exemplos • `format(100+1: "d")` retorna uma string, `101`. • `format("The result is %d", 100+1)` retorna uma string, `The result is 101`.

Função	Descrição
`f'expression'`	Retorna uma string concatenada. Com essa função formatada, você pode usar uma expressão simples para concatenar e formatar strings. Essas funções podem conter expressões aninhadas. Você pode usar `{}` (chaves) para interpolar expressões. Isso se comporta de forma semelhante aos literais de string formatados em Python. Example Exemplos • `f'abc{1+2: "f"}d'` Retorna `abc3.000000d` . Para avaliar esse exemplo de expressão, faça o seguinte: 1. `format(1+2: "f")` retorna um número de ponto flutuante, `3.000000`. 2. `join('', "abc", 1+2, 'd')` retorna uma string, `abc3.000000d` . Você também pode escrever a expressão da seguinte maneira: `join('', "abc", format(1+2: "f"), 'd')` .

Usando funções de agregação em expressões de fórmulas

Somente em métricas, você pode usar as seguintes funções que agregam valores de entrada a cada intervalo de tempo e calculam um único valor de saída: Algumas funções de agregação não podem agregar dados de ativos associados.

Os argumentos da função de agregação podem ser variáveis, literais numéricos, funções temporais, expressões aninhadas ou funções de agregação. A fórmula `max(latest(x), latest(y), latest(z))` usa uma função de agregação como argumento e retorna o maior valor atual das propriedades `x`, `y` e `z`.

Você pode usar expressões aninhadas em funções de agregação. Ao usar expressões aninhadas, as seguintes regras se aplicam:

- Cada argumento pode ter apenas uma variável.

  Example

  Por exemplo, `avg(x*(x-1))` e `sum(x/2 )/avg(y^2 )` são suportadas.

  Por exemplo, `min(x/y)` não é suportada.
- Cada argumento pode ter expressões aninhadas de vários níveis.

  Example

  Por exemplo, `sum(avg(x^2 )/2)` é suportada.
- Argumentos diferentes podem ter variáveis diferentes.

  Example

  Por exemplo, `sum(x/2, y*2)` é suportada.

> **Note**
>
> - Se suas expressões contiverem medidas, AWS IoT SiteWise use os últimos valores no intervalo de tempo atual para que as medidas calculem agregados.
> - Se suas expressões contiverem atributos, AWS IoT SiteWise use os valores mais recentes dos atributos para calcular agregados.

Função	Descrição
$avg(x_0, ..., x_n)$	Retorna a média dos valores das variáveis fornecidas ao longo do intervalo de tempo atual. Essa função gera um ponto de dados somente se as variáveis fornecidas tiverem pelo menos um ponto de dados no intervalo de tempo atual.

Função	Descrição
`sum(x0, ..., xn)`	Retorna a soma dos valores das variáveis fornecidas ao longo do intervalo de tempo atual. Essa função gera um ponto de dados somente se as variáveis fornecidas tiverem pelo menos um ponto de dados no intervalo de tempo atual.
`min(x0, ..., xn)`	Retorna o valor mínimo dos valores das variáveis fornecidas ao longo do intervalo de tempo atual. Essa função gera um ponto de dados somente se as variáveis fornecidas tiverem pelo menos um ponto de dados no intervalo de tempo atual.
`max(x0, ..., xn)`	Retorna o valor máximo das variáveis fornecida s ao longo do intervalo de tempo atual. Essa função gera um ponto de dados somente se as variáveis fornecidas tiverem pelo menos um ponto de dados no intervalo de tempo atual.
`count(x0, ..., xn)`	Retorna o número total de pontos de dados das variáveis fornecidas ao longo do intervalo de tempo atual. Para obter mais informaçõ es sobre como contar o número de pontos de dados que atendem a uma condição, consulte Contando pontos de dados que correspondam a uma condição. Esta função calcula um ponto de dados para cada intervalo de tempo.

Função	Descrição
`stdev(x0, ..., xn)`	Retorna o desvio padrão dos valores das variáveis fornecidos ao longo do intervalo de tempo atual. Essa função gera um ponto de dados somente se as variáveis fornecidas tiverem pelo menos um ponto de dados no intervalo de tempo atual.

Usando funções temporais em expressões de fórmula

Use funções temporais para retornar valores com base nos registros de data e hora dos pontos de dados.

Usando funções temporais em métricas

Apenas em métricas, você pode usar as seguintes funções que retornam valores com base em a função de horas dos pontos de dados:

Os argumentos da função temporal devem ser propriedades do modelo de ativo local ou expressões aninhadas. Isso significa que você não pode usar propriedades de modelos de ativos filho em funções temporais.

Você pode usar expressões aninhadas em funções temporais. Ao usar expressões aninhadas, as seguintes regras se aplicam:

- Cada argumento pode ter apenas uma variável.

  Por exemplo, `latest( t*9/5 + 32 )` é suportada.
- Os argumentos não podem ser funções de agregação.

  Por exemplo, `first( sum(x) )` não é suportada.

Função	Descrição
`first(x)`	Retorna o valor da variável fornecida com o primeiro a função de hora ao longo do intervalo de tempo atual.
`last(x)`	Retorna o valor da variável fornecida com o a função de hora mais recente ao longo do intervalo de tempo atual.
`earliest(x)`	Retorna o último valor da variável fornecida antes do início do intervalo de tempo atual. Se a propriedade de entrada tiver pelo menos um ponto de dados em seu histórico, esta função calcula um ponto de dados para cada intervalo de tempo. Para mais detalhes, consulte time-range-defintion.
`latest(x)`	Retorna o último valor da variável fornecida com a data e hora mais recente antes do final do intervalo de tempo atual. Se a propriedade de entrada tiver pelo menos um ponto de dados em seu histórico, esta função calcula um ponto de dados para cada intervalo de tempo. Para mais detalhes, consulte time-range-defintion.
`statetime(x)`	Retorna a quantidade de tempo em segundos que as variáveis fornecidas são positivas ao longo do intervalo de tempo atual. É possível usar as funções comparativas para criar uma propriedade de transformação para a função `statetime` consumir. Por exemplo, se tiver uma propriedade `Idle` que seja `0` ou `1`, você poderá calcular o

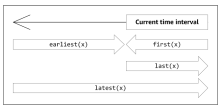
Função	Descrição
	tempo ocioso por intervalo de tempo com esta expressão: `IdleTime = statetime (Idle)` . Para obter mais informações, consulte o exemplo de cenário de statetime. Essa função não é compatível com as propriedades de métrica como variáveis de entrada. Se a propriedade de entrada tiver pelo menos um ponto de dados em seu histórico, esta função calcula um ponto de dados para cada intervalo de tempo.

Função	Descrição
`TimeWeightedAvg(x, [interpolation])`	Retorna a média dos dados de entrada ponderada com intervalos de tempo entre os pontos. Consulte Parâmetros de funções ponderado no tempo para obter detalhes sobre cálculos e intervalos. O argumento opcional `interpolaton` deve ser uma constante de string: • `locf` – Esse é o padrão. O cálculo usa o algoritmo de computação Último Transporte Observado para intervalos entre pontos de dados. Nessa abordagem, o ponto de dados é calculado como o último valor observado até o próximo a função de hora de ponto de dados de entrada. O valor após um bom ponto de dados é extrapolado como seu valor até o próximo a função de hora de ponto de dados. • `linear` — cálculo usa o algoritmo de computação de interpolação linear para intervalos entre pontos de dados. O valor entre dois bons pontos de dados é extrapolado como interpolação linear entre os valores desses pontos de dados. O valor entre pontos de dados bons e ruins, ou o valor após o último ponto de dados bom, será extrapolado como um bom ponto de dados.

Função	Descrição
`TimeWeightedStDev(x, [algo])`	Retorna o desvio padrão dos dados de entrada ponderados com intervalos de tempo entre os pontos. Consulte Parâmetros de funções ponderado no tempo para obter detalhes sobre cálculos e intervalos. O cálculo usa o algoritmo de computação Último Transporte Observado para intervalos entre pontos de dados. Nessa abordagem, o ponto de dados é calculado como o último valor observado até o próximo a função de hora de ponto de dados de entrada. O peso é calculado como intervalo de tempo em segundos entre pontos de dados ou limites de intervalo. O argumento opcional `algo` deve ser uma constante de string: • `f` – esse é o padrão. Ele retorna uma variância de amostra ponderada imparcial com pesos de frequência, onde TimeWeigh t é calculada em segundos. Esse algoritmo geralmente é assumido sob desvio padrão e é conhecido como correção de Bessel de desvio padrão para amostras ponderadas. • p — retorna a variância amostral ponderada imparcial, também conhecida como variância Populacional. As fórmulas a seguir são usadas para computação onde: • S_p = desvio padrão populacional

Função	Descrição
	• S_f = desvio padrão de frequência • X_i = dados recebidos • ω_i = peso igual ao intervalo de tempo em segundos • μ^* = uma média ponderada dos dados recebidos Equação para o desvio padrão populacional: $$S_p^2 = \frac{\sum_{i=1}^{N} \omega_i (x_i - \mu^*)^2}{\sum_{i=1}^{N} \omega_i}$$ Equação para desvio padrão de frequência: $$S_f^2 = \frac{\sum_{i=1}^{N} \omega_i (x_i - \mu^*)^2}{\sum_{i=1}^{N} \omega_i - 1}$$

O diagrama a seguir mostra como AWS IoT SiteWise computa as funções temporais`first`,`last`,`earliest`, `elatest`, em relação ao intervalo de tempo atual.



Note

- O intervalo de tempo para`first(x)`, `last(x)` é (início da janela atual, fim da janela atual].
- O intervalo de tempo para `latest(x)` é (início do tempo, fim da janela atual]).
- O intervalo de tempo para `earliest(x)` é (início do tempo, fim da janela anterior].

Parâmetros de funções ponderadas pelo tempo

As funções ponderadas pelo tempo calculadas para a janela agregada levam em consideração o seguinte:

- Pontos de dados dentro da janela
- Intervalos de tempo entre pontos de dados
- Último ponto de dados antes da janela
- Primeiro ponto de dados após a janela (para alguns algoritmos)

Termos:

- Ponto de dados ruim — qualquer ponto de dados com qualidade inadequada ou valor não numérico. Isso não é considerado no cálculo do resultado de uma janela.
- Intervalo ruim — intervalo após um ponto de dados inválido. O intervalo antes do primeiro ponto de dados conhecido também é considerado um intervalo ruim.
- Bom ponto de dados — qualquer ponto de dados com boa qualidade e valor numérico.

> **Note**
>
> - AWS IoT SiteWise só consome dados `GOOD` de qualidade quando calcula transformações e métricas. Ele ignora os pontos de dados `UNCERTAIN` e `BAD`.
> - O intervalo antes do primeiro ponto de dados conhecido é considerado um intervalo ruim. Consulte the section called “Tutoriais de expressão de fórmulas” Para mais informações.

O intervalo após o último ponto de dados conhecido continua indefinidamente, e afeta todas as janelas seguintes. Quando um novo ponto de dados chega, a função recalcula o intervalo.

Seguindo as regras acima, o resultado agregado da janela é calculado e limitado aos limites da janela. Por padrão, a função só envia o resultado da janela se a janela inteira tiver um bom intervalo.

Se o intervalo bom da janela for menor que seu comprimento, a função não enviará a janela.

Quando os pontos de dados que afetam o resultado da janela mudam, a função recalcula a janela, mesmo que os pontos de dados estejam fora da janela.

Se a propriedade de entrada tiver pelo menos um ponto de dados em seu histórico e um cálculo for sido iniciado, a função calculará as funções agregadas ponderadas pelo tempo para cada intervalo de tempo.

Example Exemplo de cenário de statetime

Considere um exemplo em que você tem um ativo com as seguintes propriedades:

- `Idle` – medida `0` ou `1`. Quando o valor é `1`, a máquina está ociosa.
- `Idle Time` – métrica que usa a fórmula `statetime(Idle)` para calcular a quantidade de tempo em segundos na qual a máquina está ociosa, por intervalo de 1 minuto.

A propriedade `Idle` tem os pontos de dados a seguir:

a função de hora	14:00:00	14:00:30	14:01:15	14:02:45	14:04:00
Idle	0	1	1	0	0

AWS IoT SiteWise calcula a `Idle Time` propriedade a cada minuto a partir dos valores de`Idle`. Depois que esse cálculo for concluído, a propriedade `Idle Time` terá os seguintes pontos de dados.

a função de hora	14:00:00	14:01:00	14:02:00	14:03:00	14:04:00
Idle Time	N/A	30	60	45	0

AWS IoT SiteWise executa os seguintes cálculos `Idle Time` no final de cada minuto.

- Às 14:00 (para 13:59 a 14:00)
  - Não há dados para `Idle` antes das 14:00, portanto nenhum ponto de dados é calculado.
- Às 14:01 (para 14:00 a 14:01)
  - Às 14:00:00, a máquina está ativa (`Idle` é `0`).
  - Às 14:00:30, a máquina está ociosa (`Idle` é `1`).

  - `Idle` não muda novamente antes do final do intervalo às 14:01:00, de maneira que `Idle Time` são 30 segundos.
- Às 14:02 (para 14:01 a 14:02)
  - Às 14:01:00, a máquina está ociosa (de acordo com o último ponto de dados às 14:00:30).
  - Às 14:01:15, a máquina ainda está ociosa.
  - `Idle` não muda novamente antes do final do intervalo às 14:02:00, de maneira que `Idle Time` são 60 segundos.
- Às 14:03 (para 14:02 a 14:03)
  - Às 14:02:00, a máquina está ociosa (de acordo com o último ponto de dados às 14:01:15).
  - Às 14:02:45, a máquina está ativa.
  - `Idle` não muda novamente antes do final do intervalo às 14:03:00, de maneira que `Idle Time` são 45 segundos.
- Às 14:04 (para 14:03 a 14:04)
  - Às 14:03:00, a máquina está ativa (de acordo com o último ponto de dados às 14:02:45).
  - `Idle` não muda novamente antes do final do intervalo às 14:04:00, de maneira que `Idle Time` são 0 segundos.

Example Exemplo TimeWeightedAvg e TimeWeightedStDev cenário

As tabelas a seguir fornecem exemplos de entradas e saídas para essas métricas de janela de um minuto: `Avg(x)`, `TimeWeightedAvg(x)`, `TimeWeightedAvg(x, "linear")`, `stDev(x)`, `timeWeightedStDev(x)`, `timeWeightedStDev(x, 'p')`

Exemplo de entrada para janela agregada de um minuto:

> **Note**
>
> Todos esses pontos de dados têm `GOOD` qualidade.

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

Saída de resultados agregados:

> **Note**
>
> Nenhum — resultado não produzido para esta janela.

Tempo	`Avg(x)`	`TimeWeighted Avg(x)`	`TimeWeighted Avg(X, "linear")`	`stDev(X)`	`timeWeighted StDev(x)`	`timeWeighted StDev(x, 'p')`
3:00:00	4	Nenhum	Nenhum	0	Nenhum	Nenhum
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	8.54400374531753	7.724054437220943	7.659416862050705
3:04:00	0	10	2,5	0	10.084389681792215	10
3:05:00	Nenhum	0	0	Nenhum	0	0

Usando funções temporais em transformações

Somente em transformações, você pode usar a função `pretrigger()` para recuperar o valor de qualidade `GOOD` de uma variável antes da atualização da propriedade que iniciou o cálculo da transformação atual.

Considere um exemplo em que um fabricante usa AWS IoT SiteWise para monitorar o status de uma máquina. O fabricante usa as seguintes medidas e transformações para representar o processo:

- Uma medida `current_state`, que pode ser 0 ou 1.
  - Se a máquina estiver no estado de limpeza, `current_state` é igual a 1.
  - Se a máquina estiver no estado de fabricação, `current_state` é igual a 1.
- Uma transformação `cleaning_state_duration` é igual a `if(pretrigger(current_state) == 1, timestamp(current_state) - timestamp(pretrigger(current_state)), none)`. Essa transformação retorna há quanto tempo a máquina está no estado de limpeza em segundos, no formato Unix epoch. Para obter mais informações, consulte Usando funções condicionais em expressões de fórmulas e a função a função de hora(s).

Se a máquina permanecer no estado de limpeza por mais tempo do que o esperado, o fabricante poderá investigar a máquina.

Você também pode usar a função `pretrigger()` em transformações multivariadas. Por exemplo, você têm duas medidas, chamadas `x` e `y`, e uma transformação, `z`,igual a `x + y + pretrigger(y)`. A tabela a seguir mostra os valores para `x`, `y` e `z` das 9:00 às 9:15.

> **Note**
>
> - Este exemplo pressupõe que os valores das medições cheguem em ordem cronológica. Por exemplo, o valor de `x` para 09:00 chega antes do valor de `x` para 09:05.
> - Se os pontos de dados das 9:05 chegarem antes dos pontos de dados das 9:05, `z` não será calculado às 9:05.
> - Se o valor de `x` para 9:05 chegar antes do valor de `x` para 09:00 e os valores de `y` chegarem cronologicamente, `z` será igual a `22 = 20 + 1 + 1` às 9:05

	09:00	09:05	09:10	09:15
`x`	10	20		30
`y`	1	2	3	
`z = x + y + pretrigger(y)`	y não recebe nenhum ponto de dados antes das 09:00. Portanto, `z` não é calculado às 09:00.	23 = 20 + 2 + 1 `pretrigger(y)` é igual a 1.	25 = 20 + 3 + 2 `x` não recebe um novo ponto de dados. `pretrigger(y)` é igual a 2.	36 = 30 + 3 + 3 y não recebe um novo ponto de dados. Portanto, `pretrigger(y)` é igual a 3 às 09:15.

Usando funções de data e hora em expressões de fórmula

Em transformações e métricas, você pode usar as funções de data e hora das seguintes formas:

- Recupere o a função de hora atual de um ponto de dados em UTC ou no fuso horário local.
- Estruture a função de horas com argumentos, como `year`, `month` e `day_of_month`.
- Extraia um período de tempo, como um ano ou mês, com o argumento `unix_time`.

Função	Descrição
`now()`	Retorna a data e a hora atuais, em segundos, no formato Unix epoch.
`timestamp()`	• Em transformações, a função retorna a função de hora, em segundos, da mensagem de entrada no formato Unix epoch. Somente em transformações, você pode realizar uma das seguintes ações: • Fornecer uma variável como argumento para a função. A função `timestamp(`*`variable-name`*`)` retorna a função de

Função	Descrição
	hora, em segundos, do valor de qualidade `GOOD` mais recente para a variável especificada no formato Unix epoch. Por exemplo, se seu ativo tiver uma propriedade de transformação chamada `Temperature_F` que use a fórmula `9/5 * Temperature_C` para converter cada ponto de dados de temperatura de Celsius para Fahrenheit, você pode usar a função `timestamp(Temperature_F)` para obter a função de hora do valor de qualidade mais recente `GOOD` da proprieda de `Temperature_F` . • Use a função `pretrigger()` como argumento para a função. A função `timestamp(pretrigger(` *`variable-name`* `))` retorna a função de hora, em segundos, do valor de qualidade `GOOD` da variável especificada [3] antes da atualização da propriedade que iniciou o cálculo da transformação atual, no formato Unix epoch. Para ter mais informações, consulte Usando funções temporais em transformações. • Nas métricas, a função retorna a função de hora recuperada no final da janela atual, em segundos, no formato Unix epoch.

Função	Descrição
`mktime(time_zone, year, month, day_of_month, hour, minute, second)`	Retorna o tempo de entrada, em segundos, no formato Unix epoch. Os seguintes requisitos se aplicam ao usar essa função: • O argumento do fuso horário deve ser uma string entre aspas (`'UTC'`). Se não especific ado, o fuso horário padrão será UTC. O argumento do fuso horário pode ser o primeiro ou o último argumento. • Os argumentos de ano, mês, dia do mês, hora, minuto e segundo devem estar em ordem. • Os argumentos de ano, mês e data são obrigatórios. Os seguintes limites se aplicam ao usar essa função: • `year` - valores válidos estão entre 1970 e 2250. • `month` - valores válidos estão entre 1 e 12. • `day-of-month` - valores válidos estão entre 1 e 31. • `hour` - valores válidos estão entre 0 e 23. • `minute` - valores válidos estão entre 0 e 59. • `second` - valores válidos estão entre 0 e 60. Ele pode ser um número de ponto flutuante. Exemplos: • `mktime(2020, 2, 29)`

Função	Descrição
	• `mktime('UTC+3', 2021, 12, 31, 22)` • `mktime(2022, 10, 13, 2, 55, 13.68, 'PST')`

Função	Descrição
`localtime(unix_time, time_zone)`	Retorna o ano, o dia do mês, o dia da semana, o dia do ano, a hora, o minuto ou o segundo no fuso horário especificado, a partir do horário Unix. Os seguintes requisitos se aplicam ao usar essa função: • O argumento do fuso horário deve ser uma string entre aspas (`'UTC'`). Se não especific ado, o fuso horário padrão será UTC. • O argumento Unix time é a hora em segundos, no formato Unix epoch. O intervalo válido é entre 1-3155688986440319 9. Ele pode ser um número de ponto flutuante. Exemplo de resposta: `2007-12-0 3T10:15:30+01:00[Europe/Paris]` `localtime(unix_time, time_zone ) ` não é uma função independente. As funções `year()`, `mon()`, `mday`, `wday()`, `yday()`, `hour()`, `minute()` e `sec()` usam `localtime(unix_time, time_zone)` como argumento. Exemplos: • `year(localtime('GMT', 160589860 8.8113723))` • `now().localtime().year()` • `timestamp().localtime('PST' ).year()`

Função	Descrição
	• `localtime(1605289736, 'Europe/London').year()`
`year(localtime(unix_time, time_zone)`	Retorna o ano de `localtime(unix_time, time_zone)` .
`mon(localtime(unix_time, time_zone))`	Retorna o mês a partir de `localtime (unix_time, time_zone)` .
`mday(localtime(unix_time, time_zone))`	Retorna o dia do mês a partir de `localtime (unix_time, time_zone)` .
`wday(localtime(unix_time, time_zone))`	Retorna o dia da semana a partir de `localtime(unix_time, time_zone)` .
`yday(localtime(unix_time, time_zone))`	Retorna o dia do ano a partir de `localtime (unix_time, time_zone)` .
`hour(localtime(unix_time, time_zone))`	Retorna a hora a partir de `localtime (unix_time, time_zone)` .
`minute(localtime(unix_time, time_zone))`	Retorna o minuto a partir de `localtime (unix_time, time_zone)` .
`sec(localtime(unix_time, time_zone))`	Retorna o segundo a partir de `localtime (unix_time, time_zone)` .

Formatos de fuso horário suportados

É possível especificar o argumento de fuso horário das seguintes maneiras:

- Deslocamento de fuso horário - especifique `'Z'` para UTC ou um deslocamento (`'+2'` ou`'-5'`).
- IDs de deslocamento - Combine uma abreviatura de fuso horário e um deslocamento. Por exemplo, `'GMT+2'` e `'UTC-01:00'`. A abreviatura do fuso horário deve conter apenas três letras.
- IDs baseadas na região - por exemplo, `'Etc/GMT+12'` e `'Pacific/Pago_Pago'`.

Abreviações de fuso horário suportadas

As funções de data e hora oferecem suporte às seguintes abreviações de fuso horário de três letras:

- EST - - 05:00
- HST - - 10:00
- MST - - 07:00
- ACT - Austrália/Darwin
- AET - Austrália/Sydney
- AGT - América/Argentina/Buenos_Aires
- ART - África/Cairo
- AST - América/Anchorage
- BRT - América/São Paulo
- BST - Ásia/Dhaka
- CAT - África/Harare
- CET - Europa/Paris
- CNT - América/St_Johns
- CST - América/Chicago
- CTT - Ásia/Xangai
- EAT - África/Addis_Ababa
- IET - América/Indiana/Indianápolis
- IST - Ásia/Kolkata
- JST - Ásia/Tóquio
- MIT - Pacífico/Apia
- NET - Ásia/Yerevan
- NST - Pacífico/Auckland
- PLT - Ásia/Karachi
- PRT - América/Porto Rico
- PST – América/Los_Angeles
- SST - Pacífico/Guadalcanal
- VST - Ásia/Ho_Chi_Minh

IDs baseados em região compatíveis

As funções de data e hora oferecem suporte aos seguintes IDs baseados em região, organizados por sua relação com 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)
- EUA/Samoa (UTC- 11:00)
- ETC/GMT+11 (UTC - 11:00)
- Pacífico/Midway (UTC - 11:00)
- Pacífico/Honolulu (UTC - 10:00)
- Pacífico/Rarotonga (UTC - 10:00)
- Pacífico/Taiti (UTC - 10:00)
- Pacífico/Johnston (UTC - 10:00)
- EUA/Havaí (UTC - 10:00)
- Sistema V/HST 10 (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)
- Sistema V/YST 9 (UTC - 10:00)
- América/Adak (UTC - 09:00)
- EUA/Aleutas (UTC - 09:00)
- ETC/GMT +8 (UTC - 18:00)
- EUA/Alasca (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)
- Sistema V/PST 8 (UTC - 08:00)
- América/Nome (UTC - 08:00)
- Sistema V/YST 9 YDT (UTC - 08:00)
- Canadá/Yukon (UTC - 07:00)
- EUA/Pacífico Novo (UTC - 07:00)
- ETC/GMT+7 (UTC - 07:00)
- EUA/Arizona (UTC- 07:00)
- América/Dawson_Creek (UTC - 07:00)
- Canadá/Pacífico (UTC - 07:00)
- PST 8 PDT (UTC - 07:00)
- Sistema V/MST 7 (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)
- Sistema V/PST8PDT (UTC - 07:00)
- América/Los_Angeles (UTC - 07:00)
- EUA/Pacífico (UTC - 07:00)
- América/El_Salvador (UTC- 06:00)

- América/Guatemala (UTC - 06:00)
- América/Belize (UTC - 06:00)
- América/Managua (UTC - 06:00)
- América/Tegucigalpa (UTC - 06:00)
- ETC/GMT+6 (UTC - 06:00)
- Pacífico/Páscoa (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/Mazatlan (UTC - 06:00)
- América/Boise (UTC - 06:00)
- América/Costa_Rica (UTC - 06:00)
- MST 7 MDT (UTC - 06:00)
- Sistema V/CST 6 (UTC - 06:00)
- América/Chihuahua (UTC - 06:00)
- América/Ojinaga (UTC - 06:00)
- Chile/ EasterIsland (UTC- 06:00)
- EUA/Montanha (UTC - 06:00)
- América/Edmonton (UTC - 06:00)
- Canadá/Montanha (UTC - 06:00)
- América/Cambridge_Bay (UTC - 06:00)
- Navajo (UTC - 06:00)
- Sistema V/MST 7 MDT (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/Geral (UTC- 05:00)
- América/Porto_Acre (UTC - 05:00)
- América/Guayaquil (UTC - 05:00)
- América/Rankin_Inlet (UTC - 05:00)
- EUA/Central (UTC - 05:00)
- América/Rainy_River (UTC - 05:00)
- América/Indiana/Knox (UTC - 05:00)
- América/Dakota do Norte/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 do Norte/Centro (UTC - 05:00)
- América/Cayman (UTC - 05:00)
- América/Indiana/Tell_City (UTC - 05:00)
- América/Cidade do México (UTC- 05:00)
- América/Matamoros (UTC - 05:00)
- CST 6 CDT (UTC - 05:00)
- América/Knox_IN (UTC - 05:00)
- América/Bogotá (UTC - 05:00)
- América/Menominee (UTC - 05:00)
- América/Resolute (UTC - 05:00)
- Sistema V/EST 5 (UTC - 05:00)
- Canadá/Central (UTC-05:00)
- Brasil/Acre (UTC - 05:00)

- América/Cancún (UTC - 05:00)
- América/Lima (UTC - 05:00)
- América/Bahia_Banderas (UTC - 05:00)
- US/Indiana-Starke (UTC - 05:00)
- América/Rio_Branco (UTC - 05:00)
- Sistema V/CST 6 CDT (UTC - 05:00)
- Jamaica (UTC - 05:00)
- América/Mérida (UTC - 05:00)
- América/Dakota do 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/Manaus (UTC - 04:00)
- América/Fort_Wayne (UTC - 04:00)
- América/St_Thomas (UTC - 04:00)
- América/Anguilla (UTC - 04:00)
- América/Havana (UTC - 04:00)
- EUA/Michigan (UTC - 04:00)
- América/Barbados (UTC - 04:00)
- América/Louisville (UTC - 04:00)
- América/Curaçao (UTC - 04:00)
- América/Guiana (UTC - 04:00)
- América/Martinica (UTC - 04:00)
- América/Porto Rico (UTC - 04:00)

- América/Port_of_Spain (UTC - 04:00)
- Sistema V/AST 4 (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/Assunção (UTC - 04:00)
- EST 5 EDT (UTC - 04:00)
- América/Nassau (UTC - 04:00)
- América/Kentucky/Monticello (UTC - 04:00)
- Brasil/Oeste (UTC - 04:00)
- América/Aruba (UTC - 04:00)
- America/Indiana/Indianapolis (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)
- EUA/Oriental (UTC - 04:00)
- Canadá/Oriental (UTC - 04:00)
- América/Porto Príncipe (UTC - 04:00)
- América/St_Barthelemy (UTC - 04:00)
- América/Nipigon (UTC - 04:00)

- US/Leste de Indiana (UTC - 04:00)
- América/St_Lucia (UTC - 04:00)
- América/Montserrat (UTC - 04:00)
- América/Lower_Princes (UTC - 04:00)
- América/Detroit (UTC - 04:00)
- América/Tortola (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/Nova_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)
- Sistema V/EST 5 EDT (UTC - 04:00)
- América/Argentina/Catamarca (UTC - 03:00)
- Canadá/Atlântico (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/Montevidéu (UTC - 03:00)
- Brasil/Leste (UTC - 03:00)
- América/Argentina/Mendoza (UTC - 03:00)

- América/Argentina/Rio_Gallegos (UTC - 03:00)
- América/Catamarca (UTC - 03:00)
- América/Córdoba (UTC - 03:00)
- América/São 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/Santarém (UTC - 03:00)
- Atlântico/Bermudas (UTC - 03:00)
- América/Maceió (UTC - 03:00)
- Atlântico/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/Belém (UTC - 03:00)
- América/Jujuy (UTC - 03:00)
- América/Bahia (UTC - 03:00)
- América/Goose_bay (UTC - 03:00)

- América/Argentina/San_Juan (UTC - 03:00)
- América/Argentina/ ComodRivadavia (UTC- 03:00)
- América/Argentina/Tucuman (UTC - 03:00)
- América/Rosário (UTC - 03:00)
- Sistema V/AST 4 ADT (UTC - 03:00)
- América/Argentina/Buenos Aires (UTC - 03:00)
- América/St_Johns (UTC - 02:30)
- Canadá/Terra Nova (UTC - 02:30)
- América/Miquelon (UTC - 02:00)
- ETC/GMT+2 (UTC - 02:00)
- América/Godthab (UTC - 02:00)
- América/Noronha (UTC - 02:00)
- Brasil/ DeNoronha (UTC- 02:00)
- Atlântico/South_Georgia (UTC - 02:00)
- ETC/GMT+2 (UTC - 01:00)
- Atlântico/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/Fiji (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 Sul (UTC+ 12:00)
- Pacífico/Tarawa (UTC+ 12:00)
- Pacífico/Auckland (UTC+ 12:00)
- Ásia/Kamchatka (UTC+ 12:00)
- ETC/GMT-12 (UTC + 12:00)
- Ásia/Anadyr (UTC + 12:00)
- Pacífico/Majuro (UTC + 12:00)
- Pacífico/Ponape (UTC + 11:00)
- Pacífico/Bougainville (UTC + 11:00)
- Antártica/Macquarie (UTC + 11:00)
- Pacífico/Pohnpei (UTC + 11:00)
- Pacífico/Efate (UTC + 11:00)
- Pacífico/Norfolk (UTC + 11:00)
- Ásia/Magadan (UTC + 11:00)
- Pacífico/Kosrae (UTC + 11:00)
- Ásia/Sakhalin (UTC + 11:00)
- Pacífico/Noumea (UTC + 11:00)
- ETC/GMT-11 (UTC + 11:00)
- Ásia/Srednekolymsk (UTC + 11:00)
- Pacífico/Guadalcanal (UTC + 11:00)
- Austrália/Lord_Howe (UTC + 10:30)
- Austrália/LHI (UTC + 10:30)
- Austrália/Hobart (UTC + 10:00)
- Pacífico/Yap (UTC + 10:00)

- Austrália/Tasmânia (UTC + 10:00)
- Pacífico/Porto_Moresby (UTC + 10:00)
- Austrália/ACT (UTC + 10:00)
- Austrália/Victoria (UTC + 10:00)
- Pacífico/Chuuk (UTC + 10:00)
- Austrália/Queensland (UTC + 10:00)
- Austrália/Canberra (UTC + 10:00)
- Austrália/Currie (UTC + 10:00)
- Pacífico/Guam (UTC + 10:00)
- Pacífico/Truk (UTC + 10:00)
- Austrália/NSW (UTC + 10:00)
- Ásia/Vladivostok (UTC + 10:00)
- Pacífico/Saipan (UTC + 10:00)
- Antártica/Dumont Durville (UTC + 10:00)
- Austrália/Sydney (UTC + 10:00)
- Austrália/Brisbane (UTC + 10:00)
- ETC/GMT-10 (UTC + 12:00)
- Ásia/Ust-Nera (UTC + 10:00)
- Austrália/Melbourne (UTC + 10:00)
- Austrália/Lindeman (UTC + 10:00)
- Austrália/Norte (UTC + 09:30)
- Austrália/Yancowinna (UTC + 09:30)
- Austrália/Adelaide (UTC + 09:30)
- Austrália/Broken_Hill (UTC + 09:30)
- Austrália/Sul (UTC + 09:30)
- Austrália/Darwin (UTC + 09:30)
- ETC/GMT-9 (UTC + 12:00)
- Pacífico/Palau (UTC + 09:00)
- Ásia/Chita (UTC + 09:00)

- Ásia/Díli (UTC + 09:00)
- Ásia/Jayapura (UTC + 09:00)
- Ásia/Yakutsk (UTC + 09:00)
- Ásia/Pyongyang (UTC + 09:00)
- ROK (UTC + 09:00)
- Ásia/Seul (UTC + 09:00)
- Ásia/Khandyga (UTC + 09:00)
- Japão (UTC + 09:00)
- Ásia/Tóquio (UTC + 09:00)
- Austrália/Eucla (UTC + 08:45)
- Ásia/Kuching (UTC + 08:00)
- Ásia/Chungking (UTC + 08:00)
- ETC/GMT-8 (UTC + 08:00)
- Austrália/Perth (UTC+ 08:00)
- Ásia/Macau (UTC + 08:00)
- Ásia/Macau (UTC+ 08:00)
- Ásia/Choibalsan (UTC + 08:00)
- Ásia/Xangai (UTC + 08:00)
- Antártica/Casey (UTC + 08:00)
- Ásia/Ulan_Bator (UTC + 08:00)
- Ásia/Chongqing (UTC + 08:00)
- Ásia/Ulaanbaatar (UTC + 08:00)
- Ásia/Taipei (UTC + 08:00)
- Ásia/Manila (UTC + 8:00)
- PRC (UTC + 08:00)
- Ásia/Ujung_Pandang (UTC + 08:00)
- Ásia/Harbin (UTC + 08:00)
- Cingapura (UTC + 08:00)
- Ásia/Brunei (UTC + 08:00)

- Austrália/Oeste (UTC + 08:00)
- Ásia/Hong_Kong (UTC + 08:00)
- Ásia/Makassar (UTC + 08:00)
- Hong Kong (UTC+ 08:00)
- Ásia/Kuala_Lumpur (UTC + 08:00)
- Ásia/Irkutsk (UTC + 08:00)
- Ásia/Cingapura (UTC + 08:00)
- Ásia/Pontianak (UTC + 07:00)
- ETC/GMT-7 (UTC + 07:00)
- Ásia/Phnom_Penh (UTC + 07:00)
- Ásia/Novosibirsk (UTC + 07:00)
- Antártica/Davis (UTC + 07:00)
- Ásia/Tomsk (UTC + 07:00)
- Ásia/Jacarta (UTC + 07:00)
- Ásia/Barnaul (UTC + 07:00)
- Índia/Natal (UTC + 07:00)
- Ásia/Ho_Chi_Minh (UTC + 07:00)
- Ásia/Hovd (UTC + 07:00)
- Ásia/Bangkok (UTC + 07:00)
- Ásia/Vientiane (UTC + 07:00)
- Ásia/Novokuznetsk (UTC + 07:00)
- Ásia/Krasnoyarsk (UTC + 07:00)
- Ásia/Saigon (UTC + 07:00)
- Ásia/Yangon (UTC+ 06:30)
- Ásia/Tangoon (UTC+ 06:30)
- Índia/Cocos (UTC + 06:30)
- Ásia/Kashgar (UTC + 06:00)
- ETC/GMT-6 (UTC + 06:00)
- Ásia/Almaty (UTC + 06:00)

- Ásia/Daca (UTC + 06:00)
- Ásia/Omsk (UTC + 06:00)
- Ásia/Dhaka (UTC + 06:00)
- Índia/Chagos (UTC + 06:00)
- Ásia/Qyzylorda (UTC + 06:00)
- Ásia/Bishkek (UTC + 06:00)
- Antártica/Vostok (UTC + 06:00)
- Ásia/Urumqi (UTC + 06:00)
- Ásia/Thimbu (UTC + 06:00)
- Ásia/Thimphu (UTC + 06:00)
- Ásia/Katmandu (UTC + 05:45)
- Ásia/Katmandu (UTC+ 05:45)
- Ásia/Calcutá (UTC + 05:30)
- Ásia/Colombo (UTC + 05:30)
- Ásia/Calcutá (UTC + 05:30)
- Ásia/Aqtau (UTC + 05:00)
- ETC/GMT-5 (UTC + 05:00)
- Ásia/Samarkand (UTC + 05:00)
- Ásia/Karachi (UTC + 05:00)
- Ásia/Ecaterimburgo (UTC + 05:00)
- Ásia/Dushanbe (UTC + 05:00)
- Índia/Maldivas (UTC + 05:00)
- Ásia/Oral (UTC + 05:00)
- Ásia/Tashkent (UTC + 05:00)
- Antártica/Mawson (UTC + 05:00)
- Ásia/Aqtobe (UTC + 05:00)
- Ásia/Ashkhabad (UTC + 05:00)
- Ásia/Ashgabat (UTC + 05:00)
- Ásia/Atyrau (UTC + 05:00)

- Índia/Kerguelen (UTC + 05:00)
- Irã (UTC + 04:30)
- Ásia/Teerã (UTC + 04:30)
- Ásia/Cabul (UTC + 04:30)
- Ásia/Yerevan (UTC + 04:00)
- ETC/GMT-4 (UTC + 04:00)
- ETC/GMT-4 (UTC + 04:00)
- Ásia/Dubai (UTC + 04:00)
- Índia/Reunião (UTC + 04:00)
- Europa/Saratov (UTC + 04:00)
- Europa/Samara (UTC + 04:00)
- Índia/Mahé (UTC + 04:00)
- Ásia/Baku (UTC + 04:00)
- Ásia/Muscat (UTC + 04:00)
- Europa/Volgograd (UTC + 04:00)
- Europa/Astrakhan (UTC + 04:00)
- Ásia/Tbilisi (UTC + 04:00)
- Europa/Ulyanovsk (UTC + 04:00)
- Ásia/Aden (UTC + 03:00)
- África/Nairobi (UTC + 03:00)
- Europa/Istambul (UTC + 03:00)
- ETC/GMT-3 (UTC + 03:00)
- Europa/Zaporozhye (UTC + 03:00)
- Israel (UTC + 03:00)
- Índia/Comores (UTC + 03:00)
- Antártica/Syowa (UTC + 03:00)
- África/Mogadíscio (UTC + 03:00)
- Europa/Bucareste (UTC + 03:00)
- África/Asmera (UTC + 03:00)

- Europa/Mariehamn (UTC + 03:00)
- Ásia/Istambul (UTC + 03:00)
- Europa/Tiraspol (UTC + 03:00)
- Europa/Moscou (UTC + 03:00)
- Europa/Chisinau (UTC + 03:00)
- Europa/Helsinque (UTC + 03:00)
- Ásia/Beirute (UTC + 03:00)
- Ásia/Tel_Aviv (UTC + 03:00)
- África/Djibouti (UTC + 03:00)
- Europa/Simferopol (UTC + 03:00)
- Europa/Sofia (UTC + 03:00)
- Ásia/Gaza (UTC + 03:00)
- África/Asmara (UTC + 03:00)
- Europa/Riga (UTC + 03:00)
- Ásia/Bagdá (UTC + 03:00)
- Ásia/Damasco (UTC + 03:00)
- África/Dar_es_Salaam (UTC + 03:00)
- África/Addis_Ababa (UTC + 03:00)
- Europa/Uzhgorod (UTC + 03:00)
- Ásia/Jerusalém (UTC + 03:00)
- Ásia/Riyadh (UTC + 03:00)
- Ásia/Kuwait (UTC + 03:00)
- Europa/Kirov (UTC + 03:00)
- África/Kampala (UTC + 03:00)
- Europa/Minsk (UTC + 03:00)
- Ásia/Catar (UTC + 03:00)
- Europa/Kiev (UTC+ 03:00)
- Ásia/Bahrain (UTC+ 03:00)
- Europa/Vilnius (UTC + 03:00)

- Índia/Antananarivo (UTC + 03:00)
- Índia/Mayotte (UTC + 03:00)
- Europa/Tallinn (UTC + 03:00)
- Turquia (UTC + 03:00)
- África/Juba (UTC + 03:00)
- Ásia/Nicósia (UTC + 03:00)
- Ásia/Famagusta (UTC + 03:00)
- W-SU (UTC + 03:00)
- EET (UTC + 03:00)
- Ásia/Hebron (UTC + 03:00)
- Ásia/Amã (UTC + 03:00)
- Europa/Nicósia (UTC + 03:00)
- Europa/Atenas (UTC + 03:00)
- África/Cairo (UTC + 02:00)
- África/Mbabane (UTC + 02:00)
- Europa/Bruxelas (UTC + 02:00)
- Europa/Varsóvia (UTC + 02:00)
- CET (UTC + 02:00)
- Europa/Luxemburgo (UTC + 02:00)
- ETC/GMT-2 (UTC + 02:00)
- Líbia (UTC + 02:00)
- África/Kigali (UTC + 02:00)
- África/Tripoli (UTC + 02:00)
- Europa/Kaliningrado (UTC + 02:00)
- África/Windhoek (UTC + 02:00)
- Europa/Malta (UTC + 02:00)
- Europa/Busingen (UTC + 02:00)
-
- Europa/Skopje (UTC + 02:00)

- Europa/Sarajevo (UTC + 02:00)
- Europa/Roma (UTC + 02:00)
- Europa/Zurique (UTC + 02:00)
- Europa/Gibraltar (UTC + 02:00)
- África/Lubumbashi (UTC + 02:00)
- Europa/Vaduz (UTC + 02:00)
- Europa/Liubliana (UTC + 02:00)
- Europa/Berlim (UTC + 02:00)
- Europa/Estocolmo (UTC + 02:00)
- Europa/Budapeste (UTC + 02:00)
- Europa/Zagreb (UTC + 02:00)
- Europa/Paris (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/Tirane (UTC+ 02:00)
- MET (UTC + 03:00)
- Europa/Amsterdã (UTC + 02:00)
- África/Maputo (UTC + 02:00)
- Europa/San_Marino (UTC + 02:00)
- Polônia (UTC + 02:00)
- Europa/Andorra (UTC + 02:00)
- Europa/Oslo (UTC + 02:00)
- Europa/Podgorica (UTC + 02:00)
- África/Bujumbura (UTC + 02:00)
- Atlântico/Jan_Mayen (UTC + 02:00)
- África/Maseru (UTC + 02:00)

- Europa/Madri (UTC + 02:00)
- África/Blantyre (UTC + 02:00)
- África/Lusaka (UTC + 02:00)
- África/Harare (UTC + 02:00)
- África/Khartoum (UTC + 02:00)
- África/Joanesburgo (UTC + 02:00)
- Europa/Belgrado (UTC + 02:00)
- Europa/Bratislava (UTC + 02:00)
- Ártico/Longyearbyen (UTC + 02:00)
- Egito (UTC + 02:00)
- Europa/Vaticano (UTC + 02:00)
- Europa/Mônaco (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/Tunísia (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/Ndjamena (UTC + 01:00)
- Atlântico/Faroé (UTC + 01:00)
- Eire (UTC + 01:00)
- Atlântico/Faroé (UTC+ 01:00)
- Europa/Dublin (UTC + 01:00)

- África/Libreville (UTC + 01:00)
- África/El_Aaiun (UTC + 01:00)
- África/El_Aaiun (UTC + 01:00)
- África/Douala (UTC+ 01:00)
- África/Brazzaville (UTC + 01:00)
- África/Porto Novo (UTC + 01:00)
- Atlântico/Madeira (UTC + 01:00)
- Europa/Lisboa (UTC + 01:00)
- Atlântico/Canário (UTC + 01:00)
- África/Casablanca (UTC + 01:00)
- Europa/Belfast (UTC + 01:00)
- África/Luanda (UTC+ 01:00)
- África/Kinshasa (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)
- Atlântico/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/Conakry (UTC + 00:00)
- Universal (UTC + 00:00)
- África/Nouakchott (UTC + 00:00)
- UTC (UTC + 00:00)
- ETC/Universal (UTC+ 00:00)
- Atlântico/Açores (UTC + 00:00)

- África/Abidjan (UTC + 00:00)
- África/Acra (UTC + 00:00)
- ETC/UCT (UTC + 00:00)
- GMT 0 (UTC + 00:00)
- Zulu (UTC+ 00:00) Zulu (UTC + 00:00)
- África/Ouagadougou (UTC + 00:00)
- Atlântico/Reykjavik (UTC + 00:00)
- Etc/Zulu (UTC + 00:00)
- Islândia (UTC + 00:00)
- África/Lomé (UTC + 00:00)
- Greenwich (UTC + 00:00)
- ETC/GMT 0 (UTC + 00:00)
- América/Danmarkshavn (UTC + 00:00)
- África/Dakar (UTC + 00:00)
- África/Bissau (UTC + 00:00)
- ETC/Greenwich (UTC + 00:00)
- África/Timbuktu (UTC + 00:00)
- UCT (UTC + 00:00)
- África/Monróvia (UTC + 00:00)
- ETC/UTC (UTC + 00:00)

Tutoriais de expressão de fórmulas

Você pode seguir esses tutoriais para usar expressões de fórmula em AWS IoT SiteWise.

Tópicos

- Valores indefinidos, infinitos e excedidos

Usando cadeias de caracteres em fórmulas

Você pode operar em strings em suas expressões de fórmula. Você também pode inserir cadeias de caracteres de variáveis que fizerem referência a propriedades de atributos e medidas.

> **Important**
>
> As expressões de fórmula só podem produzir valores duplos ou de string. Expressões aninhadas podem gerar outros tipos de dados, como strings, mas a fórmula como um todo deve ser avaliada como um número ou string. Você pode usar a função jp para converter uma string em um número. O valor Booleano deve ser 1 (verdadeiro) ou 0 (falso). Para ter mais informações, consulte Valores indefinidos, infinitos e excedidos.

AWS IoT SiteWise fornece os seguintes recursos de expressão de fórmula que você pode usar para operar em cadeias de caracteres:

- Literais string
- O operador de índice (`s[index]`)
- O operador de fatia (`s[start:end:step]`)
- Funções de comparação, que você pode usar para comparar strings por ordem lexicográfica
- Funções de string, que incluem a `jp` função que pode analisar objetos JSON serializados e converter strings em números

Como filtrar pontos de dados

Você pode usar a função if para filtrar pontos de dados que não atendam a uma condição. A função `if` avalia uma condição e retorna valores diferentes para resultados `true` e `false`. Você pode usar a constante nula como saída para um caso de função `if`, para descartar o ponto de dados desse caso.

Para filtrar pontos de dados que correspondam a uma condição

- Crie uma transformação que use a função `if` para definir uma condição que verifica se uma outra foi atendida e retornar `none` como valor `result_if_true` ou `result_if_false`.

Example Exemplo: filtrar pontos de dados onde a água não esteja fervendo

Considere um cenário onde você tenha uma medição `temp_c` que forneça a temperatura (em Celsius) da água em uma máquina. Você pode definir a seguinte transformação para filtrar os pontos de dados nos quais a água não estiver fervendo:

- Transformar: `boiling_temps = if(gte(temp_c, 100), temp_c, none)` — retorna a temperatura se maior ou igual a 100 graus Celsius, caso contrário, não retornará nenhum ponto de dados.

Contando pontos de dados que correspondam a uma condição

Você pode usar funções comparativas e soma () para contar o número de pontos de dados para os quais uma condição é verdadeira.

Para contar pontos de dados que correspondam a uma condição

1. Crie uma transformação que use uma função comparativa para definir uma condição de filtro em outra propriedade.
2. Crie uma métrica que some os pontos de dados onde essa condição é atendida.

Example Exemplo: contar o número de pontos de dados onde a água está fervendo

Considere um cenário onde você tenha uma medição `temp_c` que forneça a temperatura (em Celsius) da água em uma máquina. Você pode definir as seguintes propriedades de transformação e métrica para contar o número de pontos de dados onde a água está fervendo:

- Transformação: `is_boiling = gte(temp_c, 100)` – Retorna 1 se a temperatura for maior ou igual a 100 graus Celsius, caso contrário, retorna `0`.
- Métrica: `boiling_count = sum(is_boiling)` – Retorna o número de pontos de dados onde a água estiver fervendo.

Dados atrasados em fórmulas

AWS IoT SiteWise suporta a ingestão tardia de dados com até 7 dias. Quando AWS IoT SiteWise recebe dados atrasados, ele recalcula os valores existentes para qualquer métrica que insira os dados atrasados em uma janela anterior. Esses recálculos resultam em cobranças de processamento de dados.

> **Note**
>
> Ao AWS IoT SiteWise computar propriedades que inserem dados atrasados, ele usa a expressão de fórmula atual de cada propriedade.

Depois de AWS IoT SiteWise recalcular uma janela anterior para uma métrica, ela substitui o valor anterior dessa janela. Se você ativou as notificações para essa métrica, AWS IoT SiteWise também emitirá uma notificação de valor de propriedade. Isso significa que você pode receber uma nova notificação de atualização de valor de propriedade para a mesma propriedade e notificação de hora para aquelas cuja notificação você tenha recebido anteriormente. Se seus aplicativos ou data lakes consumirem notificações de valor de propriedade, você deve atualizar o valor anterior com o novo valor para que os dados estejam precisos.

Qualidade de dados em fórmulas

Em AWS IoT SiteWise, cada ponto de dados tem um código de qualidade, que pode ser um dos seguintes:

- `GOOD` – os dados não são afetados por nenhum problema.
- `BAD` – os dados são afetados por um problema, como a falha do sensor.
- `UNCERTAIN` – os dados são afetados por um problema, como a imprecisão do sensor.

AWS IoT SiteWise consome somente dados `GOOD` de qualidade ao computar transformações e métricas. AWS IoT SiteWise gera somente dados `GOOD` de qualidade para cálculos bem-sucedidos. Se um cálculo não for bem-sucedido, AWS IoT SiteWise não produzirá um ponto de dados para esse cálculo. Isso pode ocorrer se uma computação resultar em um valor indefinido, infinito ou em um estouro.

Para obter mais informações sobre como consultar dados e filtrar por qualidade de dados, consulte Consultar dados de AWS IoT SiteWise.

Valores indefinidos, infinitos e excedidos

Algumas expressões de fórmula (como `x / 0`, `sqrt(-1)`, `oulog(0)`) calculam valores indefinidos em um sistema numérico real, infinitos ou fora do intervalo suportado por AWS IoT SiteWise. Quando a expressão de uma propriedade de ativo computa um valor indefinido, infinito ou excedente, AWS IoT SiteWise não gera um ponto de dados para esse cálculo.

AWS IoT SiteWise também não gera um ponto de dados se computar um valor não numérico como resultado de uma expressão de fórmula. Isso significa que, se você definir uma fórmula que calcula uma string, matriz ou constante nenhuma, então o AWS IoT SiteWise não irá gerar um ponto de dados para esse cálculo.

Example Exemplos

Cada uma das expressões de fórmula a seguir resulta em um valor que não AWS IoT SiteWise pode ser representado como um número. AWS IoT SiteWise não gera um ponto de dados quando calcula essas expressões de fórmula.

- `x / 0` é indefinido.
- `log(0)` é indefinido.
- `sqrt(-1)` é indefinido em um sistema numérico real.
- `"hello" + " world"` é uma string.
- `jp('{"values":[3,6,7]}', '$.values')` é uma matriz.
- `if(gte(temp, 300), temp, none)` é `none` quando `temp` é menor que `300`.

Criação de modelos compostos personalizados (componentes)

Modelos compostos personalizados, ou componentes, se você estiver usando o console, fornecem outro nível de organização para seus modelos de ativos e modelos de componentes. Você pode usá-los para estruturar seus modelos agrupando propriedades ou referenciando outros modelos. Para obter mais informações sobre como trabalhar com modelos compostos personalizados, consulteModelos compostos personalizados (componentes).

Você cria um modelo composto personalizado dentro de um modelo de ativo ou modelo de componente existente. Há dois tipos de modelos compostos personalizados. Para agrupar propriedades relacionadas em um modelo, você pode criar um modelo composto personalizado em linha. Para referenciar um modelo de componente em seu modelo de ativo ou modelo de componente, você pode criar um modelo composto personalizado baseado em modelo de componente.

As seções a seguir descrevem como usar a AWS IoT SiteWise API para criar modelos compostos personalizados.

Tópicos

- Criação de um componente embutido (console)

- Criação de um modelo composto personalizado em linha ()AWS CLI
- Criando um component-model-based componente (console)
- Criação de um modelo composto component-model-based personalizado ()AWS CLI

Criação de um componente embutido (console)

Você pode usar o AWS IoT SiteWise console para criar um componente embutido que define suas próprias propriedades.

> **Note**
>
> Como esse é um componente embutido, essas propriedades se aplicam somente ao modelo de ativo atual e não são compartilhadas em nenhum outro lugar.
> Se você precisar produzir um modelo reutilizável (por exemplo, para compartilhar entre vários modelos de ativos ou incluir várias instâncias em um modelo de ativo), você deve criar um componente com base em um modelo de componente. Consulte a seção a seguir para obter detalhes.

Para criar um componente (console)

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Modelos.
3. Escolha o modelo de ativo ao qual você deseja adicionar um componente.
4. Na guia Propriedades, escolha Componentes.
5. Escolha Criar componente.
6. Na página Criar componente, faça o seguinte:

    a. Insira um nome para o componente, como **`ServoMotor`** ou**`ServoMotor Model`**. Esse nome deve ser exclusivo em todos os componentes da sua conta nessa região.

    b. (Opcional) Adicione Definições de atributo ao modelo. Os atributos representam informações que raramente mudam. Para ter mais informações, consulte Definindo dados estáticos (atributos).

    c. (Opcional) Adicione Definições de medição ao modelo. As medições representam fluxos de dados do seu equipamento. Para ter mais informações, consulte Definindo fluxos de dados do equipamento (medições).

d. (Opcional) Adicione Definições de transformação ao modelo. As transformações são fórmulas que mapeiam dados de um formulário para outro. Para ter mais informações, consulte Transformando dados (transformações).

e. (Opcional) Adicione Definições de métrica ao modelo. Métricas são fórmulas que agregam dados em intervalos de tempo. As métricas podem inserir dados de entrada de ativos associados, para que você possa calcular valores que representem sua operação ou um subconjunto de sua operação. Para ter mais informações, consulte Agregando dados de propriedades e outros ativos (métricas).

f. Escolha Criar componente.

Criação de um modelo composto personalizado em linha ()AWS CLI

Você pode usar o AWS Command Line Interface (AWS CLI) para criar um modelo composto personalizado em linha que define suas próprias propriedades.

Use a operação CreateAssetModelCompositeModel para criar um modelo em linha com propriedades. Essa operação espera uma carga útil com a seguinte estrutura.

> **Note**
>
> Como esse é um modelo composto em linha, essas propriedades se aplicam somente ao modelo de ativo atual e não são compartilhadas em nenhum outro lugar. O que o torna "embutido" é que ele não fornece um valor para o `composedAssetModelId` campo.
> Se você precisar produzir um modelo reutilizável (por exemplo, para compartilhar entre vários modelos de ativos ou incluir várias instâncias em um modelo de ativo), crie um modelo composto baseado em modelo de componente. Consulte a seção a seguir para obter detalhes.

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

Criando um component-model-based componente (console)

Você pode usar o AWS IoT SiteWise console para criar um componente com base em um modelo de componente.

Para criar um component-model-based componente (console)

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Modelos.
3. Escolha o modelo de ativo ao qual você deseja adicionar um componente.
4. Na guia Propriedades, escolha Componentes.
5. Escolha Criar componente.
6. Na página Criar componente, faça o seguinte:
    a. Selecione o modelo de componente no qual você deseja basear o componente.
    b. Insira um nome para o componente, como **`ServoMotor`** ou**`ServoMotor Model`**. Esse nome deve ser exclusivo em todos os componentes da sua conta nessa região.
    c. Escolha Criar componente.

Criação de um modelo composto component-model-based personalizado ()AWS CLI

Você pode usar o AWS CLI para criar um modelo composto component-model-based personalizado dentro do seu modelo de ativo. Um modelo composto component-model-based personalizado é uma referência a um modelo de componente que você já definiu em outro lugar.

Use a operação CreateAssetModelCompositeModel para criar um modelo composto component-model-based personalizado. Essa operação espera uma carga útil com a seguinte estrutura.

> **Note**
>
> Neste exemplo, o valor de `composedAssetModelId` é a ID do modelo de ativo ou a ID externa de um modelo de componente existente. Para obter mais informações, consulte Referenciando objetos com IDs externos no Guia de Usuário AWS IoT SiteWise . Para obter um exemplo de como criar um modelo de componente, consulteCriando um modelo de componente (AWS CLI).

```
{
    "assetModelCompositeModelName": "CNCLathe_ServoMotorA",
    "assetModelCompositeModelType": "CUSTOM",
    "composedAssetModelId": component model ID
]
```

Como é apenas uma referência, um modelo composto component-model-based personalizado não tem propriedades próprias, além de um nome.

Se você quiser adicionar várias instâncias do mesmo componente ao seu modelo de ativos (por exemplo, uma máquina CNC com vários servomotores), você pode adicionar vários modelos compostos component-model-based personalizados, cada um com seu próprio nome, mas que fazem referência ao mesmo. `composedAssetModelId`

Você pode agrupar componentes em outros componentes. Para fazer isso, você pode adicionar um modelo component-model-based composto, conforme mostrado neste exemplo, a um dos seus modelos de componentes.

Criação de ativos

É possível criar um ativo de um modelo de ativo. Você deve ter um modelo de ativo para criar um ativo. Se você ainda não tiver criado um modelo de ativo, consulte Criar modelos de ativo.

> **Note**
>
> Só é possível criar ativos a partir de modelos `ACTIVE`. Se o estado do seu modelo não for `ACTIVE`, talvez seja necessário aguardar alguns minutos para poder criar ativos a partir desse modelo. Para ter mais informações, consulte Estados de ativos e modelos.

Tópicos

Criar um ativo (console)

Você pode usar o AWS IoT SiteWise console para criar um ativo.

Como criar um ativo (console)

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Ativos.
3. Escolha Criar ativo.
4. Na página Criar ativo, faça o seguinte:
   a. Em Modelo, escolha o modelo de ativo a ser usado para criar um ativo.

      > **Note**
      >
      > Se o modelo não estiver ATIVO, você deverá aguardar até que ele esteja ativo ou resolver problemas se ele estiver COM FALHA.

   b. Insira um Nome para o ativo.
   c. (Opcional) Adicione tags ao ativo. Para ter mais informações, consulte Marcando seus recursos AWS IoT SiteWise.
   d. Escolha Criar ativo.

Quando você cria um ativo, o AWS IoT SiteWise console navega até a página do novo ativo. Nesta página, você pode ver o Status do ativo que, inicialmente, é CRIANDO. Essa página é atualizada automaticamente, para que você possa aguardar a atualização do status do ativo.

> **Note**
>
> O processo de criação de ativos pode levar até um minuto. Depois que o Status estiver ATIVO, você poderá executar operações de atualização no ativo. Para ter mais informações, consulte Estados de ativos e modelos.

Depois de criar um ativo, consulte Configurar um novo ativo.

Criação de um ativo (AWS CLI)

Você pode usar o AWS Command Line Interface (AWS CLI) para criar um ativo a partir de um modelo de ativo.

É necessário um `assetModelId` para criar um ativo. Se você criou um modelo de ativo, mas não o conhece`assetModelId`, use a API de ListAssetmodelos para visualizar todos os seus modelos de ativos.

Para criar um ativo a partir de um modelo de ativo, use a CreateAssetAPI com os seguintes parâmetros:

- `assetName` – o nome do novo ativo. Dê um nome ao seu ativo para ajudá-lo a identificá-lo.
- `assetModelId` – O ID do ativo. Esse é o ID real no formato UUID, ou `externalId:myExternalId` se ele tiver um. Para obter mais informações, consulte Referenciando objetos com IDs externos no Guia de Usuário AWS IoT SiteWise .

Para criar um ativo (AWS CLI)

- Execute o seguinte comando para criar um ativo. Substitua *`asset-name`* por um nome para o ativo e *`asset-model-id pelo ID ou ID externo`* do modelo de ativo.

```
aws iotsitewise create-asset \
  --asset-name asset-name \
```

```
  --asset-model-id asset-model-id
```

A operação retorna uma resposta que contém os detalhes do novo ativo e o status no formato a seguir.

```
{
  "assetId": "String",
  "assetArn": "String",
  "assetStatus": {
    "state": "String",
    "error": {
      "code": "String",
      "message": "String"
    }
  }
}
```

O ativo `state` é `CREATING` até que seja criado.

> **Note**
>
> O processo de criação de ativos pode levar até um minuto. Para verificar o status do seu ativo, use a DescribeAssetoperação com o ID do seu ativo como `assetId` parâmetro. Depois que o `state` do ativo estiver `ACTIVE`, você poderá executar operações de atualização no ativo. Para ter mais informações, consulte Estados de ativos e modelos.

Depois de criar um ativo, consulte Configurar um novo ativo.

Configurar um novo ativo

Conclua a configuração do ativo com as seguintes ações opcionais:

- Mapeamento de fluxos de dados industriais para propriedades de ativos se o ativo tiver propriedades de medição.
- Atualizar valores de atributo se o ativo tiver valores de atributo exclusivos.
- Associar e desassociar ativos se o ativo for um ativo pai.

Pesquisando ativos

Use a funcionalidade Console do AWS IoT SiteWise de pesquisa para encontrar ativos com base em metadados e filtros de valor de propriedades em tempo real.

Pré-requisitos

AWS IoT SiteWise requer permissões de integração AWS IoT TwinMaker para melhor organizar e modelar dados industriais. Se você concedeu permissões para AWS IoT SiteWise, use a ExecuteQueryAPI. Se você não concedeu permissões e precisa de ajuda para AWS IoT SiteWise começar, consulteIntegração do AWS IoT SiteWise e do AWS IoT TwinMaker.

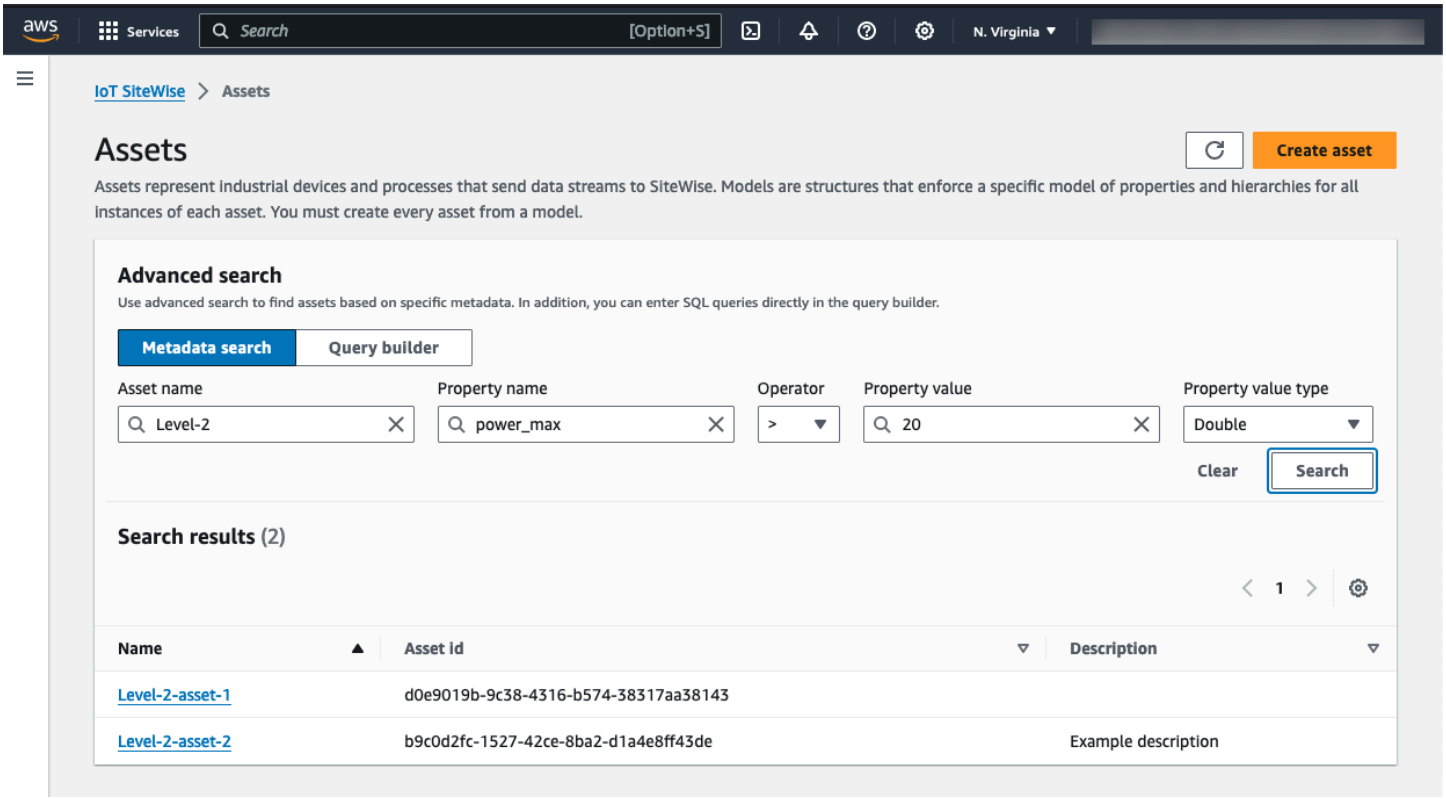
Pesquisa avançada em Console do AWS IoT SiteWise

Pesquisa de metadados

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, escolha Pesquisa avançada em Ativos.
3. Em Pesquisa avançada, escolha a opção Pesquisa de metadados.
4. Preencha os parâmetros. Preencha o máximo de campos possível para uma pesquisa eficiente.
    a. Nome do ativo — insira um nome completo do ativo ou parcial para uma pesquisa ampla.
    b. Nome da propriedade — insira um nome completo da propriedade ou um nome parcial para uma pesquisa ampla.
    c. Operador — Escolha um operador entre:
        - =
        - <
        - >
        - <=
        - >=
    d. Valor da propriedade — Esse valor é comparado com o valor mais recente da propriedade.
    e. Tipo de valor da propriedade — O tipo de dados da propriedade. Escolha uma das seguintes opções:
        - Duplo

- Inteiro
- String
- Booleano

5. Selecione a opção Pesquisar.
6. Na tabela de resultados da pesquisa, escolha o ativo na coluna Nome. Isso leva você à página detalhada do ativo.



Pesquisa parcial

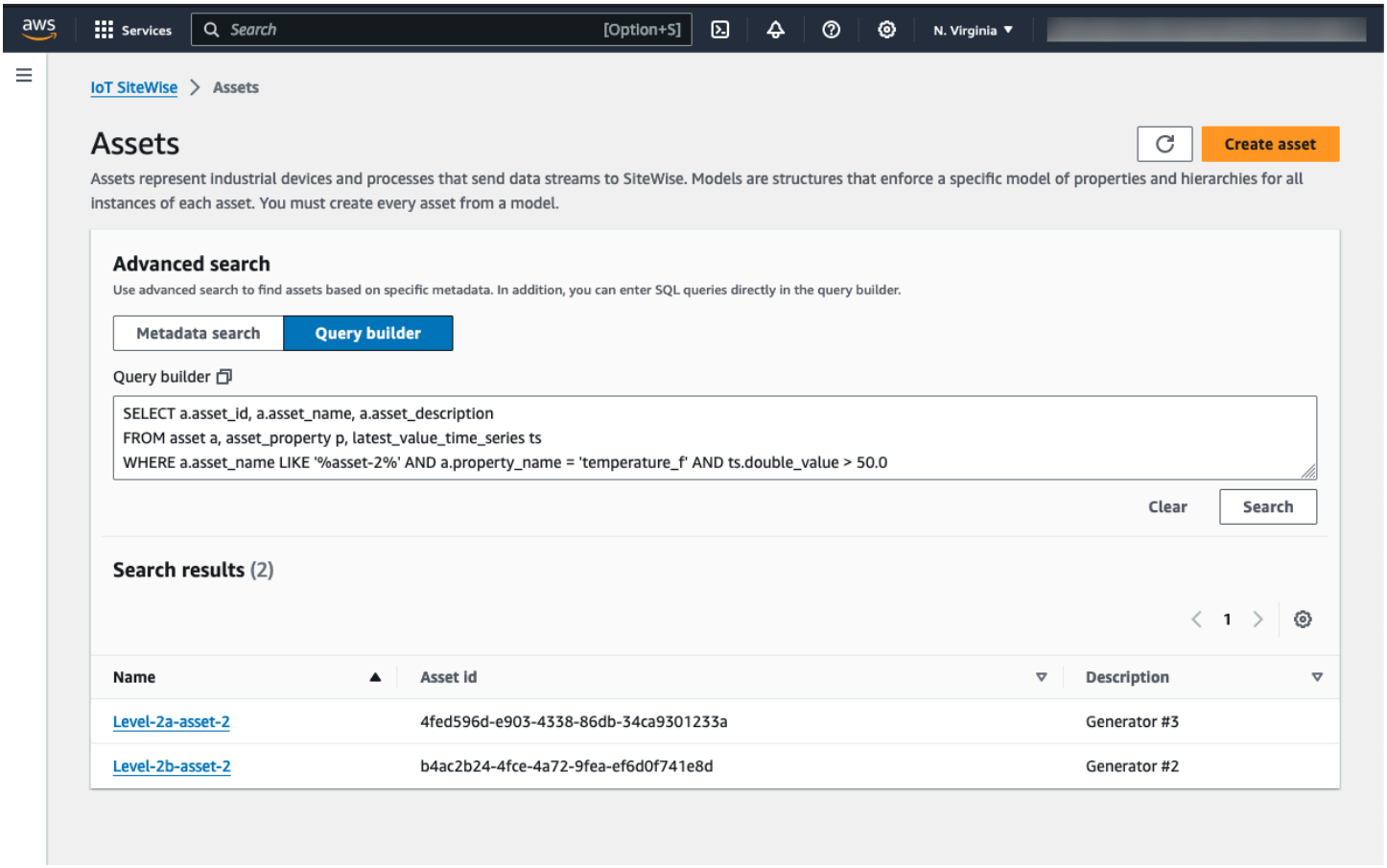
Nem todos os parâmetros precisam ser fornecidos para uma pesquisa de ativos. Aqui estão alguns exemplos de pesquisas parciais usando a opção de pesquisa de metadados:

- Encontre ativos pelo nome:
  - Insira um valor somente no campo Nome do ativo.
  - Os campos Nome da propriedade e Valor da propriedade estão vazios.
- Encontre ativos contendo propriedades com um nome específico:
  - Insira um valor somente no campo Nome da propriedade.

  - Os campos Nome do ativo e Valor da propriedade estão vazios.
- Encontre ativos com base nos valores mais recentes de suas propriedades:
  - Insira valores nos campos Nome da propriedade e Valor da propriedade.
  - Selecione um tipo de valor de Operador e Propriedade.

Pesquisa do Query Builder

1. Navegue até o Console do AWS IoT SiteWise.
2. No painel de navegação, escolha Pesquisa avançada em Ativos.
3. Em Pesquisa avançada, escolha a opção Criador de consultas.
4. No painel Criador de consultas, escreva sua consulta SQL para recuperar um `asset_name` e. `asset_id` `asset_description`
5. Selecione a opção Pesquisar.
6. Na tabela de resultados da pesquisa, escolha o ativo na coluna Nome. Isso leva você à página detalhada do ativo.



> **Note**
>
> - A `SELECT` cláusula na consulta SQL deve incluir os `asset_id` campos `asset_name` e para garantir um ativo válido na tabela de resultados da pesquisa.
> - O Criador de consultas exibe somente o nome, a ID do ativo e a descrição na tabela de resultados. Adicionar mais campos à `SELECT` cláusula não adiciona mais colunas à tabela de resultados

Mapeamento de fluxos de dados industriais para propriedades de ativos

Você pode definir um alias de propriedade na propriedade do ativo. Isso ajuda você a identificar uma propriedade do ativo ao ingerir ou recuperar dados do ativo. Se o ativo tiver propriedades de medição, será possível definir os apelidos das propriedades para mapear os fluxos de dados para essas propriedades de medição.

Esse processo requer conhecer o apelido da sua propriedade.

- Se você ingerir dados de servidores OPC-UA usando uma fonte de dados OPC-UA em um gateway SiteWise Edge, seu alias de propriedade é o caminho para uma variável no nó Objetos, começando com. `/`

  Example

  Se o caminho para sua variável for`company/windfarm/3/turbine/7/temperature`, então seu alias de propriedade é`/company/windfarm/3/turbine/7/temperature`.

  Para obter mais informações sobre a arquitetura de informações do OPC-UA, consulte Modelo de informações e mapeamento do espaçamento de endereços na Referência Online do OPC UA.

  > Observações
  >
  > - Se você configurar um prefixo do fluxo de dados para a origem do OPC-UA, será necessário incluir esse prefixo no apelido da propriedade em todos os fluxos de dados dessa origem.
  >
  >   Example
  >
  >   Se `/RentonWA` for um prefixo, o alias anterior será. `/RentonWA/company/windfarm/3/turbine/7/temperature`
  > - Os apelidos de propriedades podem conter até 1.000 bytes. Os caminhos de variáveis do OPC-UA podem conter até 4.096 bytes. Atualmente, AWS IoT SiteWise não suporta a ingestão de dados de variáveis OPC-UA com caminhos longos.

- Se você ingerir dados de servidores Modbus usando uma fonte de dados Modbus TCP em um gateway SiteWise Edge, o alias de sua propriedade é:

  Modbus `register set tag name`

  Use esse valor para enviar dados desse conjunto de registros para uma propriedade do ativo.

- Se você ingerir dados de outras fontes, como o uso de AWS IoT regras ou da API, deverá definir seus aliases de propriedade. É possível definir um sistema de nomenclatura de apelido de propriedade aplicável à configuração do seu dispositivo. Por exemplo, se você ingerir dados de coisas AWS IoT , será possível incluir o nome da coisa nos apelidos de propriedade para

identificar os fluxos de dados de forma exclusiva. Para obter mais informações sobre esse exemplo, consulte o tutorial Como ingerir dados de AWS IoT coisas.

Os aliases de propriedade devem ser exclusivos dentro de uma região e AWS conta. AWS IoT SiteWise retornará um erro se você definir um alias de propriedade como um que já existe em outra propriedade do ativo.

Se você tiver várias fontes OPC-UA com caminhos de fluxo de dados idênticos, adicione um prefixo aos caminhos de cada fonte para formar aliases exclusivos. Para ter mais informações, consulte Configurar fontes de dados.

> **Note**
>
> Esta seção descreve como definir apelidos de propriedades para propriedades de medição. Para obter mais informações sobre como definir apelidos de propriedades para propriedades externas de estado de alarme, consulte Mapear fluxos externos de estado de alarme.

Tópicos

Definir um apelido de propriedade (console)

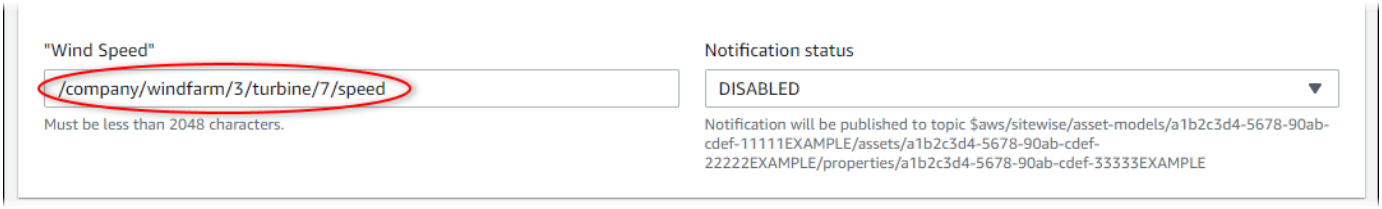
Você pode usar o AWS IoT SiteWise console para definir um alias para uma propriedade do ativo.

Como definir um apelido de propriedade (console)

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Ativos.
3. Escolha o ativo para o qual deseja definir um apelido de propriedade.

> **Tip**
>
> Você pode escolher o ícone de seta para expandir uma hierarquia de ativos para localizar seu ativo.

4. Selecione a opção Editar.
5. Localize a propriedade para a qual você deseja definir um apelido e insira o apelido da propriedade.



6. Selecione Save (Salvar).

Definindo um alias de propriedade ()AWS CLI

Use o AWS Command Line Interface (AWS CLI) para definir um alias para uma propriedade do ativo.

Para executar este procedimento, é necessário saber quais são o `assetId` do ativo e o `propertyId` da propriedade. Você também pode usar o ID externo. Se você criou um ativo e não o conhece`assetId`, use a ListAssetsAPI para listar todos os ativos de um modelo específico. Use a DescribeAssetoperação para visualizar as propriedades do seu ativo, incluindo IDs de propriedade.

Use a operação UpdateAssetPropriedade para mapear um fluxo de dados para a propriedade do seu ativo. Especifique os seguintes parâmetros:

- `assetId`— O ID do ativo ou o ID externo. Para obter mais informações, consulte Referenciando objetos com IDs externos no Guia de Usuário AWS IoT SiteWise .
- `propertyId`— O ID da propriedade do ativo ou o ID externo.
- `propertyAlias` – O caminho do fluxo de dados para o apelido para a propriedade.
- `propertyNotificationState` – O estado de notificação do valor da propriedade: `ENABLED` ou `DISABLED`. Especifique o estado de notificação existente da propriedade ao atualizar o apelido da propriedade. Você pode recuperar o estado de notificação existente com a operação DescribeAssetPropriedade.

  Se você omitir esse parâmetro, o novo estado de notificação será `DISABLED`. Para obter mais informações sobre notificações de propriedade, consulte Interagindo com outros serviços AWS.

Para definir um alias de propriedade ()AWS CLI

1. Execute o seguinte comando para recuperar o estado da notificação atual da propriedade. Substitua *asset-id* e *property-id* pelas IDs da propriedade do ativo.

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

A operação retorna uma resposta que contém os detalhes da propriedade do ativo no formato a seguir. O estado da notificação da propriedade está em `assetProperty.notification.state` no 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. Execute o seguinte comando para definir o apelido da propriedade do ativo: Substitua *property-apelido* pelo apelido da propriedade e *notification-state* pelo estado da notificação ou omita `--property-notification-state` para desabilitar as notificações. Opcionalmente, você pode atualizar a unidade do ativo com uma nova *unidade* e. `--property-unit`

```
aws iotsitewise update-asset-property \
```

```
  --asset-id asset-id \
  --property-id property-id \
  --property-alias property-alias \
  --property-notification-state notification-state \
  --property-unit unit
```

3. Para verificar se o apelido foi definido, execute o comando a seguir para recuperar os detalhes da propriedade: Substitua *asset-id* e *property-id* pelas IDs da propriedade do ativo.

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

A operação retorna uma resposta que contém os detalhes da propriedade do ativo no formato a seguir. O apelido da propriedade é `assetProperty.alias` no objeto JSON e está definido como `myAlias` neste exemplo.

```
{
  "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": {}
    }
  }
}
```

Atualizar valores de atributo

Os ativos herdam os atributos de seu modelo de ativo, incluindo o valor padrão do atributo. Em alguns casos, é melhor deixar o atributo padrão do modelo de ativo, como uma propriedade do fabricante do ativo. Em outros casos, é melhor substituir o atributo herdado, como a latitude e a longitude de um ativo.

Updating an attribute value (console)

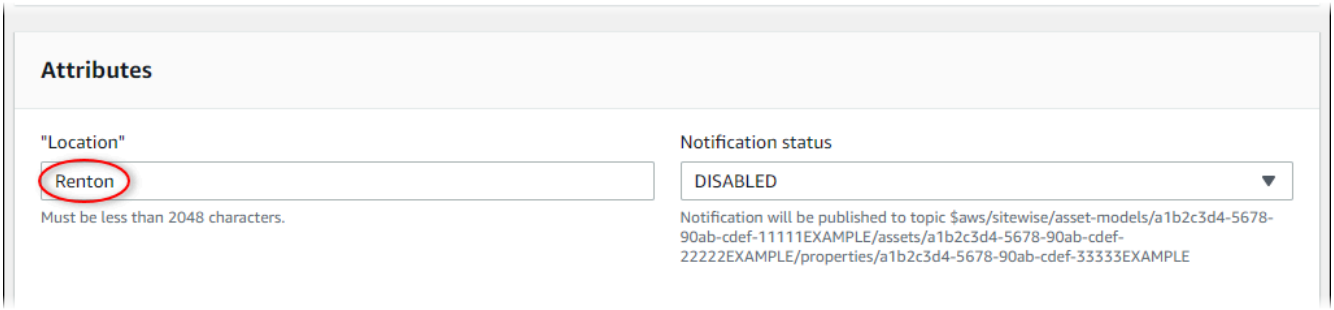
Você pode usar o AWS IoT SiteWise console para atualizar o valor de uma propriedade de ativo de atributo.

Como atualizar o valor de um atributo (console)

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Ativos.
3. Escolha o ativo para o qual deseja atualizar um atributo.

> **Tip**
>
> Você pode escolher o ícone de seta para expandir uma hierarquia de ativos para localizar seu ativo.

4. Selecione a opção Editar.
5. Localize o atributo a ser atualizado e insira seu novo valor.



6. Selecione Save (Salvar).

Updating an attribute value (AWS CLI)

Você pode usar o AWS Command Line Interface (AWS CLI) para atualizar um valor de atributo.

Para executar este procedimento, é necessário saber quais são o `assetId` do ativo e o `propertyId` da propriedade. Você também pode usar o ID externo. Se você criou um ativo e não o conhece`assetId`, use a ListAssetsAPI para listar todos os ativos de um modelo específico. Use a DescribeAssetoperação para visualizar as propriedades do seu ativo, incluindo IDs de propriedade.

Use a operação BatchPutAssetPropertyValue para atribuir valores de atributos ao seu ativo. É possível usar essa operação para definir vários atributos de uma vez. A carga útil dessa operação contém uma lista de entradas, e cada entrada contém a ID do ativo, a ID da propriedade e o valor do atributo.

Para atualizar o valor de um atributo (AWS CLI)

1. Crie um arquivo chamado `batch-put-payload.json` e copie o seguinte objeto JSON no arquivo. Este exemplo de carga útil demonstra como definir a latitude e a longitude de uma turbina eólica. Atualize as IDs, os valores e as funções de horas para modificar a carga útil do 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 na carga contém um `entryId` que você pode definir como qualquer string exclusiva. Se qualquer entrada de solicitação falhar, cada erro conterá o `entryId` da solicitação correspondente, para que você saiba quais solicitações tentar novamente.
- Para definir um valor de atributo, você pode incluir uma estrutura timestamp-quality-value (TQV) na lista de `propertyValues` para cada propriedade de atributo. Essa estrutura deve conter o novo `value` e o `timestamp` atual.
  - `value` – uma estrutura contendo um dos valores a seguir, a depender do tipo de propriedade sendo definida:
    - `booleanValue`
    - `doubleValue`
    - `integerValue`
    - `stringValue`
  - `timestamp`— Uma estrutura que contém o tempo atual da época do Unix em segundos,. `timeInSeconds` AWS IoT SiteWise rejeita todos os pontos de dados com carimbos de data/hora que existiam há mais de 7 dias ou menos de 5 minutos no futuro.

Para obter mais informações sobre como preparar uma carga para BatchPutAssetPropertyValue, consulteIngestão de dados usando a API AWS IoT SiteWise.

2. Execute o comando a seguir para enviar os valores dos atributos para AWS IoT SiteWise:

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

Associar e desassociar ativos

Se o modelo do ativo definir quaisquer hierarquias de modelo de ativo filho, você poderá associar ativos filho ao ativo. Os ativos pai podem acessar e agregar dados de ativos associados. Para obter mais informações sobre modelos de ativos de hierarquia, consulte Definindo hierarquias de modelos de ativos.

Tópicos

Associar e desassociar ativos (console)

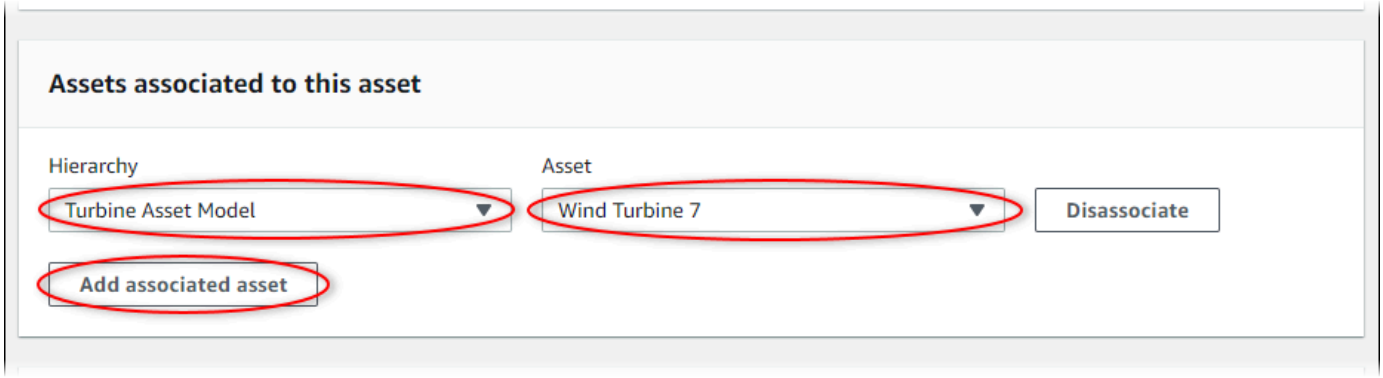
Você pode usar o AWS IoT SiteWise console para associar e desassociar ativos.

Como associar um ativo (console)

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Ativos.
3. Escolha o ativo pai ao qual deseja associar um ativo filho.

> **Tip**
>
> Você pode escolher o ícone de seta para expandir uma hierarquia de ativos para localizar seu ativo.

4. Selecione a opção Editar.
5. Em Ativos associados a este ativo, escolha Adicionar ativo associado.



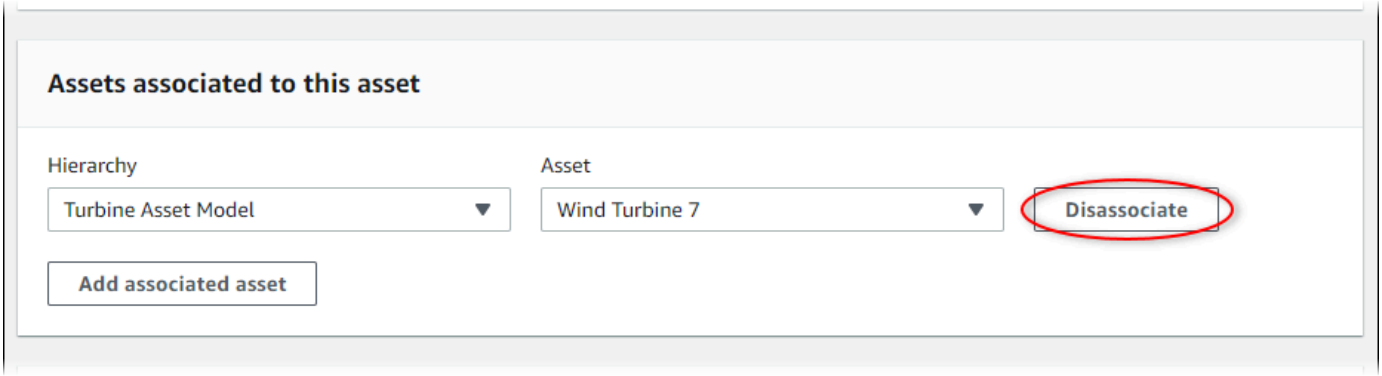
6. Em Hierarquia, escolha a hierarquia que define o relacionamento entre o ativo pai e o ativo filho.
7. Em Ativo, escolha o ativo filho a ser associado.
8. Selecione Save (Salvar).

Como desassociar um ativo (console)

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Ativos.
3. Escolha o ativo pai do qual deseja desassociar um ativo filho.

> **Tip**
>
> Você pode escolher o ícone de seta para expandir uma hierarquia de ativos para localizar seu ativo.

4. Selecione a opção Editar.
5. Em Ativos associados a este ativo, escolha Desassociar para o ativo.



6. Selecione Save (Salvar).

Associando e desassociando ativos ()AWS CLI

Você pode usar o AWS Command Line Interface (AWS CLI) para associar e desassociar ativos.

Para este procedimento, você deve saber a ID da hierarquia (`hierarchyId`) no modelo do ativo pai que define o relacionamento com o modelo do ativo filho. Use a DescribeAssetoperação para encontrar o ID da hierarquia na resposta.

Como localizar um ID de hierarquia

- Execute o seguinte comando para descrever o ativo pai. Substitua *parent-asset-id pela ID* do ativo principal ou pela ID externa.

  ```
  aws iotsitewise describe-asset --asset-id parent-asset-id
  ```

  A operação retorna uma resposta que contém os detalhes do ativo. A resposta contém uma `assetHierarchies` lista com a seguinte estrutura:

  ```
  {
    ...
    "assetHierarchies": [
      {
        "id": "String",
        "name": "String"
      }
    ],
    ...
  }
  ```

  a ID da hierarquia é o valor de `id` de uma hierarquia na lista de hierarquias de ativos.

Depois de obter a ID da hierarquia, associe ou desassocie um ativo com essa hierarquia.

Para associar um ativo secundário a um ativo principal, use a AssociateAssetsoperação. Para desassociar um ativo secundário de um ativo principal, use a DisassociateAssetsoperação. Especifique os seguintes parâmetros, que são os mesmos para as duas operações:

- `assetId`— O ID do ativo principal ou o ID externo.
- `hierarchyId`— O ID da hierarquia ou ID externo no ativo principal.
- `childAssetId`— O ID do ativo secundário ou o ID externo.

Para associar um ativo (AWS CLI)

- Execute o seguinte comando para associar um ativo filho a um ativo pai. *Substitua parent-asset-id, hierarchy-id e child-asset-id pelos respectivos IDs:*

  ```
  aws iotsitewise associate-assets \
  ```

```
  --asset-id parent-asset-id \
  --hierarchy-id hierarchy-id \
  --child-asset-id child-asset-id
```

Para desassociar um ativo ()AWS CLI

- Execute o seguinte comando para desassociar um ativo filho de um ativo pai. *Substitua parent-asset-id, hierarchy-id e child-asset-id pelos respectivos IDs:*

```
aws iotsitewise disassociate-assets \
  --asset-id parent-asset-id \
  --hierarchy-id hierarchy-id \
  --child-asset-id child-asset-id
```

Atualizar ativos e modelos

Você pode atualizar seus ativos, modelos de ativos e modelos de componentes AWS IoT SiteWise para modificar seus nomes e definições. Essas operações de atualização são assíncronas e demoram para serem propagadas. AWS IoT SiteWise Verifique o status do ativo ou modelo antes de fazer alterações adicionais. Você deve aguardar até que as alterações sejam propagadas para poder continuar a usar o ativo ou o modelo atualizado.

Tópicos

- Atualizar ativos
- Atualização de modelos de ativos e modelos de componentes
- Atualização de modelos compostos personalizados (componentes)

Atualizar ativos

Você pode usar o AWS IoT SiteWise console ou a API para atualizar o nome de um ativo.

Ao atualizar um ativo, o status do ativo será `UPDATING` até que as alterações sejam propagadas. Para ter mais informações, consulte Estados de ativos e modelos.

Tópicos

- Atualizar um ativo (console)

- Atualizando um ativo (AWS CLI)

Atualizar um ativo (console)

Você pode usar o AWS IoT SiteWise console para atualizar os detalhes do ativo.

Como atualizar um ativo (console)

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Ativos.
3. Escolha o ativo a ser atualizado.

   > **Tip**
   >
   > Você pode escolher o ícone de seta para expandir uma hierarquia de ativos para localizar seu ativo.

4. Selecione a opção Editar.
5. Atualize o Nomedo ativo.
6. (Opcional) Nessa página, atualize outras informações para o ativo. Para obter mais informações, consulte:

   - Mapeamento de fluxos de dados industriais para propriedades de ativos
   - Atualizar valores de atributo
   - Interagindo com outros serviços AWS
7. Selecione Save (Salvar).

Atualizando um ativo (AWS CLI)

Você pode usar o AWS Command Line Interface (AWS CLI) para atualizar o nome de um ativo.

Use a UpdateAssetoperação para atualizar um ativo. Especifique os seguintes parâmetros:

- `assetId` – O ID do ativo. Esse é o ID real no formato UUID, ou `externalId:myExternalId` se ele tiver um. Para obter mais informações, consulte Referenciando objetos com IDs externos no Guia de Usuário AWS IoT SiteWise .
- `assetName` – o novo nome do ativo.

Para atualizar o nome de um ativo (AWS CLI)

- Execute o seguinte comando para atualizar o nome de um ativo. Substitua *asset-id* pelo ID ou ID externo do ativo. Atualize o *nome do ativo* com o novo nome do ativo.

```
aws iotsitewise update-asset \
  --asset-id asset-id \
  --asset-name asset-name
```

Atualização de modelos de ativos e modelos de componentes

Você pode usar o AWS IoT SiteWise console ou a API para atualizar um modelo de ativo ou modelo de componente.

Você não pode alterar o tipo ou o tipo de dados de uma propriedade existente ou a janela de uma métrica existente. Você também não pode alterar o tipo do modelo de modelo de ativo para modelo de componente ou vice-versa.

> **Important**
>
> - Se você remover uma propriedade de um modelo de ativo ou modelo de componente, AWS IoT SiteWise excluirá todos os dados anteriores dessa propriedade. Para modelos de componentes, isso afeta todos os modelos de ativos que usam esse modelo de componente, portanto, tenha especial cuidado ao entender até que ponto sua alteração pode ser aplicada.
> - Se você remover uma definição de hierarquia de um modelo de ativo, AWS IoT SiteWise desassociará todos os ativos dessa hierarquia.

Quando você atualiza um modelo de ativo, cada ativo baseado nesse modelo reflete todas as alterações feitas no modelo subjacente. Até que as alterações se propaguem, cada ativo estará definido com o estado `UPDATING`. É necessário aguardar até que esses ativos retornem ao estado `ACTIVE` antes de interagir com eles. Durante esse período, o status do modelo de ativo atualizado será `PROPAGATING`.

Quando você atualiza um modelo de componente, cada modelo de ativo que incorpora esse modelo de componente reflete as mudanças. Até que as alterações do modelo de componentes se

propaguem, cada modelo de ativo afetado tem o `UPDATING` estado, seguido pela `PROPAGATING` atualização dos ativos associados, conforme descrito no parágrafo anterior. Você deve esperar até que esses modelos de ativos retornem ao `ACTIVE` estado antes de interagir com eles. Durante esse período, o status do modelo de componente atualizado será`PROPAGATING`.

Para ter mais informações, consulte Estados de ativos e modelos.

Tópicos

- Atualização de um modelo de ativo ou componente (console)
- Atualizando um modelo de ativo ou componente (AWS CLI)

Atualização de um modelo de ativo ou componente (console)

Você pode usar o AWS IoT SiteWise console para atualizar um modelo de ativo ou modelo de componente.

Para atualizar um modelo de ativo ou modelo de componente (console)

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Modelos.
3. Escolha o modelo do ativo ou o modelo do componente a ser atualizado.
4. Selecione a opção Editar.
5. Na página Editar modelo siga um destes procedimentos:
    - Em Detalhes do modelo, altere o Nome do modelo.
    - Altere qualquer uma das Definições de atributos. Não é possível alterar o Tipo de dados dos atributos existentes. Para ter mais informações, consulte Definindo dados estáticos (atributos).
    - Altere qualquer uma das Definições de medição. Não é possível alterar o Tipo de dados das medições existentes. Para ter mais informações, consulte Definindo fluxos de dados do equipamento (medições).
    - Altere qualquer uma das Definições de transformação. Para ter mais informações, consulte Transformando dados (transformações).
    - Altere qualquer uma das Definições de métrica. Não é possível alterar o Intervalo de tempo das métricas existentes. Para ter mais informações, consulte Agregando dados de propriedades e outros ativos (métricas).

- (Somente modelos de ativos) Altere qualquer uma das definições de hierarquia. Não é possível alterar o Modelo de hierarquia das hierarquias existentes. Para ter mais informações, consulte Definindo hierarquias de modelos de ativos.

6. Escolha Salvar.

Atualizando um modelo de ativo ou componente (AWS CLI)

Você pode usar o AWS Command Line Interface (AWS CLI) para atualizar um modelo de ativo ou modelo de componente.

Use a API de UpdateAssetmodelo para atualizar o nome, a descrição e as propriedades de um modelo de ativo ou modelo de componente. Somente para modelos de ativos, você pode atualizar hierarquias. Especifique os seguintes parâmetros:

- `assetModelId` – O ID do ativo. Esse é o ID real no formato UUID, ou `externalId:myExternalId` se ele tiver um. Para obter mais informações, consulte Referenciando objetos com IDs externos no Guia de Usuário AWS IoT SiteWise .

Especifique o modelo atualizado na carga útil. Para saber mais sobre o formato esperado de um modelo de ativo ou modelo de componente, consulteCriar modelos de ativo.

> **Warning**
>
> A API de UpdateAssetmodelo substitui o modelo existente pelo modelo que você fornece na carga útil. Para evitar a exclusão das propriedades ou hierarquias do seu modelo, você deve incluir suas IDs e definições na carga útil do modelo atualizado. Para saber como consultar a estrutura existente do seu modelo, consulte a operação do DescribeAssetmodelo.

> **Note**
>
> O procedimento a seguir só pode atualizar modelos compostos do tipo`AWS/ALARM`. Se você quiser atualizar modelos `CUSTOM` compostos, use UpdateAssetModelCompositeModel em vez disso. Para ter mais informações, consulte Atualização de modelos compostos personalizados (componentes).

Para atualizar um modelo de ativo ou modelo de componente (AWS CLI)

1. Execute o comando a seguir para recuperar a definição do modelo existente. Substitua *asset-model-id pela ID* ou pela ID externa do modelo de ativo ou modelo de componente a ser atualizado.

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

   A operação retorna uma resposta que contém os detalhes do modelo. A resposta tem a seguinte estrutura:

   ```
   {
     "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 obter mais informações, consulte a operação do DescribeAssetmodelo.

2. Crie um arquivo chamado `update-asset-model.json` e copie a resposta do comando anterior no arquivo.

3. Remova os seguintes pares de chave-valor do objeto JSON em `update-asset-model.json`:

   - `assetModelId`
   - `assetModelArn`

- `assetModelCompositeModelSummaries`
- `assetModelCreationDate`
- `assetModelLastUpdateDate`
- `assetModelStatus`
- `assetModelType`

A operação do UpdateAssetmodelo espera uma carga útil com a seguinte estrutura:

```
{
  "assetModelName": "String",
  "assetModelDescription": "String",
  "assetModelProperties": Array of AssetModelProperty,
  "assetModelHierarchies": Array of AssetModelHierarchyDefinition,
  "assetModelCompositeModels": Array of AssetModelCompositeModel
}
```

4. Em `update-asset-model.json` proceda de uma das seguintes maneiras:
   - Altere o nome do modelo de ativo (`assetModelName`).
   - Altere, adicione ou remova a descrição do modelo de ativo (`assetModelDescription`).
   - Altere, adicione ou remova qualquer uma das propriedades do modelo de ativo (`assetModelProperties`). Não é possível alterar o `dataType` de propriedades existentes ou a `window` das métricas existentes. Para ter mais informações, consulte Definir propriedades de dados.
   - Altere, adicione ou remova qualquer uma das hierarquias de modelos de ativo (`assetModelHierarchies`). Não é possível alterar o `childAssetModelId` das hierarquias existentes. Para ter mais informações, consulte Definindo hierarquias de modelos de ativos.
   - Altere, adicione ou remova qualquer um dos modelos compostos do modelo de ativo do tipo `AWS/ALARM` (`assetModelCompositeModels`). Os alarmes monitoram outras propriedades para que você possa identificar quando equipamentos ou processos requerem atenção. Cada definição de alarme é um modelo composto que padroniza o conjunto de propriedades que o alarme usa. Para obter mais informações, consulte Monitorar dados com alarmes e Definir alarmes em modelos de ativos.
5. Execute o seguinte comando para atualizar o modelo de ativo com a definição armazenada no `update-asset-model.json`. Substitua *`asset-model-id pelo ID`* do modelo de ativo:

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

Atualização de modelos compostos personalizados (componentes)

Você pode usar a AWS IoT SiteWise API para atualizar um modelo composto personalizado ou o AWS IoT SiteWise console para atualizar componentes.

Tópicos

- Atualizando um componente (console)
- Atualizando um modelo composto personalizado ()AWS CLI

Atualizando um componente (console)

Você pode usar o AWS IoT SiteWise console para atualizar um componente.

Para atualizar um componente (console)

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Modelos.
3. Escolha o modelo de ativo em que o componente está.
4. Na guia Propriedades, escolha Componentes.
5. Escolha o componente que você deseja atualizar.
6. Selecione a opção Editar.
7. Na página Editar componente, faça o seguinte:
   - Em Detalhes do modelo, altere o Nome do modelo.
   - Altere qualquer uma das Definições de atributos. Não é possível alterar o Tipo de dados dos atributos existentes. Para ter mais informações, consulte Definindo dados estáticos (atributos).
   - Altere qualquer uma das Definições de medição. Não é possível alterar o Tipo de dados das medições existentes. Para ter mais informações, consulte Definindo fluxos de dados do equipamento (medições).

- Altere qualquer uma das Definições de transformação. Para ter mais informações, consulte Transformando dados (transformações).
- Altere qualquer uma das Definições de métrica. Não é possível alterar o Intervalo de tempo das métricas existentes. Para ter mais informações, consulte Agregando dados de propriedades e outros ativos (métricas).

8. Escolha Salvar.

Atualizando um modelo composto personalizado ()AWS CLI

Você pode usar o AWS Command Line Interface (AWS CLI) para atualizar um modelo composto personalizado.

Para atualizar o nome ou a descrição, use a operação UpdateAssetModelCompositeModelo. Somente para modelos compostos personalizados em linha, você também pode atualizar as propriedades. Você não pode atualizar as propriedades de um modelo composto component-model-based personalizado, porque o modelo de componente referenciado fornece as propriedades associadas.

> **Important**
>
> Se você remover uma propriedade de um modelo composto personalizado, AWS IoT SiteWise excluirá todos os dados anteriores dessa propriedade. Você não pode alterar o tipo ou o tipo de dados de uma propriedade existente.
> Para substituir uma propriedade de modelo composto existente por uma nova com a mesma`name`, faça o seguinte:
>
> 1. Envie uma `UpdateAssetModelCompositeModel` solicitação com toda a propriedade existente removida.
> 2. Envie uma segunda `UpdateAssetModelCompositeModel` solicitação que inclua a nova propriedade. A nova propriedade do ativo terá a `name` mesma que a anterior e AWS IoT SiteWise gerará uma nova propriedade exclusiva`id`.

Para atualizar um modelo composto personalizado ()AWS CLI

1. Para recuperar a definição do modelo composto existente, execute o comando a seguir. Substitua *`composite-model-id`* pelo ID ou ID externo do modelo composto personalizado

a ser atualizado e *asset-model-id* pelo modelo de ativo ao qual o modelo composto personalizado está associado. Para obter mais informações, consulte AWS IoT SiteWise no Manual do Usuário do .

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

Para obter mais informações, consulte a operação do DescribeAssetModelCompositemodelo.

2. Crie um arquivo chamado e`update-custom-composite-model.json`, em seguida, copie a resposta do comando anterior para o arquivo.
3. Remova todos os pares de valores-chave do objeto JSON, `update-custom-composite-model.json` exceto nos seguintes campos:

   - `assetModelCompositeModelName`
   - `assetModelCompositeModelDescription`(se presente)
   - `assetModelCompositeModelProperties`(se presente)
4. Em `update-custom-composite-model.json` proceda de uma das seguintes maneiras:

   - Altere o valor de`assetModelCompositeModelName`.
   - Adicione`assetModelCompositeModelDescription`, remova ou altere seu valor.
   - Somente para modelos compostos personalizados em linha: altere, adicione ou remova qualquer uma das propriedades do modelo de ativo em. `assetModelCompositeModelProperties`

   Para obter mais informações sobre o formato necessário para esse arquivo, consulte a sintaxe da solicitação para UpdateAssetModelCompositeModel.
5. Execute o comando a seguir para atualizar o modelo composto personalizado com a definição armazenada em`update-custom-composite-model.json`. Substitua *composite-model-id* pelo ID do modelo composto e *asset-model-id pelo ID* do modelo de ativo em que ele está.

```
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
```

Excluir ativos e modelos

Você pode excluir seus ativos e modelos AWS IoT SiteWise quando terminar de usá-los. As operações de exclusão são assíncronas e demoram para se propagar. AWS IoT SiteWise

Tópicos

Excluir ativos

Você pode usar o AWS IoT SiteWise console ou a API para excluir um ativo.

Para excluir um ativo, primeiro você deve desassociar seus ativos filho e desassociá-lo do ativo pai. Para ter mais informações, consulte Associar e desassociar ativos. Se você usar o AWS Command Line Interface (AWS CLI), poderá usar a operação ListAssociatedAssets para listar os filhos de um ativo.

Ao excluir um ativo, seu status será `DELETING` até que as alterações sejam propagadas. Para ter mais informações, consulte Estados de ativos e modelos. Depois que o ativo for excluído, não será possível consultá-lo. Se você fizer isso, a API retornará uma resposta HTTP 404.

> **Important**
>
> AWS IoT SiteWise exclui todos os dados de propriedade dos ativos excluídos.

Tópicos

Excluir um ativo (console)

Você pode usar o AWS IoT SiteWise console para excluir um ativo.

Para excluir um ativo (console)

1. Navegue até o console do AWS IoT SiteWise.

2. No painel de navegação, selecione Ativos.
3. Escolha o ativo a ser excluído.

> **Tip**
>
> Você pode escolher o ícone de seta para expandir uma hierarquia de ativos para localizar seu ativo.

4. Se o ativo tiver Ativos associados, exclua cada ativo. Você pode escolher o nome de um ativo para navegar até sua página e poder excluí-lo.
5. Na página do ativo, escolha Excluir.
6. Na caixa de diálogo Excluir ativo, faça o seguinte:
   a. Insira **`Delete`** para confirmar a exclusão.
   b. Escolha Excluir.

Excluindo um ativo ()AWS CLI

Você pode usar o AWS Command Line Interface (AWS CLI) para excluir um ativo.

Use a DeleteAssetoperação para excluir um ativo. Defina o seguinte parâmetro:

- `assetId` – O ID do ativo. Esse é o ID real no formato UUID, ou `externalId:myExternalId` se ele tiver um. Para obter mais informações, consulte Referenciando objetos com IDs externos no Guia de Usuário AWS IoT SiteWise .

Para excluir um ativo (AWS CLI)

1. Execute o seguinte comando para listar as hierarquias do ativo. Substitua *`asset-id`* pelo ID ou pelo ID externo do ativo:

```
aws iotsitewise describe-asset --asset-id asset-id
```

   A operação retorna uma resposta que contém os detalhes do ativo. A resposta contém uma `assetHierarchies` lista com a seguinte estrutura:

```
{
```

```
  ...
  "assetHierarchies": [
    {
      "id": "String",
      "name": "String"
    }
  ],
  ...
}
```

Para obter mais informações, consulte a DescribeAssetoperação.

2. Para cada hierarquia, execute o seguinte comando para listar os filhos do ativo que estão associados a essa hierarquia. Substitua *asset-id* pelo ID ou ID externo do ativo e *hierarchy-id pelo ID ou ID* externo da hierarquia.

```
aws iotsitewise list-associated-assets \
  --asset-id asset-id \
  --hierarchy-id hierarchy-id
```

Para obter mais informações, consulte a operação ListAssociatedAssets.

3. Execute o seguinte comando para excluir cada ativo associado e excluir o ativo. Substitua *asset-id* pelo ID ou ID externo do ativo.

```
aws iotsitewise delete-asset --asset-id asset-id
```

Excluir modelos de ativo

Você pode usar o AWS IoT SiteWise console ou a API para excluir um modelo de ativo.

Antes de excluir um modelo de ativo, você deve primeiro excluir todos os ativos que foram criados a partir do modelo de ativo.

Ao excluir um modelo de ativo, seu status será `DELETING` até que as alterações sejam propagadas. Para ter mais informações, consulte Estados de ativos e modelos. Depois que o modelo de ativo for excluído, não será possível consultá-lo. Se você fizer isso, a API retornará uma resposta HTTP 404.

Tópicos

- Excluir um modelo de ativo (console)

- Excluindo um modelo de ativo ()AWS CLI

Excluir um modelo de ativo (console)

Você pode usar o AWS IoT SiteWise console para excluir um modelo de ativo.

Como excluir um modelo de ativo (console)

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Modelos.
3. Escolha o modelo de ativo a ser excluído.
4. Se o modelo tiver Ativos, exclua cada ativo. Escolha o nome de um ativo para navegar até sua página e poder excluí-lo. Para ter mais informações, consulte Excluir um ativo (console).
5. Na página do modelo, escolha Excluir.
6. Na caixa de diálogo Excluir modelo, faça o seguinte:

   a. Insira **`Delete`** para confirmar a exclusão.

   b. Escolha Excluir.

Excluindo um modelo de ativo ()AWS CLI

Você pode usar o AWS Command Line Interface (AWS CLI) para excluir um modelo de ativo.

Use a operação DeleteAssetModelo para excluir um modelo de ativo. Defina o seguinte parâmetro:

- `assetModelId` – O ID do ativo. Esse é o ID real no formato UUID, ou `externalId:myExternalId` se ele tiver um. Para obter mais informações, consulte Referenciando objetos com IDs externos no Guia de Usuário AWS IoT SiteWise .

Para excluir um modelo de ativo (AWS CLI)

1. Execute o seguinte comando para listar todos os ativos criados usando o modelo. Substitua *`asset-model-id pelo ID`* ou pelo ID externo do modelo de ativo.

   ```
   aws iotsitewise list-assets --asset-model-id asset-model-id
   ```

   Para obter mais informações, consulte a ListAssetsoperação.

2. Se o comando anterior retornar quaisquer ativos do modelo, exclua cada ativo. Para ter mais informações, consulte Excluindo um ativo ()AWS CLI.
3. Execute o comando a seguir para excluir o modelo de ativo. Substitua *asset-model-id pelo ID* ou ID externo do modelo de ativo.

```
aws iotsitewise delete-asset-model --asset-model-id asset-model-id
```

Operações em massa com ativos e modelos

Para trabalhar com um grande número de ativos ou modelos de ativos, use operações em massa para importar e exportar recursos em massa para um local diferente. Por exemplo, você pode criar um arquivo de dados que define ativos ou modelos de ativos em um bucket do Amazon S3 e usar a importação em massa para criá-los ou atualizá-los. AWS IoT SiteWise Como alternativa, se você tiver um grande número de ativos ou modelos de ativos AWS IoT SiteWise, poderá exportá-los para o Amazon S3.

> **Note**
>
> Você realiza operações em massa AWS IoT SiteWise chamando operações na AWS IoT TwinMaker API. Você pode fazer isso sem configurar AWS IoT TwinMaker ou criar um AWS IoT TwinMaker espaço de trabalho. Tudo o que você precisa é de um bucket Amazon S3 onde você possa colocar seu AWS IoT SiteWise conteúdo.

Tópicos

Principais conceitos e terminologia

AWS IoT SiteWise Os recursos de importação e exportação em massa se baseiam nos seguintes conceitos e terminologia:

- Importação: a ação de mover ativos ou modelos de ativos de um arquivo em um bucket do Amazon S3 para o. AWS IoT SiteWise
- Exportação: a ação de mover ativos ou modelos de ativos AWS IoT SiteWise para um bucket do Amazon S3.
- Fonte: o local inicial de onde você deseja mover o conteúdo.

  Por exemplo, um bucket do Amazon S3 é uma fonte de importação e AWS IoT SiteWise uma fonte de exportação.
- Destino: o local desejado para onde você deseja mover seu conteúdo.

  Por exemplo, um bucket do Amazon S3 é um destino de exportação e AWS IoT SiteWise um destino de importação.
- AWS IoT SiteWise Esquema: Esse esquema é usado para importar e exportar metadados do. AWS IoT SiteWise
- Recurso de nível superior: um AWS IoT SiteWise recurso que você pode criar ou atualizar individualmente, como um ativo ou modelo de ativo.
- Sub-recurso: um recurso aninhado em um AWS IoT SiteWise recurso de nível superior. Os exemplos incluem propriedades, hierarquias e modelos compostos.
- Metadados: informações importantes necessárias para importar ou exportar recursos com sucesso. Exemplos de metadados são definições de ativos e modelos de ativos.
- metadados TransferJob: o objeto criado quando você `CreateMetadataTransferJob` executa.

Funções compatíveis

Este tópico explica o que você pode fazer ao executar uma operação em massa. As operações em massa oferecem suporte às seguintes funcionalidades:

- Criação de recursos de nível superior: quando você importa um ativo ou modelo de ativo que não define um ID ou cujo ID não corresponde ao de um existente, ele será criado como um novo recurso.

- Substituição de recursos de nível superior: quando você importa um ativo ou modelo de ativo cuja ID corresponde a uma que já existe, ele substitui o recurso existente.
- Criação, substituição ou exclusão de sub-recursos: quando sua importação substitui um recurso de nível superior, como um ativo ou modelo de ativo, a nova definição substitui todos os sub-recursos, como propriedades, hierarquias ou modelos compostos.

  Por exemplo, se você atualizar um modelo de ativo durante uma importação em massa e a versão atualizada definir uma propriedade que não estava presente no original, uma nova propriedade será criada. Se definir uma propriedade que já existe, a propriedade existente será atualizada. Se o modelo de ativo atualizado omitir uma propriedade que estava presente no original, a propriedade será excluída.
- Sem exclusão de recursos de nível superior: operações em massa não excluem um ativo ou modelo de ativo. As operações em massa apenas as criam ou atualizam.

Pré-requisitos de operação em massa

Esta seção explica os pré-requisitos de operação em massa, incluindo permissões AWS Identity and Access Management (IAM) para troca de recursos entre Serviços da AWS e sua máquina local. Antes de iniciar uma operação em massa, preencha os seguintes pré-requisitos:

- Crie um bucket do Amazon S3 para armazenar recursos. Para obter mais informações sobre o uso do Amazon S3, consulte O que é o Amazon S3?

Permissões do IAM

Para realizar operações em massa, você deve criar uma política AWS Identity and Access Management (IAM) com permissões que permitam a troca de AWS recursos entre o Amazon S3 e sua máquina local. AWS IoT SiteWise Para obter mais informações sobre como criar políticas do IAM, consulte Criar políticas do IAM.

Para realizar operações em massa, você precisa das seguintes políticas.

AWS IoT SiteWise política

Essa política permite o acesso às ações de AWS IoT SiteWise API necessárias para operações em massa:

```
{
```

```
    "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

Essa política permite acesso às operações de AWS IoT TwinMaker API que você usa para trabalhar com operações em massa:

```
{
    "Sid": "MetadataTransferJobApiAccess",
```

```
    "Effect": "Allow",
    "Action": [
        "iottwinmaker:CreateMetadataTransferJob",
        "iottwinmaker:CancelMetadataTransferJob",
        "iottwinmaker:GetMetadataTransferJob",
        "iottwinmaker:ListMetadataTransferJobs"
    ],
    "Resource": "*"
}
```

Política do Amazon S3

Essa política fornece acesso aos buckets do Amazon S3 para transferir metadados para operações em massa.

For a specific Amazon S3 bucket

Se você usar um bucket específico para trabalhar com seus metadados de operações em massa, essa política fornecerá acesso a esse bucket:

```
{
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:AbortMultipartUpload",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
    ],
    "Resource": [
        "arn:aws:s3:::bucket name",
        "arn:aws:s3:::bucket name/*"
    ]
}
```

To allow any Amazon S3 bucket

Se você usar vários buckets diferentes para trabalhar com seus metadados de operações em massa, essa política fornecerá acesso a qualquer bucket:

```
{
```

```
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:AbortMultipartUpload",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
    ],
    "Resource": "*"
}
```

Para obter informações sobre como solucionar problemas nas operações de importação e exportação, consulteSolução de problemas de importação e exportação em massa.

Executando um trabalho de importação em massa

A importação em massa é a ação de mover metadados para um espaço AWS IoT SiteWise de trabalho. Por exemplo, a importação em massa pode mover metadados de um arquivo local ou de um arquivo em um bucket do Amazon S3 para AWS IoT SiteWise um espaço de trabalho.

Etapa 1: Preparar o arquivo a ser importado

Baixe o arquivo de formato AWS IoT SiteWise nativo para importar ativos e modelos de ativos. Consulte AWS IoT SiteWise esquema de trabalho de transferência de metadados para obter mais detalhes.

Etapa 2: Faça o upload do arquivo preparado para o Amazon S3

Faça o upload do arquivo para o Amazon S3. Consulte Fazer upload de um arquivo para o Amazon S3 no Guia do usuário do Amazon Simple Storage Service para obter detalhes.

Importar metadados (console)

Você pode usar o Console do AWS IoT SiteWise para importar metadados em massa. Siga Etapa 1: Preparar o arquivo a ser importado e Etapa 2: Faça o upload do arquivo preparado para o Amazon S3 prepare um arquivo que esteja pronto para ser importado.

Importar dados do Amazon S3 para Console do AWS IoT SiteWise

1. Navegue até o console do AWS IoT SiteWise.
2. Escolha Operações em massa Novas no painel de navegação.
3. Escolha Nova importação para iniciar o processo de importação.
4. Na página Importar metadados:
   - Escolha Navegar no Amazon S3 para visualizar o bucket e os arquivos do Amazon S3.
   - Navegue até o bucket do Amazon S3 que contém o arquivo de importação preparado.
   - Selecione o arquivo a ser importado.
   - Revise o arquivo selecionado e escolha Importar.
5. A página Operações em massa em SiteWise metadados do Console do AWS IoT SiteWise exibe o trabalho de importação recém-criado na tabela de progresso dos trabalhos.

Importar metadados ()AWS CLI

Para realizar uma ação de importação, use o procedimento a seguir:

Importar dados do Amazon S3 para AWS CLI

1. Crie um arquivo de metadados que especifique os recursos que você deseja importar, seguindo o. AWS IoT SiteWise esquema de trabalho de transferência de metadados Armazene esse arquivo em seu bucket do Amazon S3.

   Para obter exemplos de arquivos de metadados a serem importados, consulteExemplos de importação de metadados.
2. Agora, crie um arquivo JSON com o corpo da solicitação. O corpo da solicitação especifica a origem e o destino da tarefa de transferência. Esse arquivo é separado do arquivo da etapa anterior. Certifique-se de especificar seu bucket do Amazon S3 como origem e `iotsitewise` destino.

   O exemplo a seguir mostra o corpo da solicitação:

```
{
      "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. Invoque o `CreateMetadataTransferJob` executando o AWS CLI comando a seguir. Neste exemplo, o arquivo do corpo da solicitação da etapa anterior é nomeado`createMetadataTransferJobExport.json`.

```
aws iottwinmaker create-metadata-transfer-job --region us-east-1 \
  --cli-input-json file://createMetadataTransferJobImport.json
```

Isso criará um trabalho de transferência de metadados e iniciará o processo de transferência dos recursos selecionados.

Executando um trabalho de exportação em massa

A exportação em massa é a ação de mover metadados de um AWS IoT SiteWise espaço de trabalho para um bucket do Amazon S3.

Ao realizar uma exportação em massa do seu AWS IoT SiteWise conteúdo para o Amazon S3, você pode especificar filtros para limitar quais modelos de ativos e ativos específicos você gostaria de exportar.

Os filtros devem ser especificados em uma `iotSiteWiseConfiguration` seção dentro da seção de fontes da sua solicitação JSON.

> **Note**
>
> Você pode incluir vários filtros em sua solicitação. A operação em massa exportará modelos de ativos e ativos que correspondam a qualquer um dos filtros.
> Se você não fornecer nenhum filtro, a operação em massa exportará todos os seus modelos e ativos de ativos.

Example corpo da solicitação com 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"
          }
      }
}
```

Exportar metadados (console)

O procedimento a seguir explica a ação de exportação do console:

Crie um trabalho de exportação no Console do AWS IoT SiteWise

1. Navegue até o console do AWS IoT SiteWise.
2. Escolha Operações em massa Novas no painel de navegação.
3. Escolha Nova exportação para iniciar o processo de exportação.
4. Na página Exportar metadados:
   - Insira um nome para o trabalho de exportação. Esse é o nome usado para o arquivo exportado em seu bucket do Amazon S3.
   - Escolha seus recursos para exportar, o que define os filtros para o trabalho:
     - Exporte todos os ativos e modelos de ativos. Use filtros em ativos e modelos de ativos.
     - Exportar ativos. Filtre seus ativos.
       - Selecione o ativo a ser usado para o filtro de exportação.
       - (Opcional) Adicione a descendência ou o modelo de ativo associado.
     - Exporte modelos de ativos. Filtre seus modelos de ativos.
       - Selecione o modelo de ativo a ser usado para o filtro de exportação.
       - (Opcional) Adicione a prole, o ativo associado ou ambos.
     - Selecione Next (Próximo).
   - Navegue até o bucket do Amazon S3:
     - Escolha Navegar no Amazon S3 para visualizar o bucket e os arquivos do Amazon S3.
     - Navegue até o bucket do Amazon S3 onde o arquivo deve ser colocado.
     - Selecione Next (Próximo).
   - Revise o trabalho de exportação e escolha Exportar.
5. A página Operações em massa em SiteWise metadados do Console do AWS IoT SiteWise exibe o trabalho de importação recém-criado na tabela de progresso dos trabalhos.

Para conhecer as diferentes formas de usar filtros ao exportar metadados, consulte. Exemplos de exportação de metadados

Exportar metadados ()AWS CLI

O procedimento a seguir explica a ação de AWS CLI exportação:

Exportar dados AWS IoT SiteWise para o Amazon S3

1. Crie um arquivo JSON com o corpo da solicitação. O corpo da solicitação especifica a origem e o destino da tarefa de transferência. O exemplo a seguir mostra um exemplo de corpo de solicitação:

```
{
    "metadataTransferJobId": "your-transfer-job-Id",
    "sources": [{
        "type": "iotsitewise"
    }],
    "destination": {
        "type": "s3",
        "s3Configuration": {
            "location": "arn:aws:s3:::your-S3-bucket-location"
        }
    }
}
```

   Certifique-se de especificar seu bucket do Amazon S3 como o destino do trabalho de transferência de metadados.

   > **Note**
   >
   > Este exemplo exportará todos os seus modelos e ativos de ativos. Para limitar a exportação a modelos de ativos ou ativos específicos, você pode incluir filtros no corpo da solicitação. Para obter mais informações sobre a aplicação de filtros de exportação, consulteExemplos de exportação de metadados.

2. Salve o arquivo do corpo da solicitação para usar na próxima etapa. Neste exemplo, o nome do arquivo é `createMetadataTransferJobExport.json`.
3. Invoque o `CreateMetadataTransferJob` executando o seguinte AWS CLI comando:

```
aws iottwinmaker create-metadata-transfer-job --region us-east-1 \
        --cli-input-json file://createMetadataTransferJobExport.json
```

Substitua o arquivo `createMetadataTransferJobExport.json` JSON de entrada pelo nome do seu próprio arquivo de transferência.

Rastreamento do progresso de trabalhos e tratamento de erros

Um trabalho de processamento em massa leva tempo para ser processado. Cada trabalho é processado na ordem de AWS IoT SiteWise recebimento da solicitação. Ele é processado one-at-a-time para cada conta. Quando um trabalho é concluído, o próximo na fila inicia automaticamente o processamento. AWS IoT SiteWise resolve os trabalhos de forma assíncrona e atualiza o status de cada um à medida que ele progride. Cada trabalho tem um campo de status que contém o estado do recurso e uma mensagem de erro, se aplicável.

O estado pode ser um dos seguintes valores:

- `VALIDATING`— Validar o trabalho, incluindo o formato do arquivo enviado e seu conteúdo.
- `PENDING`— O trabalho está em uma fila. Você pode cancelar trabalhos nesse estado no AWS IoT SiteWise console, mas todos os outros estados continuarão até o final.
- `RUNNING`— Processando o trabalho. Ele está criando e atualizando recursos conforme definido pelo arquivo de importação ou exportando recursos com base nos filtros de trabalho de exportação escolhidos. Se cancelado, nenhum recurso importado por esse trabalho não será excluído. Consulte Analise o progresso e os detalhes do trabalho (console) Para mais informações.
- `CANCELLING`— O trabalho está sendo cancelado ativamente.
- `ERROR`— Falha no processamento de um ou mais recursos. Consulte o relatório detalhado do trabalho para obter mais informações. Consulte Inspecione os detalhes do erro (console) Para mais informações.
- `COMPLETED`— Job concluído sem erros.
- `CANCELLED`— O trabalho foi cancelado e não está na fila. Se você cancelou um `RUNNING` trabalho, os recursos já importados por esse trabalho no momento do cancelamento não serão excluídos do AWS IoT SiteWise.

Tópicos

- Acompanhamento do progresso de trabalhos
- Inspecione erros

Acompanhamento do progresso de trabalhos

Analise o progresso e os detalhes do trabalho (console)

Veja Importar metadados (console) ou Exportar metadados (console) inicie um trabalho em massa.

Visão geral do progresso do trabalho no AWS IoT SiteWise console:

1. Navegue até o console do AWS IoT SiteWise.
2. Escolha Operações em massa Novas no painel de navegação.
3. A tabela de progresso de trabalhos no AWS IoT SiteWise console exibe a lista de trabalhos de operação em massa.
4. A coluna Tipo de trabalho descreve se é um trabalho de exportação ou importação. As colunas Data de importação exibem a data de início do trabalho.
5. A coluna Status exibe o status do trabalho. Você pode selecionar um trabalho para ver detalhes sobre o trabalho.
6. O trabalho selecionado mostra Sucesso ao ser bem-sucedido ou uma lista de falhas se o trabalho falhou. Uma descrição do erro também é exibida com cada tipo de recurso.

Visão geral dos detalhes do trabalho no AWS IoT SiteWise console:

A tabela de progresso de trabalhos no AWS IoT SiteWise console exibe a lista de trabalhos de operação em massa.

1. Escolha um emprego para ver mais detalhes.
2. Para um trabalho de importação, o `Data source ARN` representa a localização do arquivo de importação no Amazon S3.
3. Para um trabalho de exportação, o `Data destination ARN` representa a localização do arquivo no Amazon S3 após a exportação.
4. O `Status` e`Status reason`, forneça detalhes adicionais sobre o trabalho atual. Consulte Rastreamento do progresso de trabalhos e tratamento de erros para obter mais detalhes.
5. O `Queued position` representa a posição do trabalho na fila do processo. Os trabalhos são processados um por vez. Uma posição na fila de 1 indica que o trabalho será processado em seguida.
6. A página de detalhes dos trabalhos também exibe as contagens de progresso do trabalho.

- Os tipos de contagem do progresso do trabalho são:

  i. `Total resources`— Indica a contagem total de ativos no processo de transferência.

  ii. `Succeeded`— Indica a contagem de ativos transferidos com sucesso durante o processo.

  iii. `Failed`— Indica a contagem de ativos que falharam durante o processo.

  iv. `Skipped`— Indica a contagem de ativos que foram ignorados durante o processo.

7. O status do trabalho de `PENDING` ou `VALIDATING` exibe todas as contas do progresso das tarefas–. Isso indica que as contagens de progresso dos trabalhos estão sendo avaliadas.
8. O status do trabalho de `RUNNING` exibe a `Total resources` contagem, o trabalho enviado para processamento. As contagens detalhadas (`Succeeded`Failed,, e`Skipped`) se aplicam aos recursos processados. A soma das contagens detalhadas é menor que a `Total resources` contagem, até que o status do trabalho seja `COMPLETED` ou`ERROR`.
9. Se o status de um trabalho for `COMPLETED` ou`ERROR`, a `Total resources` contagem será igual à soma das contagens detalhadas (`Succeeded`,`Failed`, e`Skipped`).
10. Se o status de um trabalho for`ERROR`, verifique a tabela Job Failures para obter detalhes sobre os erros e falhas específicos. Consulte Inspecione os detalhes do erro (console) para obter mais detalhes.

Analise o progresso e os detalhes do trabalho (AWS CLI)

Depois de iniciar uma operação em massa, você pode verificar ou atualizar seu status usando as seguintes ações de API:

- Para recuperar informações sobre um trabalho específico, use a ação da GetMetadataTransferJobAPI.

  Recupere informações com a **`GetMetadataTransferJob`** API:

  1. Crie e execute um trabalho de transferência. Chame a API `GetMetadataTransferJob`.

     Example AWS CLI comando:

```
aws iottwinmaker get-metadata-transfer-job \
        --metadata-transfer-job-id your_metadata_transfer_job_id \
```

```
        --region your_region
```

2. A `GetMetadataTransferJob` API retorna um `MetadataTransferJobProgress` objeto com os seguintes parâmetros:
   - SucceededCount — Indica a contagem de ativos transferidos com sucesso no processo.
   - FailedCount — Indica a contagem de ativos que falharam durante o processo.
   - skippedCount — Indica a contagem de ativos que foram ignorados durante o processo.
   - TotalCount — Indica a contagem total de ativos no processo de transferência.

   Esses parâmetros indicam o status do progresso do trabalho. Se o status for`RUNNING`, eles ajudarão a rastrear o número de recursos ainda a serem processados.

   Se você encontrar erros de validação do esquema ou se failedCount for maior ou igual a 1, o estado de progresso do trabalho será alterado para. `ERROR` Um relatório completo de erros do trabalho é colocado em seu bucket do Amazon S3. Consulte Inspecione erros para obter mais detalhes.

- Para listar os trabalhos atuais, use a ação ListMetadataTransferJobsda API.

  Use um arquivo JSON para filtrar os trabalhos retornados com base em seu estado atual. Veja o procedimento a seguir:

  1. Para especificar os filtros que você deseja usar, crie um arquivo JSON AWS CLI de entrada. quero usar:

     ```
     {
         "sourceType": "s3",
         "destinationType": "iottwinmaker",
         "filters": [{
             "state": "COMPLETED"
         }]
     }
     ```

     Para ver uma lista de `state` valores válidos, consulte ListMetadataTransferJobsFiltro no Guia de referência AWS IoT TwinMaker da API.

  2. Use o arquivo JSON como argumento no seguinte AWS CLI exemplo de comando:

     ```
     aws iottwinmaker list-metadata-transfer-job --region your_region \
     ```

```
        --cli-input-json file://ListMetadataTransferJobsExample.json
```

- Para cancelar um trabalho, use a ação CancelMetadataTransferJobda API. Essa API cancela a tarefa específica de transferência de metadados, sem afetar nenhum recurso já exportado ou importado:

```
aws iottwinmaker cancel-metadata-transfer-job \
        --region your_region \
        --metadata-transfer-job-id job-to-cancel-id
```

Inspecione erros

Inspecione os detalhes do erro (console)

Detalhes do erro no AWS IoT SiteWise console:

1. Navegue até o console do AWS IoT SiteWise.
2. Consulte a tabela de progresso de trabalhos em Console do AWS IoT SiteWise para obter uma lista de trabalhos de operação em massa.
3. Selecione um trabalho para ver os detalhes do trabalho.
4. Se o status de um trabalho for `COMPLETED` ou`ERROR`, a `Total resources` contagem será igual à soma das contagens detalhadas (`Succeeded`,`Failed`, e`Skipped`).
5. Se o status de um trabalho for`ERROR`, verifique a tabela Job Failures para obter detalhes sobre os erros e falhas específicos.
6. A tabela Job Failures exibe o conteúdo do relatório do trabalho. O `Resource type` campo indica a localização do erro ou das falhas, como as seguintes:

   - Por exemplo, um erro de validação no `Resource type` campo indica que o modelo de importação e o formato do arquivo do esquema de metadados não coincidem. `Bulk operations template` Consulte AWS IoT SiteWise esquema de trabalho de transferência de metadados Para mais informações.
   - Uma falha `Asset` no `Resource type` campo indica que o ativo não foi criado devido a um conflito com outro ativo. Consulte Erros comuns para obter informações sobre erros e conflitos de AWS IoT SiteWise recursos.

Inspecione os detalhes do erro ()AWS CLI

Para tratar e diagnosticar erros produzidos durante um trabalho de transferência, consulte o procedimento a seguir sobre como usar a ação da `GetMetadataTransferJob` API:

1. Depois de criar e executar um trabalho de transferência, ligue para GetMetadataTransferJob:

```
aws iottwinmaker get-metadata-transfer-job \
        --metadata-transfer-job-id your_metadata_transfer_job_id \
        --region us-east-1
```

2. Depois de ver o estado do trabalho para o qual se `COMPLETED` candidata, você pode começar a verificar os resultados do trabalho.
3. Quando você chama`GetMetadataTransferJob`, ele retorna um objeto chamado `MetadataTransferJobProgress`.

   O MetadataTransferJobProgress objeto contém os seguintes parâmetros:

   - FailedCount: indica a contagem de ativos que falharam durante o processo de transferência.
   - skippedCount: indica a contagem de ativos que foram ignorados durante o processo de transferência.
   - SucceededCount: indica a contagem de ativos que foram bem-sucedidos durante o processo de transferência.
   - TotalCount: indica a contagem total de ativos envolvidos no processo de transferência.
4. Além disso, a chamada da API retorna um elemento`reportUrl`, que contém uma URL pré-assinada. Se seu trabalho de transferência tiver algum problema que você precise investigar mais detalhadamente, visite este URL.

Exemplos de importação de metadados

Esta seção mostra como criar arquivos de metadados para importar modelos e ativos de ativos com uma única operação de importação em massa.

Exemplo de importação em massa

Você pode importar vários modelos e ativos de ativos com uma única operação de importação em massa. O exemplo a seguir mostra como criar um arquivo de metadados para fazer isso.

Neste cenário de exemplo, você tem vários locais de trabalho que contêm robôs industriais em células de trabalho.

O exemplo define dois modelos de ativos:

- `RobotModel1`: Esse modelo de ativo representa um tipo específico de robô que você tem em seus locais de trabalho. O robô tem uma propriedade de medição,`Temperature`.
- `WorkCell`: esse modelo de ativo representa uma coleção de robôs em um de seus locais de trabalho. O modelo de ativos define uma hierarquia,`robotHierarchyOEM1`, para representar a relação que uma célula de trabalho contém robôs.

O exemplo também define alguns ativos:

- `WorkCell1`: uma célula de trabalho em seu site em Boston
- `RobotArm123456`: um robô dentro dessa célula de trabalho
- `RobotArm987654`: outro robô dentro dessa célula de trabalho

O arquivo de metadados JSON a seguir define esses modelos e ativos de ativos. A execução de uma importação em massa com esses metadados cria os modelos de ativos e os ativos internos AWS IoT SiteWise, incluindo seus relacionamentos hierárquicos.

Arquivo de metadados para importação

```
{
    "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"
            }
        ]
```

```
        }
    ]
}
```

Exemplo de integração inicial de modelos e ativos

Neste cenário de exemplo, você tem vários locais de trabalho que contêm robôs industriais em uma empresa.

O exemplo define vários modelos de ativos:

- `Sample_Enterprise`— Esse modelo de ativos representa a empresa da qual os sites fazem parte. O modelo de ativos define uma hierarquia`Enterprise to Site`,, para representar a relação dos sites com a empresa.
- `Sample_Site`— Esse modelo de ativos representa os locais de fabricação dentro da empresa. O modelo de ativos define uma hierarquia`Site to Line`,, para representar a relação das linhas com o site.
- `Sample_Welding Line`— Esse modelo de ativos representa uma linha de montagem dentro dos locais de trabalho. O modelo de ativos define uma hierarquia,`Line to Robot`, para representar a relação dos robôs com a linha.
- `Sample_Welding Robot`— Esse modelo de ativos representa um tipo específico de robô em seus locais de trabalho.

O exemplo também define ativos com base nos modelos de ativos.

- `Sample_AnyCompany Motor`— Esse ativo é criado a partir do modelo de `Sample_Enterprise` ativos.
- `Sample_Chicago`— Esse ativo é criado a partir do modelo de `Sample_Site` ativos.
- `Sample_Welding Line 1`— Esse ativo é criado a partir do modelo de `Sample_Welding Line` ativos.
- `Sample_Welding Robot 1`— Esse ativo é criado a partir do modelo de `Sample_Welding Robot` ativos.
- `Sample_Welding Robot 2`— Esse ativo é criado a partir do modelo de `Sample_Welding Robot` ativos.

O arquivo de metadados JSON a seguir define esses modelos e ativos de ativos. A execução de uma importação em massa com esses metadados cria os modelos de ativos e os ativos internos AWS IoT SiteWise, incluindo seus relacionamentos hierárquicos.

Arquivo JSON para integrar ativos e modelos para importação

```
{
    "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",
```

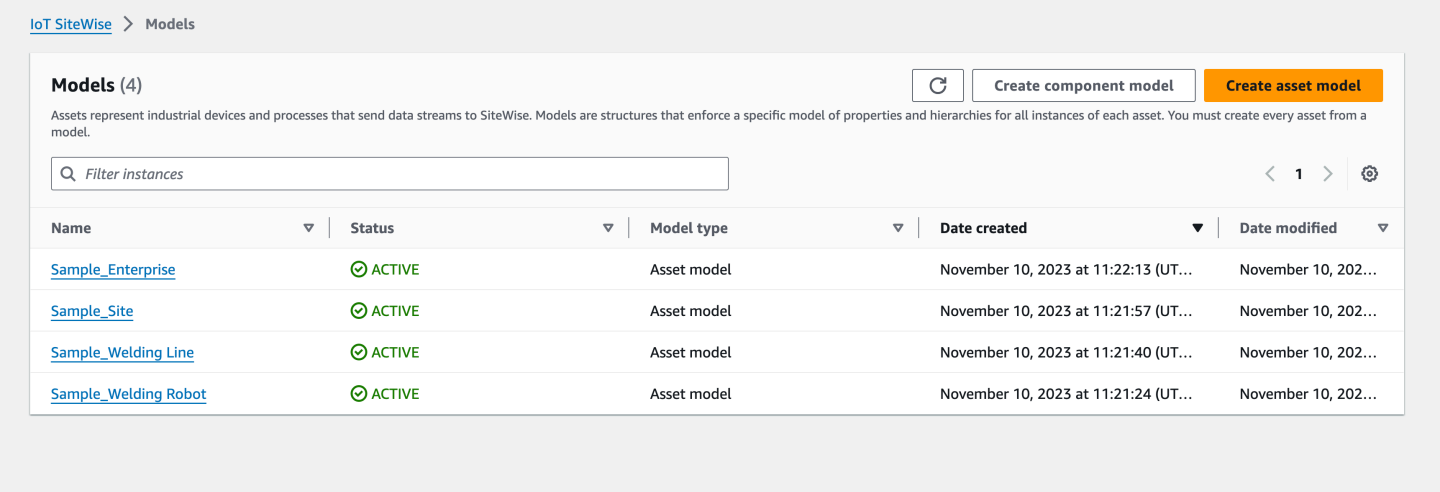
```
                "childAssetModelExternalId": "External_Id_Welding_Robot"
            }
        ]
    },
    {
        "assetModelExternalId": "External_Id_Site",
        "assetModelName": "Sample_Site",
        "assetModelProperties": [
            {
                "dataType": "STRING",
                "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",
```

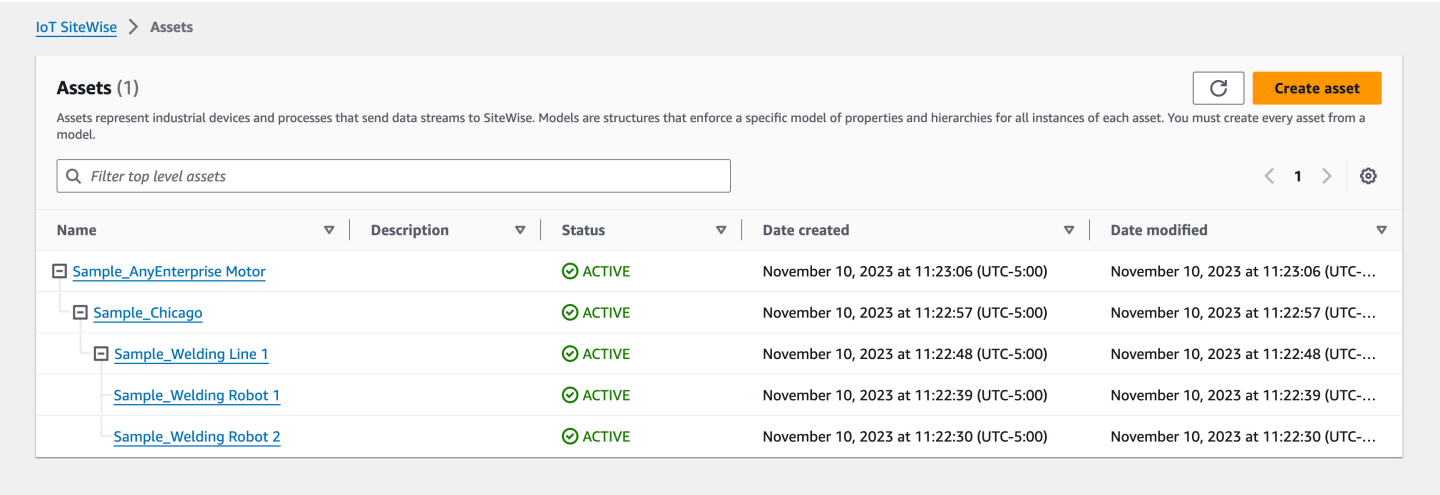
```
                "alias": "AnyCompany/Chicago/Welding Line/S2000/1/Current"
            }
        ]
    },
    {
        "assetExternalId": "External_Id_Welding_Line_1",
        "assetName": "Sample_Welding Line 1",
        "assetModelExternalId": "External_Id_Welding_Line",
        "assetProperties": [
            {
                "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"
```

```
                }
            ]
        }
    ]
}
```

A captura de tela a seguir mostra os modelos exibidos Console do AWS IoT SiteWise após a execução do exemplo de código anterior.



A captura de tela a seguir mostra modelos, ativos e hierarquias que são exibidos Console do AWS IoT SiteWise após a execução do exemplo de código anterior.



Exemplo de integração de ativos adicionais

Este exemplo define ativos adicionais a serem importados para um modelo de ativo existente em sua conta:

- `Sample_Welding Line 2`— Esse ativo é criado a partir do modelo de `Sample_Welding Line` ativos.
- `Sample_Welding Robot 3`— Esse ativo é criado a partir do modelo de `Sample_Welding Robot` ativos.
- `Sample_Welding Robot 4`— Esse ativo é criado a partir do modelo de `Sample_Welding Robot` ativos.

Para criar os ativos iniciais para este exemplo, consulteExemplo de integração inicial de modelos e ativos.

O arquivo de metadados JSON a seguir define esses modelos e ativos de ativos. A execução de uma importação em massa com esses metadados cria os modelos de ativos e os ativos internos AWS IoT SiteWise, incluindo seus relacionamentos hierárquicos.

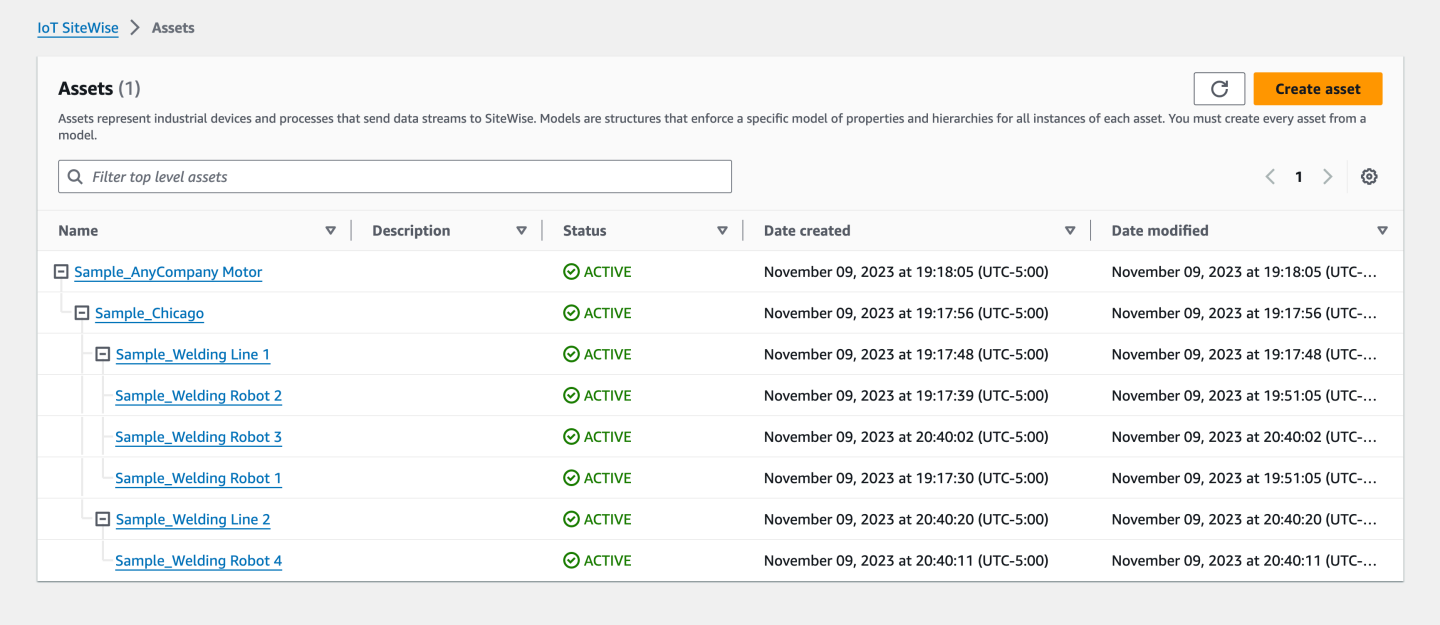
Arquivo JSON para integrar ativos adicionais

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

A captura de tela a seguir mostra modelos, ativos e hierarquias que são exibidos Console do AWS IoT SiteWise após a execução do exemplo de código anterior.



Exemplo de integração de novas propriedades

Este exemplo define novas propriedades em modelos de ativos existentes. Consulte Exemplo de integração de ativos adicionais a integração de ativos e modelos adicionais.

- `Joint 1 Temperature`— Essa propriedade é adicionada ao modelo do `Sample_Welding Robot` ativo. Essa nova propriedade também se propagará para cada ativo criado a partir do modelo de `Sample_Welding Robot` ativo.

Para adicionar uma nova propriedade a um modelo de ativo existente, consulte o exemplo de arquivo de metadados JSON a seguir. Conforme mostrado no JSON, toda a definição do modelo `Sample_Welding Robot` de ativo existente deve ser fornecida junto com a nova propriedade. Se a lista de propriedades inteira da definição existente não for fornecida, AWS IoT SiteWise excluirá as propriedades omitidas.

Arquivo JSON para integrar novas propriedades

Este exemplo adiciona uma nova propriedade `Joint 1 Temperature` ao modelo de ativos.

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

```
    ]
}
```

Exemplos de exportação de metadados

Ao realizar uma exportação em massa do seu AWS IoT SiteWise conteúdo para o Amazon S3, você pode especificar filtros para limitar quais modelos de ativos e ativos específicos você gostaria de exportar.

Você especifica os filtros em uma `iotSiteWiseConfiguration` seção dentro da `sources` seção do corpo da solicitação.

> **Note**
>
> Você pode incluir vários filtros. A operação em massa exportará qualquer modelo de ativo ou ativo que corresponda a qualquer um dos filtros.
> Se você não fornecer nenhum filtro, a operação exportará todos os seus modelos e ativos de ativos.

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

Filtragem por modelo de ativo

Você pode filtrar um modelo de ativo específico. Você também pode incluir todos os ativos usando esse modelo ou todos os modelos de ativos em sua hierarquia. Você não pode incluir ativos e hierarquia.

Para obter mais informações sobre hierarquias, consulte Definindo hierarquias de modelos de ativos.

Asset model

Esse filtro inclui o modelo de ativo especificado:

```
"filterByAssetModel": {
    "assetModelId": "asset model ID"
}
```

Asset model and its assets

Esse filtro inclui o modelo de ativo especificado, junto com todos os ativos que usam esse modelo de ativo:

```
"filterByAssetModel": {
    "assetModelId": "asset model ID",
    "includeAssets": true
}
```

Asset model and its hierarchy

Esse filtro inclui o modelo de ativo especificado, junto com todos os modelos de ativos associados em sua hierarquia:

```
"filterByAssetModel": {
    "assetModelId": "asset model ID",
    "includeOffspring": true
}
```

Filtragem por ativo

Você pode filtrar um ativo específico. Você também pode incluir seu modelo de ativos ou todos os ativos associados em sua hierarquia. Você não pode incluir tanto o modelo de ativos quanto a hierarquia.

Para obter mais informações sobre hierarquias, consulte Definindo hierarquias de modelos de ativos.

Asset

Esse filtro inclui o ativo especificado:

```
"filterByAsset": {
    "assetId": "asset ID"
}
```

Asset and its asset model

Esse filtro inclui o ativo especificado, junto com o modelo de ativo que ele usa:

```
"filterByAsset": {
    "assetId": "asset ID",
    "includeAssetModel": true
}
```

Asset and its hierarchy

Esse filtro inclui o ativo especificado, junto com todos os ativos associados em sua hierarquia:

```
"filterByAsset": {
    "assetId": "asset ID",
    "includeOffspring": true
}
```

AWS IoT SiteWise esquema de trabalho de transferência de metadados

Use o esquema de tarefas de transferência de AWS IoT SiteWise metadados como referência ao realizar suas próprias operações de importação e exportação em massa:

```
{
  "$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"
      }
    }
  }
}
```

Monitorar dados com alarmes

Você pode configurar alarmes para que seus dados alertem sua equipe quando seu equipamento ou processos funcionarem abaixo da qualidade. O desempenho ideal de uma máquina ou de um processo significa que os valores de determinadas métricas devem estar dentro de um intervalo de limites alto e baixo. Quando essas métricas estão fora do intervalo operacional, os operadores de equipamentos devem ser notificados para que possam corrigir o problema. Use alarmes para identificar problemas rapidamente e notificar os operadores para maximizar o desempenho de equipamentos e processos.

Tópicos

Tipos de alarmes

Você pode definir alarmes que são detectados na AWS nuvem e alarmes que você detecta com processos externos. AWS IoT SiteWise suporta os seguintes tipos de alarmes:

- AWS IoT Events alarmes

  AWS IoT Events alarmes são alarmes que detectam em. AWS IoT Events AWS IoT SiteWise envia valores de propriedades de ativos para um modelo de alarme em AWS IoT Events. Em seguida, AWS IoT Events envia o estado do alarme para AWS IoT SiteWise. Você pode configurar opções como quando o alarme detecta e quem notificar quando o estado do alarme mudar. Você também pode definir as AWS IoT Events ações que ocorrem quando o estado do alarme muda.

  Os alarmes em AWS IoT Events são exemplos de modelos de alarme. O modelo de alarme especifica o limite e a gravidade do alarme, o que fazer quando o estado do alarme muda e muito mais. Ao configurar cada característica do modelo de alarme, você especifica uma propriedade de

atributo do modelo de ativo que o alarme monitora. Todos os ativos baseados no modelo de ativos usam o valor do atributo ao AWS IoT Events avaliar essa característica do alarme. Para obter mais informações, consulte Usar alarmes, no Guia do desenvolvedor do AWS IoT Events .

Você pode responder a um AWS IoT Events alarme quando ele muda de estado. Por exemplo, você pode reconhecer ou adiar um alarme quando ele se torna ativo. Você também pode habilitar, desabilitar e redefinir os alarmes.

SiteWise Os usuários do Monitor podem visualizar, configurar e responder aos AWS IoT Events alarmes nos portais do SiteWise Monitor. Para obter mais informações, consulte Monitorar com alarmes, no Guia do aplicativo do AWS IoT SiteWise Monitor .

> **Note**
>
> AWS IoT Events cobranças se aplicam para avaliar esses alarmes e transferir dados entre AWS IoT SiteWise e. AWS IoT Events Para obter mais informações, consulte Preços do AWS IoT Events.

- Alarmes externos

  Alarmes externos são alarmes que você avalia externamente. AWS IoT SiteWise Use alarmes externos se você tiver uma fonte de dados que informe o estado do alarme. O alarme externo contém uma propriedade de medição à qual você ingere os dados do estado do alarme.

  Você não pode reconhecer ou adiar um alarme externo quando ele muda de estado.

  SiteWise Os usuários do monitor podem ver o estado dos alarmes externos nos portais do SiteWise Monitor, mas não podem configurar nem responder a esses alarmes.

  AWS IoT SiteWise não avalia o estado dos alarmes externos.

Estados de alarme

Os alarmes industriais incluem informações sobre o estado do equipamento ou processo que monitoram e informações (opcionais) sobre a resposta do operador ao estado do alarme.

Ao definir um AWS IoT Events alarme, você especifica se deseja ou não ativar o fluxo de reconhecimento. Por padrão, o fluxo de reconhecimento está habilitado. Quando você ativa essa opção, os operadores podem reconhecer o alarme e deixar uma nota com detalhes sobre o alarme

ou as ações que tomaram para resolvê-lo. Se um operador não reconhecer um alarme ativo antes que ele se torne inativo, o alarme será travado. O estado travado indica que o alarme ficou ativo e não foi reconhecido e, portanto, o operador precisa verificar o equipamento ou o processo e reconhecer o alarme travado.

Os alarmes têm os seguintes estados:

- Normal (`Normal`): o alarme está habilitado, mas inativo. O processo industrial ou equipamento opera conforme o esperado.
- Ativo (`Active`): o alarme está ativo. O processo industrial ou equipamento está fora de sua faixa operacional e precisa de atenção.
- Reconhecido (`Acknowledged`): um operador reconheceu o estado do alarme.

  Esse estado se aplica somente aos alarmes nos quais você habilita o fluxo de reconhecimento.
- Travado (`Latched`): o alarme voltou ao normal, mas estava ativo e nenhum operador o reconheceu. O processo industrial ou equipamento requer atenção para reconfigurar o alarme para normal.

  Esse estado se aplica somente aos alarmes nos quais você habilita o fluxo de reconhecimento.
- Adiado (`SnoozeDisabled`): o alarme está desabilitado porque um operador adiou o alarme. O operador define a duração da soneca do alarme. Após esse período, o alarme retorna ao estado normal.
- Desabilitado (`Disabled`): o alarme está desabilitado e não será detectado.

Propriedades do estado do alarme

AWS IoT SiteWise armazena dados do estado do alarme como um objeto JSON serializado em uma string. Esse objeto contém o estado e informações adicionais sobre o alarme, como ações de resposta do operador e a regra que o alarme avalia.

Você identifica a propriedade do estado do alarme pelo nome e tipo de estrutura, `AWS/ALARM_STATE`. Para ter mais informações, consulte Definir alarmes em modelos de ativos.

O objeto dos dados do estado do alarme contém as seguintes informações:

`stateName`

O estado do alarme. Para ter mais informações, consulte Estados de alarme.

Tipo de dados: STRING

customerAction

(Opcional) Um objeto que contém informações sobre a resposta do operador ao alarme. Os operadores podem habilitar, desabilitar, reconhecer e adiar os alarmes. Quando fazem isso, os dados do estado do alarme incluem sua resposta e a nota que eles podem deixar quando responderem. Esse objeto contém as seguintes informações:

actionName

O nome da ação que o operador adota para responder ao alarme. Este valor contém uma das seguintes strings:

- ENABLE
- DISABLE
- SNOOZE
- ACKNOWLEDGE
- RESET

Tipo de dados: STRING

enable

(Opcional) Um objeto que está presente no customerAction quando o operador habilita o alarme. Quando um operador habilita o alarme, o estado do alarme muda para Normal. Esse objeto contém as seguintes informações:

note

(Opcional) A nota que o cliente deixa quando habilita o alarme.

Tipo de dados: STRING

Tamanho máximo: 128 caracteres

disable

(Opcional) Um objeto que está presente em customerAction quando o operador desabilita o alarme. Quando um operador habilita o alarme, o estado do alarme muda para Disabled. Esse objeto contém as seguintes informações:

note

(Opcional) A nota que o cliente deixa quando desabilita o alarme.

Tipo de dados: `STRING`

Tamanho máximo: 128 caracteres

`acknowledge`

(Opcional) Um objeto que está presente em `customerAction` quando o operador reconhece o alarme. Quando um operador habilita o alarme, o estado do alarme muda para `Acknowledged`. Esse objeto contém as seguintes informações:

`note`

(Opcional) A nota que o cliente deixa quando reconhece o alarme.

Tipo de dados: `STRING`

Tamanho máximo: 128 caracteres

`snooze`

(Opcional) Um objeto que está presente `customerAction` quando o operador adia o alarme. Quando um operador habilita o alarme, o estado do alarme muda para `SnoozeDisabled`. Esse objeto contém as seguintes informações:

`snoozeDuration`

A duração em segundos em que o operador adia o alarme. O alarme muda para o estado `Normal` depois desse período.

Tipo de dados: `INTEGER`

`note`

(Opcional) A nota que o cliente deixa quando adia o alarme.

Tipo de dados: `STRING`

Tamanho máximo: 128 caracteres

`ruleEvaluation`

(Opcional) Um objeto que contém informações sobre a regra que avalia o alarme. Esse objeto contém as seguintes informações:

`simpleRule`

Um objeto que contém informações sobre uma regra simples, que compara um valor de propriedade a um valor limite com um operador de comparação. Esse objeto contém as seguintes informações:

`inputProperty`

O valor da propriedade que esse alarme avalia.

Tipo de dados: `DOUBLE`

`operator`

O operador de comparação que esse alarme usa para comparar a propriedade com o limite. Este valor contém uma das seguintes strings:

- <: menor que
- <=: menor ou igual a
- ==: igual
- !=: não igual
- >=: maior ou igual a
- >: maior que

Tipo de dados: `STRING`

`threshold`

O valor limite com o qual esse alarme compara o valor da propriedade.

Tipo de dados: `DOUBLE`

Definir alarmes em modelos de ativos

Os modelos de ativo promovem a padronização de seus dados industriais. É possível estabelecer definições de alarme em modelos de ativos para padronizar os alarmes para todos os ativos com base em um modelo de ativo.

Você usa modelos de ativos compostos para definir alarmes no modelo de ativos. Os modelos de ativos compostos são modelos de ativos que padronizam um conjunto específico de propriedades

em outro modelo de ativo. Modelos de ativos compostos garantem que determinadas propriedades estejam presentes em um modelo de ativo. Os alarmes têm propriedades de tipo, estado e fonte (opcionais) e, portanto, o modelo composto de alarme garante que essas propriedades existam.

Cada modelo composto tem um tipo que define as propriedades para o modelo composto. Os modelos compostos de alarme definem propriedades para tipo de alarme, estado de alarme e fonte de alarme (opcional). Quando você cria um ativo a partir de um modelo de ativo com modelos compostos, o ativo inclui as propriedades do modelo composto juntamente com as propriedades que você especifica no modelo de ativo.

Cada propriedade em um modelo composto deve ter o nome que a identifique por seu tipo de modelo composto. As propriedades do modelo composto são compatíveis propriedades com tipos de dados complexos. Essas propriedades têm o tipo de dados `STRUCT` e um atributo `dataTypeSpec` que especifica o tipo de dados complexos da propriedade. As propriedades de tipos de dados complexos contêm dados JSON serializados como strings.

Os modelos compostos de alarme têm as propriedades abaixo. Cada propriedade em um modelo composto deve ter o nome que os identifica por seu tipo de modelo composto.

Tipo de alarme

O tipo do alarme. Especifique um dos seguintes:

- `IOT_EVENTS`— Um AWS IoT Events alarme. AWS IoT SiteWise envia dados AWS IoT Events para avaliar o estado desse alarme. Você deve especificar a propriedade da fonte de alarme para definir o modelo de AWS IoT Events alarme para essa definição de alarme.
- `EXTERNAL`: um alarme externo. Você ingere o estado do alarme como medição.

Nome da propriedade: `AWS/ALARM_TYPE`

Tipo de propriedade: atributo

Tipo de dados: `STRING`

Estado do alarme

Os dados de séries temporais do estado do alarme. Este é um objeto serializado como uma string que contém o estado e outras informações sobre o alarme. Para ter mais informações, consulte Propriedades do estado do alarme.

Nome da propriedade: `AWS/ALARM_STATE`

Tipo de propriedade: medição

Tipo de dados: `STRUCT`

Tipo de estrutura de dados: `AWS/ALARM_STATE`

Fonte de alarme

(Opcional) O nome do recurso da Amazon (ARN) do recurso que avalia o estado do alarme. Para AWS IoT Events alarmes, esse é o ARN do modelo de alarme.

Nome da propriedade: `AWS/ALARM_SOURCE`

Tipo de propriedade: atributo

Tipo de dados: `STRING`

Example Exemplo de modelo de alarme composto

O modelo de ativos a seguir representa uma caldeira que tem um alarme para monitorar sua temperatura. AWS IoT SiteWise envia os dados de temperatura AWS IoT Events para detectar o alarme.

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

Tópicos

- Definindo AWS IoT Events alarmes
- Definir alarmes externos

Definindo AWS IoT Events alarmes

Quando você cria um AWS IoT Events alarme, AWS IoT SiteWise envia valores de propriedades do ativo AWS IoT Events para avaliar o estado do alarme. AWS IoT Events as definições de alarme dependem de um modelo de alarme que você define em AWS IoT Events. Para definir um AWS IoT Events alarme em um modelo de ativo, você define um modelo composto de alarme que especifica o modelo de AWS IoT Events alarme como sua propriedade de fonte de alarme.

AWS IoT Events os alarmes dependem de entradas, como limites de alarme e configurações de notificação de alarme. Você define essas entradas como atributos no modelo do ativo. Em seguida, você pode personalizar essas entradas em cada ativo com base no modelo. O AWS IoT SiteWise console pode criar esses atributos para você. Se você definir alarmes com a API AWS CLI ou, deverá definir manualmente esses atributos no modelo de ativo.

Você também pode definir outras ações que acontecem quando o alarme detecta, como ações personalizadas de notificação de alarme. Por exemplo, você pode configurar uma ação que envie uma notificação push para um tópico do Amazon SNS. Para obter mais informações sobre as ações que você pode definir, consulte Trabalhando com outros AWS serviços no Guia do AWS IoT Events desenvolvedor.

Quando você atualiza ou exclui um modelo de ativo, AWS IoT SiteWise pode verificar se um modelo de alarme AWS IoT Events está monitorando uma propriedade de ativo associada a esse modelo de ativo. Isso impede que você exclua uma propriedade do ativo que um AWS IoT Events alarme está usando atualmente. Para ativar esse recurso AWS IoT SiteWise, você deve ter a `iotevents:ListInputRoutings` permissão. Essa permissão permite AWS IoT SiteWise fazer chamadas para a operação da API ListInputRoutings suportada pelo AWS IoT Events. Para ter mais informações, consulte ListInputRoutings Permissão (opcional).

> **Note**
>
> O recurso de notificações de alarme não está disponível na Região da China (Pequim).

Tópicos

- Requisitos para notificações de alarmes
- Definindo um AWS IoT Events alarme (AWS IoT SiteWise console)
- Definindo um AWS IoT Events alarme (AWS IoT Events console)

- Definindo um AWS IoT Events alarme (AWS CLI)

Requisitos para notificações de alarmes

AWS IoT Events usa uma AWS Lambda função na sua AWS conta para enviar notificações de alarme. Você deve criar essa função Lambda na mesma AWS região dos seus alarmes para ativar as notificações de alarme. Essa função do Lambda usa o Amazon Simple Notification Service (Amazon SNS) para enviar notificações por texto e o Amazon Simple Email Service (Amazon SES) para enviar notificações por e-mail. Ao criar o AWS IoT Events alarme, você configura os protocolos e as configurações que o alarme usa para enviar notificações.

AWS IoT Events fornece um modelo de AWS CloudFormation pilha que você pode usar para criar essa função Lambda em sua conta. Para obter mais informações, consulte Notificação de alarme da função do Lambda no Guia do desenvolvedor do AWS IoT Events .

Definindo um AWS IoT Events alarme (AWS IoT SiteWise console)

Você pode usar o AWS IoT SiteWise console para definir um AWS IoT Events alarme em um modelo de ativo existente. Para definir um AWS IoT Events alarme em um novo modelo de ativo, crie o modelo de ativo e conclua essas etapas. Para ter mais informações, consulte Criar modelos de ativo.

> **Important**
>
> Cada alarme requer um atributo que especifique o valor limite a ser comparado ao alarme. Você deve definir o atributo de valor limite no modelo do ativo antes de definir um alarme. Pense em um exemplo em que você deseja definir um alarme que detecta quando uma turbina eólica excede sua taxa máxima de velocidade do vento de 50 mph. Antes de definir o alarme, você deve definir um atributo (Velocidade máxima do vento) com um valor padrão do `50`.

Para definir um AWS IoT Events alarme em um modelo de ativo

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Modelos.
3. Escolha o modelo de ativo para o qual o alarme será definido.
4. Escolha a guia Alarme.

5. Escolha Adicionar alarme.
6. Na seção Opções do tipo de alarme, escolha alarme do AWS IoT Events .
7. Na seção Detalhes básicos, faça o seguinte:
   a. Insira um nome para o alarme.
   b. (Opcional) Insira uma descrição do seu alarme.
8. Na página Definir limite, você define quando o alarme detecta e a gravidade do alarme. Faça o seguinte:
   a. Selecione a Propriedade na qual o alarme detecta. Cada vez que essa propriedade recebe um novo valor, AWS IoT SiteWise envia o valor AWS IoT Events para avaliar o estado do alarme.
   b. Selecione o Operador a ser usado para comparar a propriedade com o valor limite. Escolha uma das seguintes opções:
      - < menor que
      - <= menor ou igual a
      - == igual
      - != não igual
      - >= maior ou igual a
      - > maior que
   c. Em Valor, selecione a propriedade do atributo a ser usada como valor limite. AWS IoT Events compara o valor da propriedade com o valor desse atributo.
   d. Insira a Gravidade do alarme. Use um número que sua equipe entenda para refletir a gravidade desse alarme.
9. (Opcional) Na seção Configurações de notificação - opcional, faça o seguinte:
   a. Selecione Ativo.

      > **Note**
      >
      > Se escolher Inativo, você e sua equipe não receberão nenhuma notificação de alarme.

   b. Em Destinatário, escolha o destinatário.

> **Important**
>
> Você pode enviar notificações de alarme aos AWS IAM Identity Center usuários. Para usar esse recurso, você deve habilitar o Centro de identidade do IAM. Você só pode ativar o IAM Identity Center em uma AWS região por vez. Isso significa que você pode definir notificações de alarme somente na região em que você habilita o Centro de identidade do IAM. Para obter mais informações, consulte Conceitos básicos no Guia do usuário do AWS IAM Identity Center .

c. Para o Protocolo, escolha uma das seguintes opções:

- E-mail e texto: o alarme notifica os usuários do Centro de identidade do IAM com uma mensagem SMS e uma mensagem de e-mail.
- E-mail: o alarme notifica os usuários do Centro de identidade do IAM com uma mensagem de e-mail.
- Texto: o alarme notifica os usuários do Centro de identidade do IAM com uma mensagem SMS.

d. Em Remetente, escolha o remetente.

> **Important**
>
> Você deve verificar o endereço de e-mail do remetente no Amazon Simple Email Service (Amazon SES). Para mais informações, consulte Verificar endereços de e-mail no Amazon SES no Guia do desenvolvedor do Amazon Simple Email Service.

10. Na seção Estado padrão do ativo, você pode definir o estado padrão para os alarmes criados a partir desse modelo de ativo.

> **Note**
>
> Você ativa ou desativa esse alarme para ativos que você cria a partir desse modelo de ativo em uma etapa posterior.

11. Na seção Configurações avançadas, você pode definir as permissões, as configurações adicionais de notificação, as ações do estado do alarme, o modelo de alarme no SiteWise Monitor e o fluxo de reconhecimento.

> **Note**
>
> AWS IoT Events os alarmes exigem as seguintes funções de serviço:
>
> - Uma função que AWS IoT Events pressupõe enviar valores de estado de alarme para AWS IoT SiteWise.
> - Uma função que AWS IoT Events pressupõe enviar dados para o Lambda. Você só precisa desse perfil se o alarme enviar notificações.

Na página Permissões, faça o seguinte:

a. Para o perfil AWS IoT Events , use um perfil existente ou crie um perfil com as permissões necessárias. Esse perfil requer a permissão de `iotsitewise:BatchPutAssetPropertyValue` e um relacionamento de confiança que permita que iotevents.amazonaws.com assuma o perfil.

b. Para o AWS IoT Events perfil do Lambda, use um perfil existente ou crie um perfil com as permissões necessárias. Esse perfil requer as permissões `lambda:InvokeFunction` e `sso-directory:DescribeUser` e um relacionamento de confiança que permita que `iotevents.amazonaws.com` assuma o perfil.

12. (Opcional) Na seção Configurações de notificação adicionais, faça o seguinte:

a. Para o Atributo destinatário, você define um atributo cujo valor especifica o destinatário da notificação. Você pode escolher os usuários do Centro de identidade do IAM como destinatários.

   Você pode criar um atributo ou usar um atributo existente no modelo de ativo.

   - Se você escolher Criar um novo atributo de destinatário, especifique o Nome do atributo do destinatário e o Valor padrão do destinatário - opcional para o atributo.
   - Se você escolher Usar um atributo de destinatário existente, escolha o atributo em Nome do atributo de destinatário. O alarme usa o valor padrão do atributo escolhido.

   Você pode substituir o valor padrão em cada ativo criado a partir desse modelo de ativo.

b. Para Atributo de mensagem personalizada, você define um atributo cujo valor especifica a mensagem personalizada a ser enviada, além da mensagem padrão de alteração de

estado. Por exemplo, você pode especificar uma mensagem que ajude sua equipe a entender como lidar com esse alarme.

Você pode escolher criar um atributo ou usar um atributo existente no modelo de ativo.

- Se você optar por Criar um novo atributo de mensagem personalizada, especifique o Nome do atributo de mensagem personalizada e o Valor padrão da mensagem personalizada - opcional para o atributo.
- Se você escolher Usar um atributo de mensagem personalizada existente, escolha o atributo em Nome do atributo de mensagem personalizada. O alarme usa o valor padrão do atributo escolhido.

Você pode substituir o valor padrão em cada ativo criado a partir desse modelo de ativo.

c. Em Gerencie sua função do Lambda, siga um destes procedimentos:

- Para AWS IoT SiteWise criar uma nova função Lambda, escolha Criar um novo lambda a partir de um modelo gerenciado pela AWS.
- Para usar um perfil da função do Lambda existente, escolha Usar um lambda existente e escolha o nome da função.

Para obter mais informações, consulte Gerenciar notificações de alarme no Guia do desenvolvedor do AWS IoT Events .

13. (Opcional) Na seção Definir ação de estado faça o seguinte:

a. Escolha Editar ação.

b. Em Adicionar ações de estado de alarme, adicione ações. e escolha Salvar.

Você pode adicionar até 10 ações.

AWS IoT Events pode realizar ações quando o alarme está ativo. Você pode definir ações integradas para usar um cronômetro, definir uma variável ou enviar dados para outros AWS recursos. Para obter mais informações, consulte Ações compatíveis no Guia do desenvolvedor do AWS IoT Events .

14. (Opcional) Em Gerenciar modelo de alarme em SiteWise Monitor - opcional, escolha Ativo ou Inativo.

Use essa opção para que você possa atualizar o modelo de alarme em SiteWise Monitores. Essa opção é habilitada por padrão.

15. Em Reconhecer fluxo, escolha Ativo ou Inativo. Para obter mais informações sobre o fluxo de reconhecimento, consulte Estados de alarme.
16. Escolha Adicionar alarme.

> **Note**
>
> O AWS IoT SiteWise console faz várias solicitações de API para adicionar o alarme ao modelo de ativos. Quando você escolhe Adicionar alarme, o console abre uma caixa de diálogo que mostra o progresso dessas solicitações de API. Permaneça nesta página até que cada solicitação de API seja bem-sucedida ou até que uma solicitação de API falhe. Se uma solicitação falhar, feche a caixa de diálogo, corrija o problema e escolha Adicionar alarme para tentar novamente.

Definindo um AWS IoT Events alarme (AWS IoT Events console)

Você pode usar o AWS IoT Events console para definir um AWS IoT Events alarme em um modelo de ativo existente. Para definir um AWS IoT Events alarme em um novo modelo de ativo, crie o modelo de ativo e conclua essas etapas. Para ter mais informações, consulte Criar modelos de ativo.

> **Important**
>
> Cada alarme requer um atributo que especifique o valor limite a ser comparado ao alarme. Você deve definir o atributo de valor limite no modelo do ativo antes de definir um alarme. Pense em um exemplo em que você deseja definir um alarme que detecta quando uma turbina eólica excede sua taxa máxima de velocidade do vento de 50 mph. Antes de definir o alarme, você deve definir um atributo (Velocidade máxima do vento) com um valor padrão do `50`.

Para definir um AWS IoT Events alarme em um modelo de ativo

1. Navegue até o console do AWS IoT Events.
2. No painel de navegação, selecione Modelos de alarme.
3. Selecione Criar modelo de alarme.

4. Insira um nome para o alarme.
5. (Opcional) Insira uma descrição do seu alarme.
6. Na seção Alarme de destino, faça o seguinte:
   a. Para Opções de destino, escolha Propriedade do ativo do AWS IoT SiteWise .
   b. Escolha o modelo de ativo para o qual deseja adicionar um alarme.
7. Na página Definir limite, você define quando o alarme detecta e a gravidade do alarme. Faça o seguinte:
   a. Selecione a Propriedade na qual o alarme detecta. Cada vez que essa propriedade recebe um novo valor, AWS IoT SiteWise envia o valor AWS IoT Events para avaliar o estado do alarme.
   b. Selecione o Operador a ser usado para comparar a propriedade com o valor limite. Escolha uma das seguintes opções:
      - **<** menor que
      - **<=** menor ou igual a
      - **==** igual
      - **!=** não igual
      - **>=** maior ou igual a
      - **>** maior que
   c. Em Valor, selecione a propriedade do atributo a ser usada como valor limite. AWS IoT Events compara o valor da propriedade com o valor desse atributo.
   d. Insira a Gravidade do alarme. Use um número que sua equipe entenda para refletir a gravidade desse alarme.
8. (Opcional) Na seção Configurações de notificação - opcional, faça o seguinte:
   a. Para o Protocolo, escolha uma das seguintes opções:
      - E-mail e texto: o alarme notifica os usuários do Centro de identidade do IAM com uma mensagem SMS e uma mensagem de e-mail.
      - E-mail: o alarme notifica os usuários do Centro de identidade do IAM com uma mensagem de e-mail.
      - Texto: o alarme notifica os usuários do Centro de identidade do IAM com uma mensagem SMS.

b. Em Remetente, escolha o remetente.

> **Important**
>
> Você deve verificar o endereço de e-mail do remetente no Amazon Simple Email Service (Amazon SES). Para mais informações, consulte Verificar endereços de e-mail no Amazon SES no Guia do desenvolvedor do Amazon Simple Email Service.

c. Escolha o atributo em Atributo do destinatário - opcional. O alarme usa o valor padrão do atributo escolhido.

d. Escolha o atributo em Atributo de mensagem personalizada - opcional. O alarme usa o valor padrão do atributo escolhido.

9. Na seção Instância, especifique o Estado padrão para esse alarme. Você pode ativar ou desativar esse alarme para todos os ativos criados a partir desse modelo de ativo em uma etapa posterior.

10. Nas configurações avançadas, você pode definir as permissões, as configurações adicionais de notificação, as ações do estado do alarme, o modelo de alarme no SiteWise Monitor e o fluxo de reconhecimento.

> **Note**
>
> AWS IoT Events os alarmes exigem as seguintes funções de serviço:
>
> - Uma função que AWS IoT Events pressupõe enviar valores de estado de alarme para AWS IoT SiteWise.
> - Uma função que AWS IoT Events pressupõe enviar dados para o Lambda. Você só precisa desse perfil se o alarme enviar notificações.

a. Na seção Reconhecer fluxo, escolha Habilitado ou Desabilitado. Para obter mais informações sobre o fluxo de reconhecimento, consulte Estados de alarme.

b. Na página Permissões, faça o seguinte:

i. Para o perfil AWS IoT Events , use um perfil existente ou crie um perfil com as permissões necessárias. Esse perfil requer a permissão de `iotsitewise:BatchPutAssetPropertyValue` e um relacionamento de confiança que permita que iotevents.amazonaws.com assuma o perfil.

ii. Para o perfil do Lambda, use um perfil existente ou crie um perfil com as permissões necessárias. Esse perfil requer as permissões `lambda:InvokeFunction` e `sso-directory:DescribeUser` e um relacionamento de confiança que permita que `iotevents.amazonaws.com` assuma o perfil.

c. (Opcional) No painel Configurações de notificação adicionais, faça o seguinte:

- Em Gerencie sua função do Lambda, siga um destes procedimentos:
  - Para AWS IoT Events criar uma nova função Lambda, escolha Criar uma nova função Lambda.
  - Para usar uma função do Lambda existente, escolha Usar uma função do Lambda existente e escolha o nome da função.

Para obter mais informações, consulte Gerenciar notificações de alarme no Guia do desenvolvedor do AWS IoT Events .

d. (Opcional) Na seção Definir ação de estado - opcional, faça o seguinte:

- Em Ações de estado de alarme, adicione ações e escolha Salvar.

Você pode adicionar até 10 ações.

AWS IoT Events pode realizar ações quando o alarme está ativo. Você pode definir ações integradas para usar um cronômetro, definir uma variável ou enviar dados para outros AWS recursos. Para obter mais informações, consulte Ações compatíveis no Guia do desenvolvedor do AWS IoT Events .

11. Escolha Criar.

> **Note**
>
> O AWS IoT Events console faz várias solicitações de API para adicionar o alarme ao modelo de ativos. Quando você escolhe Adicionar alarme, o console abre uma caixa de diálogo que mostra o progresso dessas solicitações de API. Permaneça nesta página até que cada solicitação de API seja bem-sucedida ou até que uma solicitação de API falhe. Se uma solicitação falhar, feche a caixa de diálogo, corrija o problema e escolha Adicionar alarme para tentar novamente.

Definindo um AWS IoT Events alarme (AWS CLI)

Você pode usar o AWS Command Line Interface (AWS CLI) para definir um AWS IoT Events alarme que monitora uma propriedade do ativo. Você pode definir o alarme em um modelo de ativo novo ou existente. Depois de definir o alarme no modelo de ativo, você cria um alarme AWS IoT Events e o conecta ao modelo de ativo. Neste processo, você faz o seguinte:

Etapas

- Etapa 1: definir um alarme em um modelo de ativo
- Etapa 2: Definindo um modelo AWS IoT Events de alarme
- Etapa 3: Habilitando o fluxo de dados entre AWS IoT SiteWise e AWS IoT Events

Etapa 1: definir um alarme em um modelo de ativo

Adicione uma definição de alarme e as propriedades associadas a um modelo de ativo novo ou existente.

Para definir um alarme em um modelo de ativo (CLI)

1. Crie um arquivo chamado `asset-model-payload.json`. Siga as etapas nessas outras seções para adicionar os detalhes do seu modelo de ativo para o arquivo, mas não envie a solicitação para criar ou atualizar o modelo de ativo. Nesta seção, você adiciona uma definição de alarme aos detalhes do modelo de ativo no arquivo `asset-model-payload.json`.
   - Para obter mais informações sobre como criar um modelo de ativo, consulte Criação de um modelo de ativo (AWS CLI).
   - Para obter mais informações sobre como atualizar um modelo de ativo existente, consulte Atualizando um modelo de ativo ou componente (AWS CLI).

   > **Note**
   >
   > Seu modelo de ativo deve definir pelo menos uma propriedade do ativo, incluindo a propriedade do ativo a ser monitorada com o alarme.

2. Adicione um modelo de alarme composto (`assetModelCompositeModels`) para o modelo do ativo. Um modelo composto de AWS IoT Events alarme especifica o `IOT_EVENTS` tipo e especifica uma propriedade da fonte de alarme. Você adiciona a propriedade da fonte de alarme depois de criar o modelo de alarme em AWS IoT Events.

> **Important**
>
> O modelo composto de alarme deve ter o mesmo nome do modelo de AWS IoT Events alarme que você criar posteriormente. Nomes de modelo de alarme podem conter apenas caracteres alfanuméricos. Especifique um nome alfanumérico exclusivo para que você possa usar o mesmo nome para o modelo de alarme.

```
{
  ...
  "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. Adicione um atributo de limite de alarme ao modelo de ativo. Especifique o valor padrão a ser usado para esse limite. Você pode substituir esse valor padrão em cada ativo com base nesse modelo.

> **Note**
>
> O atributo de limite de alarme deve ser um `INTEGER` ou um `DOUBLE`.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "Temperature Max Threshold",
      "dataType": "DOUBLE",
      "type": {
        "attribute": {
          "defaultValue": "105.0"
        }
      }
    }
  ]
}
```

4. (Opcional) Adicione atributos de notificação de alarme ao modelo de ativo. Esses atributos especificam o destinatário do IAM Identity Center e outras entradas AWS IoT Events usadas para enviar notificações quando o alarme muda de estado. Você pode substituir esses padrões em cada ativo com base nesse modelo.

   > **Important**
   >
   > Você pode enviar notificações de alarme aos AWS IAM Identity Center usuários. Para usar esse recurso, você deve habilitar o Centro de identidade do IAM. Você só pode ativar o IAM Identity Center em uma AWS região por vez. Isso significa que você pode definir notificações de alarme somente na região em que você habilita o Centro de identidade do IAM. Para obter mais informações, consulte Conceitos básicos no Guia do usuário do AWS IAM Identity Center .

   Faça o seguinte:

a. Adicionar um atributo que especifique o ID do seu repositório de identidades do Centro de identidade do IAM. Você pode usar a operação da ListInstancesAPI do IAM Identity Center para listar seus repositórios de identidade. Essa operação funciona somente na região em que você habilita o Centro de identidade do IAM.

```
aws sso-admin list-instances
```

Em seguida, especifique a ID do repositório de identidade (por exemplo, `d-123EXAMPLE`) como o valor padrão para o atributo.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "identityStoreId",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "d-123EXAMPLE"
        }
      }
    }
  ]
}
```

b. Adicionar um atributo que especifique a ID do usuário do Centro de identidade do IAM que recebe notificações. Para definir um destinatário padrão da notificação, adicione uma ID de usuário do Centro de identidade do IAM como valor padrão. Faça o seguinte para obter uma ID de usuário do Centro de identidade do IAM:

i. Você pode usar a ListUsersAPI do IAM Identity Center para obter o ID de um usuário cujo nome de usuário você conhece. Substitua o *D-123Example* pela ID do seu repositório de identidade e substitua *Nome* pelo nome de usuário do usuário.

```
aws identitystore list-users \
  --identity-store-id d-123EXAMPLE \
  --filters AttributePath=UserName,AttributeValue=Name
```

ii. Use o console do Centro de identidade do IAM para procurar seus usuários e encontrar uma ID de usuário.

Em seguida, especifique a ID do usuário (por exemplo, `123EXAMPLE-a1b2c3d4-5678-90ab-cdef-33333EXAMPLE`) como o valor padrão para o atributo ou defina o atributo sem um valor padrão.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "userId",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "123EXAMPLE-a1b2c3d4-5678-90ab-cdef-33333EXAMPLE"
        }
      }
    }
  ]
}
```

c. (Opcional) Adicione um atributo que especifique a ID do remetente padrão para notificações por mensagens SMS (texto). A ID do remetente é exibida como o remetente da mensagem em mensagens enviadas pelo Amazon Simple Notification Service (Amazon SNS). Para obter mais informações, consulte Solicitar IDs do remetente para mensagens SMS com o Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "senderId",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "MyFactory"
        }
      }
```

```
    }
  ]
}
```

d. (Opcional) Adicione um atributo que especifique o endereço de e-mail padrão a ser usado como endereço De nas notificações por e-mail.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "fromAddress",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "my.factory@example.com"
        }
      }
    }
  ]
}
```

e. (Opcional) Adicione um atributo que especifique o assunto padrão a ser usado nas notificações por e-mail.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "emailSubject",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "[ALERT] High boiler temperature"
        }
      }
    }
  ]
}
```

f. (Opcional) Adicione um atributo que especifique uma mensagem adicional a ser incluída nas notificações. Por padrão, as mensagens de notificação incluem informações sobre o alarme. Você também pode incluir uma mensagem adicional que forneça mais informações ao usuário.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "additionalMessage",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "Turn off the power before you check the alarm."
        }
      }
    }
  ]
}
```

5. Crie o modelo de ativo ou atualize o modelo de ativo existente. Execute um destes procedimentos:

   - Para criar o modelo de ativo, execute o comando a seguir.

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

   - Para atualizar o modelo de ativo existente, execute o comando a seguir. Substitua *asset-model-id* pela ID do modelo de ativo.

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

   Depois de executar o comando, observe o `assetModelId` na resposta.

Exemplo: modelo de ativos de caldeiras

O modelo de ativo a seguir representa uma caldeira que relata dados de temperatura. Esse modelo de ativos define um alarme que detecta quando a caldeira superaquece.

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

Etapa 2: Definindo um modelo AWS IoT Events de alarme

Crie o modelo de alarme em AWS IoT Events. Em AWS IoT Events, você usa expressões para especificar valores em modelos de alarme. Você pode usar expressões para especificar valores AWS IoT SiteWise para avaliar e usar como entradas para o alarme. Ao AWS IoT SiteWise enviar valores da propriedade do ativo para o modelo de alarme, AWS IoT Events avalia a expressão para obter o valor da propriedade ou o ID do ativo. Você pode usar as expressões a seguir no modelo de alarme:

- Valores de propriedade de ativos

  Para obter o valor de uma propriedade de ativos, use a expressão a seguir. ModelIdSubstitua o *`ativo`* pelo ID do modelo do ativo e substitua *`propertyID`* pelo ID da propriedade.

  ```
  $sitewise.assetModel.`assetModelId`.`propertyId`.propertyValue.value
  ```

- IDs de ativo

Para obter a ID do ativo, use a expressão a seguir. ModelIdSubstitua o *ativo* pelo ID do modelo do ativo e substitua *propertyID* pelo ID da propriedade.

```
$sitewise.assetModel.`assetModelId`.`propertyId`.assetId
```

> **Note**
>
> Ao criar o modelo de alarme, você pode definir literais em vez de expressões que são avaliadas como AWS IoT SiteWise valores. Isso pode reduzir o número de atributos que você define em seu modelo de ativo. No entanto, se você definir um valor como substantivo, não poderá personalizar esse valor nos ativos com base no modelo do ativo. Seus AWS IoT SiteWise Monitor usuários também não podem personalizar o alarme, pois podem definir as configurações de alarme somente nos ativos.

Para criar um modelo AWS IoT Events de alarme (CLI)

1. Ao criar o modelo de alarme em AWS IoT Events, você deve especificar o ID de cada propriedade que o alarme usa, o que inclui o seguinte:

   - A propriedade do estado do alarme no modelo de ativo composto
   - A propriedade que o alarme monitora
   - O atributo limite
   - (Opcional) O atributo de ID do repositório de identidades do Centro de identidade do IAM
   - (Opcional) O atributo de ID de usuário do Centro de identidade do IAM
   - (Opcional) O atributo de ID de remetente de SMS
   - (Opcional) O atributo e-mail do endereço De
   - (Opcional) O atributo do assunto do e-mail
   - (Opcional) O atributo adicional de mensagem

   Execute o comando a seguir para recuperar as IDs dessas propriedades no modelo de ativo. Substitua *asset-model-id* pela ID do modelo de ativo da etapa anterior.

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

A operação retorna uma resposta que contém os detalhes do modelo de ativo. Anote a ID de cada propriedade que o alarme usa. Você usa essas IDs quando cria o modelo de alarme do AWS IoT Events na próxima etapa.

2. Crie o modelo de alarme em AWS IoT Events. Faça o seguinte:

   a. Crie um arquivo chamado `alarm-model-payload.json`.

   b. Copie o JSON a seguir no arquivo.

   c. Insira um nome(`alarmModelName`), uma descrição (`alarmModelDescription`) e a gravidade (`severity`) para o alarme. Para gravidade, especifique um número inteiro que reflita os níveis de gravidade da sua empresa.

   > **Important**
   >
   > O modelo de alarme deve ter o mesmo nome do modelo de alarme composto que você definiu em seu modelo de ativo anteriormente.
   > Nomes de modelo de alarme podem conter apenas caracteres alfanuméricos.

   ```
   {
     "alarmModelName": "BoilerTemperatureHighAlarm",
     "alarmModelDescription": "Detects when the boiler temperature is high.",
     "severity": 3
   }
   ```

   d. Adicione a regra de comparação (`alarmRule`) para o alarme. Essa regra define a propriedade a ser monitorada (`inputProperty`), o valor limite a ser comparado (`threshold`) e o operador de comparação a ser usado (`comparisonOperator`).

   - ModelIdSubstitua o *`ativo`* pelo ID do modelo de ativo.
   - PropertyIdSubstitua o *`alarme`* pela ID da propriedade que o alarme monitora.
   - Substitua o *`limite AttributeId`* pelo ID da propriedade do atributo de limite.
   - Substitua *`MAIOR`* pelo operador a ser usado para comparar a propriedade com o valor limite. Escolha uma das seguintes opções:
     - `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. Adicione uma ação (`alarmEventActions`) para enviar o estado do alarme para AWS IoT SiteWise quando o alarme muda de estado.

> **Note**
>
> Para configuração avançada, você pode definir ações adicionais a serem realizadas quando o alarme mudar de estado. Por exemplo, você pode chamar uma função AWS Lambda ou publicar em um tópico do MQTT. Para obter mais informações, consulte Trabalhando com outros AWS serviços no Guia do AWS IoT Events desenvolvedor.

- ModelIdSubstitua o *`ativo`* pelo ID do modelo de ativo.
- PropertyIdSubstitua o *`alarme`* pela ID da propriedade que o alarme monitora.
- Substitua o *`StatePropertyID`* do alarme pelo ID da propriedade do estado do alarme no modelo composto do alarme.

```
{
```

```
  "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) Definir configurações de notificação de alarmes. A ação de notificação de alarme usa uma função do Lambda em sua conta para enviar notificações de alarme. Para ter mais informações, consulte Requisitos para notificações de alarmes. Nas configurações de notificação de alarme, você pode configurar notificações por SMS e e-mail para enviar aos usuários do Centro de identidade do IAM. Faça o seguinte:

   i. Adicione a configuração de notificação de alarme (`alarmNotification`) à carga útil em `alarm-model-payload.json`.

      - Substitua o *alarme NotificationFunction Arn* pelo ARN da função Lambda que manipula as notificações de alarme.

```
{
  "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 as notificações por SMS (`smsConfigurations`) para enviar a um usuário do Centro de identidade do IAM quando o alarme mudar de estado.

- StoreIdAttributeIdSubstitua a *`identidade`* pela ID do atributo que contém a ID do repositório de identidades do IAM Identity Center.
- Substitua o *`IdAttributeID do usuário`* pelo ID do atributo que contém o ID do usuário do IAM Identity Center.
- Substitua o *`IdAttributeID do remetente`* pelo ID do atributo que contém o ID do remetente do Amazon SNS ou `senderId` remova-o da carga.

- Substitua a *`MessageAttributeID adicional`* pela ID do atributo que contém a mensagem adicional ou remova-a `additionalMessage` da carga.

```
{
  "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 as notificações por e-mail (`emailConfigurations`) para enviar a um usuário do Centro de identidade do IAM quando o alarme mudar de estado.

- Substitua a *`identidade StoreId AttributeId`* pela ID da propriedade do atributo ID do repositório de identidades do IAM Identity Center.
- Substitua o *`IdAttributeID do usuário`* pelo ID da propriedade do atributo ID do usuário do IAM Identity Center.
- Substitua *`from AddressAttribute Id`* pela ID da propriedade do atributo de endereço “`from`from” ou remova da carga útil.
- Substitua a *`SubjectAttributeID`* do e-mail pela ID da propriedade do atributo do assunto do e-mail ou remova `subject` da carga.
- Substitua a *`MessageAttributeID adicional`* pela ID da propriedade adicional do atributo da mensagem ou remova `additionalMessage` da carga.

```
{
  "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) Adicione as funcionalidades de alarme (`alarmCapabilities`) à carga útil em `alarm-model-payload.json`. Nesse objeto, você pode especificar se o fluxo de reconhecimento está habilitado e o estado de habilitação padrão para ativos com base no modelo do ativo. Para obter mais informações sobre o fluxo de reconhecimento, consulte Estados de alarme.

```
{
  "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. Adicione a função de serviço do IAM (`roleArn`) que AWS IoT Events pode assumir o envio de dados para AWS IoT SiteWise. Esse perfil requer a permissão `iotsitewise:BatchPutAssetPropertyValue` e um relacionamento de confiança que permita que `iotevents.amazonaws.com` assuma o perfil. Para enviar notificações, esse perfil também requer as permissões `lambda:InvokeFunction` e `sso-directory:DescribeUser`. Para obter mais informações, consulte Perfis de serviço de alarme no Guia do desenvolvedor do AWS IoT Events .

- `roleArn`Substitua o pelo ARN da função que AWS IoT Events pode assumir para realizar essas ações.

```
{
  "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. Execute o comando a seguir para criar o modelo de AWS IoT Events alarme a partir da carga em`alarm-model-payload.json`.

```
aws iotevents create-alarm-model --cli-input-json file://alarm-model-
payload.json
```

j. A operação retorna uma resposta que inclui o ARN do modelo de alarme, `alarmModelArn` Copie esse ARN para configurar a definição de alarme em seu modelo de ativo na próxima etapa.

Etapa 3: Habilitando o fluxo de dados entre AWS IoT SiteWise e AWS IoT Events

Depois de criar os recursos necessários em AWS IoT SiteWise e AWS IoT Events, você pode ativar o fluxo de dados entre os recursos para ativar seu alarme. Nesta seção, você atualiza a definição de alarme no modelo de ativo para usar o modelo de alarme criado na etapa anterior.

Para habilitar o fluxo de dados entre AWS IoT SiteWise e AWS IoT Events (CLI)

- Defina o modelo de alarme como a fonte do alarme no modelo de ativo. Faça o seguinte:

  a. Execute o seguinte comando para recuperar a definição do modelo de ativo existente. Substitua *`asset-model-id`* pela ID do modelo de ativo.

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

  A operação retorna uma resposta que contém os detalhes do modelo de ativo.

  b. Crie um arquivo chamado `update-asset-model-payload.json` e copie a resposta do comando anterior no arquivo.

  c. Remova os seguintes pares de chave-valor do arquivo `update-asset-model-payload.json`:

  - `assetModelId`
  - `assetModelArn`
  - `assetModelCreationDate`

- `assetModelLastUpdateDate`
- `assetModelStatus`

d. Adicione a propriedade da fonte de alarme (`AWS/ALARM_SOURCE`) ao modelo de alarme composto que você definiu anteriormente. ModelArnSubstitua o *`alarme`* pelo ARN do modelo de alarme, que define o valor da propriedade da fonte do alarme.

```
{
  ...
  "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. Execute o seguinte comando para atualizar o modelo de ativo com a definição armazenada no arquivo `update-asset-model-payload.json`. Substitua *`asset-model-id`* pela ID do modelo de ativo.

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

Seu modelo de ativo agora define um alarme que detecta em AWS IoT Events. O alarme monitora a propriedade de destino em todos os ativos com base nesse modelo de ativo. Você pode configurar o alarme em cada ativo para personalizar propriedades como o limite ou o destinatário do Centro de identidade do IAM para cada ativo. Para ter mais informações, consulte Configurar alarmes em ativos.

Definir alarmes externos

Os alarmes externos contêm o estado de um alarme que você detecta fora do AWS IoT SiteWise.

Definir um alarme externo (console)

Você pode usar o AWS IoT SiteWise console para definir um alarme externo em um modelo de ativo existente. Para definir um alarme externo em um novo modelo de ativo, crie o modelo de ativo e execute essas etapas. Para ter mais informações, consulte Criar modelos de ativo.

Para definir um alarme em um modelo de ativo

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Modelos.
3. Escolha o modelo de ativo para o qual o alarme será definido.
4. Escolha a guia Definições de alarme.
5. Escolha Adicionar alarme.
6. Em Opções do tipo de alarme, escolha Alarme externo.
7. Insira um nome para o alarme.

8. (Opcional) Insira uma descrição do seu alarme.
9. Escolha Adicionar alarme.

Definir um alarme externo (CLI)

Você pode usar o AWS CLI para definir um alarme externo em um modelo de ativo novo ou existente.

Para adicionar um alarme externo a um modelo de ativo, você adiciona um modelo de alarme composto ao modelo de ativo. Um modelo de alarme composto especifica o tipo do `EXTERNAL` e não especifica uma propriedade da fonte de alarme. O exemplo de alarme composto a seguir define um alarme externo 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 obter mais informações sobre como adicionar um modelo composto a um modelo de ativo novo ou existente, consulte o seguinte:

- Criação de um modelo de ativo (AWS CLI)
- Atualizando um modelo de ativo ou componente (AWS CLI)

Depois de definir o alarme externo, você pode ingerir o estado do alarme nos ativos com base no modelo do ativo. Para ter mais informações, consulte Ingestão do estado de alarme externo.

Configurar alarmes em ativos

Depois de definir um AWS IoT Events alarme em um modelo de ativo, você pode configurar o alarme em cada ativo com base no modelo de ativo. Você pode editar o valor limite e as configurações de notificação do alarme. Cada um desses valores é um atributo no ativo, então você pode atualizar o valor padrão do atributo para configurar esses valores.

> **Note**
>
> Você pode configurar esses valores para AWS IoT Events alarmes, mas não para alarmes externos.

Tópicos

- Configurar um valor limite (console)
- Configurando um valor limite ()AWS CLI
- Definir configurações de notificação (console)
- Definir configurações de notificação (CLI)

Configurar um valor limite (console)

Você pode usar o AWS IoT SiteWise console para atualizar o valor do atributo que especifica o valor limite de um alarme.

Para atualizar o valor limite de um alarme (console)

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Ativos.

3. Escolha o ativo para o qual você deseja atualizar um valor limite de alarme.

> **Tip**
>
> Você pode escolher o ícone de seta para expandir uma hierarquia de ativos para localizar seu ativo.

4. Selecione a opção Editar.
5. Encontre o atributo que o alarme usa para seu valor limite e, então, insira seu novo valor.
6. Escolha Salvar.

Configurando um valor limite ()AWS CLI

Você pode usar o AWS Command Line Interface (AWS CLI) para atualizar o valor do atributo que especifica o valor limite de um alarme.

Para executar este procedimento, é necessário saber quais são o `assetId` do ativo e o `propertyId` da propriedade. Você também pode usar o ID externo. Se você criou um ativo e não o conhece`assetId`, use a ListAssetsAPI para listar todos os ativos de um modelo específico. Use a DescribeAssetoperação para visualizar as propriedades do seu ativo, incluindo IDs de propriedade.

Use a operação BatchPutAssetPropertyValue para atribuir valores de atributos ao seu ativo. É possível usar essa operação para definir vários atributos de uma vez. A carga útil dessa operação contém uma lista de entradas, e cada entrada contém a ID do ativo, a ID da propriedade e o valor do atributo.

Para atualizar o valor de um atributo (AWS CLI)

1. Crie um arquivo chamado `batch-put-payload.json` e copie o seguinte objeto JSON no arquivo. Este exemplo de carga útil demonstra como definir a latitude e a longitude de uma turbina eólica. Atualize as IDs, os valores e as funções de horas para modificar a carga útil do 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 na carga contém um `entryId` que você pode definir como qualquer string exclusiva. Se qualquer entrada de solicitação falhar, cada erro conterá o `entryId` da solicitação correspondente, para que você saiba quais solicitações tentar novamente.
- Para definir um valor de atributo, você pode incluir uma estrutura timestamp-quality-value (TQV) na lista de `propertyValues` para cada propriedade de atributo. Essa estrutura deve conter o novo `value` e o `timestamp` atual.
  - `value` – uma estrutura contendo um dos valores a seguir, a depender do tipo de propriedade sendo definida:
    - `booleanValue`
    - `doubleValue`
    - `integerValue`

- `stringValue`

- `timestamp`— Uma estrutura que contém o tempo atual da época do Unix em segundos,. `timeInSeconds` AWS IoT SiteWise rejeita todos os pontos de dados com carimbos de data/hora que existiam há mais de 7 dias ou menos de 5 minutos no futuro.

Para obter mais informações sobre como preparar uma carga para BatchPutAssetPropertyValue, consulteIngestão de dados usando a API AWS IoT SiteWise.

2. Execute o comando a seguir para enviar os valores dos atributos para AWS IoT SiteWise:

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

Definir configurações de notificação (console)

Você pode usar o AWS IoT SiteWise console para atualizar o valor dos atributos que especificam as configurações de notificação para um alarme.

Para atualizar as configurações de notificação de um alarme (console)

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Ativos.
3. Escolha o ativo para o qual você deseja atualizar as configurações do alarme.
4. Selecione a opção Editar.
5. Encontre o atributo que o alarme usa para a configuração de notificação que você quer alterar e, em seguida, insira seu novo valor.
6. Escolha Salvar.

Definir configurações de notificação (CLI)

Você pode usar o AWS Command Line Interface (AWS CLI) para atualizar o valor do atributo que especifica as configurações de notificação para um alarme.

Para executar este procedimento, é necessário saber quais são o `assetId` do ativo e o `propertyId` da propriedade. Você também pode usar o ID externo. Se você criou um ativo e não

o conheceassetId, use a ListAssetsAPI para listar todos os ativos de um modelo específico. Use a DescribeAssetoperação para visualizar as propriedades do seu ativo, incluindo IDs de propriedade.

Use a operação BatchPutAssetPropertyValue para atribuir valores de atributos ao seu ativo. É possível usar essa operação para definir vários atributos de uma vez. A carga útil dessa operação contém uma lista de entradas, e cada entrada contém a ID do ativo, a ID da propriedade e o valor do atributo.

Para atualizar o valor de um atributo (AWS CLI)

1. Crie um arquivo chamado `batch-put-payload.json` e copie o seguinte objeto JSON no arquivo. Este exemplo de carga útil demonstra como definir a latitude e a longitude de uma turbina eólica. Atualize as IDs, os valores e as funções de horas para modificar a carga útil do 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 na carga contém um `entryId` que você pode definir como qualquer string exclusiva. Se qualquer entrada de solicitação falhar, cada erro conterá o `entryId` da solicitação correspondente, para que você saiba quais solicitações tentar novamente.
- Para definir um valor de atributo, você pode incluir uma estrutura timestamp-quality-value (TQV) na lista de `propertyValues` para cada propriedade de atributo. Essa estrutura deve conter o novo `value` e o `timestamp` atual.
  - `value` – uma estrutura contendo um dos valores a seguir, a depender do tipo de propriedade sendo definida:
    - `booleanValue`
    - `doubleValue`
    - `integerValue`
    - `stringValue`
  - `timestamp`— Uma estrutura que contém o tempo atual da época do Unix em segundos,. `timeInSeconds` AWS IoT SiteWise rejeita todos os pontos de dados com carimbos de data/hora que existiam há mais de 7 dias ou menos de 5 minutos no futuro.

Para obter mais informações sobre como preparar uma carga para BatchPutAssetPropertyValue, consulteIngestão de dados usando a API AWS IoT SiteWise.

2. Execute o comando a seguir para enviar os valores dos atributos para AWS IoT SiteWise:

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

Responder a alarmes

Quando um AWS IoT Events alarme muda de estado, você pode fazer o seguinte para responder ao alarme:

- Reconheça um alarme para indicar que você está lidando com o problema.
- Adie um alarme para desabilitá-lo temporariamente.
- Desabilite um alarme para desabilitá-lo permanentemente até que você o habilite novamente.
- Habilite um alarme desabilitado para detectar o estado do alarme.
- Reconfigure um alarme para limpar seu estado e o valor mais recente.

Você pode usar o AWS IoT SiteWise console ou a AWS IoT Events API para responder a um alarme.

> **Note**
>
> Você pode responder aos AWS IoT Events alarmes, mas não aos alarmes externos.

Tópicos

Responder a um alarme (console)

Você pode usar o AWS IoT SiteWise console para reconhecer, adiar, desativar ou ativar um alarme.

Tópicos

Reconhecer um alarme (console)

Você pode reconhecer um alarme para indicar que está lidando com o problema.

> **Note**
>
> Você deve habilitar o fluxo de reconhecimento no alarme para poder reconhecer o alarme. Essa opção é habilitada por padrão se você definir o alarme no console do AWS IoT SiteWise .

Para reconhecer um alarme (console)

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Ativos.
3. Escolha o ativo para o qual deseja reconhecer um alarme.

   > **Tip**
   >
   > Você pode escolher o ícone de seta para expandir uma hierarquia de ativos para localizar seu ativo.

4. Escolha a guia Alarmes.
5. Selecione o alarme a ser reconhecido e, em seguida, escolha Ações para abrir o menu de ação de resposta.
6. Escolha Reconhecer. O estado do alarme muda para Confirmado.

Adiar um alarme (console)

Você pode adiar um alarme para desabilitá-lo temporariamente. Especifique o período de adiamento do alarme.

Para adiar um alarme (console)

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Ativos.
3. Escolha o ativo para o qual deseja adiar um alarme.

> **Tip**
>
> Você pode escolher o ícone de seta para expandir uma hierarquia de ativos para localizar seu ativo.

4. Escolha a guia Alarmes.
5. Selecione o alarme a adiar e, depois, escolha Ações para abrir o menu de ação de resposta.
6. Escolha Adiar. Um modelo é aberto onde você especifica a duração do adiamento.
7. Escolha a Duração do adiamento ou insira uma Duração de adiamento personalizada.
8. Escolha Salvar. O estado do alarme muda para Adiado.

Desabilitar um alarme (console)

Você pode desabilitar um alarme para que ele não detecte mais. Depois de desabilitar o alarme, você deve habilitá-lo novamente se quiser que o alarme detecte.

Para desabilitar um alarme (console)

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Ativos.
3. Escolha o ativo para o qual deseja desabilitar um alarme.

> **Tip**
>
> Você pode escolher o ícone de seta para expandir uma hierarquia de ativos para localizar seu ativo.

4. Escolha a guia Alarmes.
5. Selecione o alarme a ser desabilitado e, em seguida, escolha Ações para abrir o menu de ação de resposta.
6. Escolha Desabilitar. O estado do alarme muda para Desabilitado.

Habilitar um alarme (console)

Você pode habilitar um alarme detectar novamente depois de desabilitá-lo ou adiá-lo.

Para habilitar um alarme (console)

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Ativos.
3. Escolha o ativo para o qual deseja habilitar um alarme.

> **Tip**
>
> Você pode escolher o ícone de seta para expandir uma hierarquia de ativos para localizar seu ativo.

4. Escolha a guia Alarmes.
5. Selecione o alarme a ser habilitado e, em seguida, escolha Ações para abrir o menu de ação de resposta.
6. Escolha Habilitar. O estado do alarme muda para Normal.

Reconfigurar um alarme (console)

Você pode reconfigurar um alarme para limpar seu estado e o valor mais recente.

Para reconfigurar um alarme (console)

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Ativos.
3. Escolha o ativo para o qual deseja reconfigurar um alarme.

> **Tip**
>
> Você pode escolher o ícone de seta para expandir uma hierarquia de ativos para localizar seu ativo.

4. Escolha a guia Alarmes.
5. Selecione o alarme a ser habilitado e, em seguida, escolha Ações para abrir o menu de ação de resposta.
6. Escolha Redefinir. O estado do alarme muda para Normal.

Responder a um alarme (API)

Você pode usar a AWS IoT Events API para reconhecer, adiar, desativar, ativar ou redefinir um alarme. Para obter mais informações, consulte as seguintes operações em Referência de API do AWS IoT Events :

- BatchAcknowledgeAlarme
- BatchSnoozeAlarme
- BatchDisableAlarme
- BatchEnableAlarme
- BatchResetAlarme

Para obter mais informações, consulte Responder a alarmes, no Guia do desenvolvedor do AWS IoT Events .

Ingestão do estado de alarme externo

Alarmes externos são alarmes que você avalia externamente. AWS IoT SiteWise Você pode usar alarmes externos quando você tem uma fonte de dados que relata o estado do alarme que você deseja ingerir em AWS IoT SiteWise.

As propriedades do estado do alarme exigem um formato específico para os valores dos dados do estado do alarme. Cada valor de dados deve ser um objeto JSON serializado em uma string. Então, você ingere a string serializada como um valor de string. Para ter mais informações, consulte Propriedades do estado do alarme.

Example Exemplo de valor de dados do estado do alarme (não serializado)

```
{
  "stateName": "Active"
}
```

Example Exemplo de valor de dados do estado do alarme (serializado)

```
{\"stateName\":\"Active\"}
```

> **Note**
>
> Se sua fonte de dados não puder relatar dados nesse formato ou você não puder converter seus dados nesse formato antes de ingeri-los, você pode optar por não usar uma propriedade de alarme. Em vez disso, você pode ingerir os dados como uma propriedade de medição com o tipo de dados de string, por exemplo. Para obter mais informações, consulte Definindo fluxos de dados do equipamento (medições) e Ingestão de dados para AWS IoT SiteWise.

Mapear fluxos externos de estado de alarme

Você pode definir aliases de propriedades para mapear seus fluxos de dados para suas propriedades de estado de alarme. Isso ajuda você a identificar facilmente uma propriedade do estado de alarme ao ingerir ou recuperar dados. Para obter mais informações sobre propriedade de aliases, consulte Mapeamento de fluxos de dados industriais para propriedades de ativos.

Tópicos

- Mapear fluxos externos de estado de alarme (console)
- Mapeando fluxos externos de estado de alarme ()AWS CLI

Mapear fluxos externos de estado de alarme (console)

Você pode definir aliases de propriedades para mapear seus fluxos de dados para suas propriedades de estado de alarme. Isso ajuda você a identificar facilmente uma propriedade do estado de alarme ao ingerir ou recuperar dados. Para obter mais informações sobre propriedade de aliases, consulte Mapeamento de fluxos de dados industriais para propriedades de ativos.

Você pode usar o AWS IoT SiteWise console para definir um alias para uma propriedade de estado de alarme.

Para definir um alias de propriedade para uma propriedade de estado de alarme (console)

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Ativos.
3. Escolha o ativo para o qual deseja definir um apelido de propriedade.

> **Tip**
>
> Você pode escolher o ícone de seta para expandir uma hierarquia de ativos para localizar seu ativo.

4. Selecione a opção Editar.
5. Vá até Alarmes e expanda a seção.
6. Em Alarmes externos, insira o alias em Alias da propriedade — opcional.
7. Selecione Save (Salvar).

Mapeando fluxos externos de estado de alarme ()AWS CLI

Você pode definir aliases de propriedades para mapear seus fluxos de dados para suas propriedades de estado de alarme. Isso ajuda você a identificar facilmente uma propriedade do estado de alarme ao ingerir ou recuperar dados. Para obter mais informações sobre propriedade de aliases, consulte Mapeamento de fluxos de dados industriais para propriedades de ativos.

Você pode usar o AWS Command Line Interface (AWS CLI) para definir um alias para uma propriedade de estado de alarme.

Para executar este procedimento, é necessário saber quais são o `assetId` do ativo e o `propertyId` da propriedade. Você também pode usar o ID externo. Se você criou um ativo e não o conhece`assetId`, use a ListAssetsAPI para listar todos os ativos de um modelo específico. Use a DescribeAssetoperação para visualizar as propriedades do seu ativo, incluindo IDs de propriedade.

> **Note**
>
> A DescribeAssetresposta inclui a lista de modelos de ativos compostos para o ativo. Cada alarme é um modelo composto. Para encontrar o `propertyId`, encontre o modelo composto para o alarme e, em seguida, encontre a propriedade do `AWS/ALARM_STATE` nesse modelo composto.

Para obter informações sobre como definir a o alias da propriedade, consulte Definindo um alias de propriedade ()AWS CLI.

Ingestão de dados do estado do alarme

As propriedades do estado do alarme esperam que o estado do alarme seja uma string JSON serializada. Para inserir o estado de alarme em um alarme externo AWS IoT SiteWise, você ingere essa string serializada como um valor de string com carimbo de data e hora. O exemplo a seguir demonstra um valor de dados de estado para um alarme ativo.

```
{\"stateName\":\"Active\"}
```

Para identificar uma propriedade de estado de alarme, você pode especificar um dos seguintes elementos:

- O `assetId` e `propertyId` da propriedade do alarme para o qual você está enviando dados.
- O `propertyAlias`, que é um alias de fluxo de dados (por exemplo, `/company/windfarm/3/turbine/7/temperature/high`). Para usar esta opção, primeiro você deve definir o alias da propriedade do seu alarme. Para saber como definir aliases de propriedades para propriedades de estado do alarme, consulte Mapear fluxos externos de estado de alarme.

O exemplo de carga útil da BatchPutAssetPropertyValue API a seguir demonstra como formatar o estado de um alarme externo. Esse alarme externo relata quando a leitura de rotações por minuto (RPM) de uma turbina eólica está muito alta.

Example Exemplo de BatchPutAssetPropertyValue carga útil para dados de estado de alarme

```
{
    "entries": [
      {
        "entryId": "unique entry ID",
        "propertyAlias": "/company/windfarm/3/turbine/7/temperature/high",
        "propertyValues": [
          {
            "value": {
              "stringValue": "{\"stateName\":\"Active\"}"
            },
            "timestamp": {
              "timeInSeconds": 1607550262
            }
          }
        ]
      }
```

```
    ]
  }
```

Para obter mais informações sobre como usar a API `BatchPutAssetPropertyValue` para ingerir dados, consulte Ingestão de dados usando a API AWS IoT SiteWise.

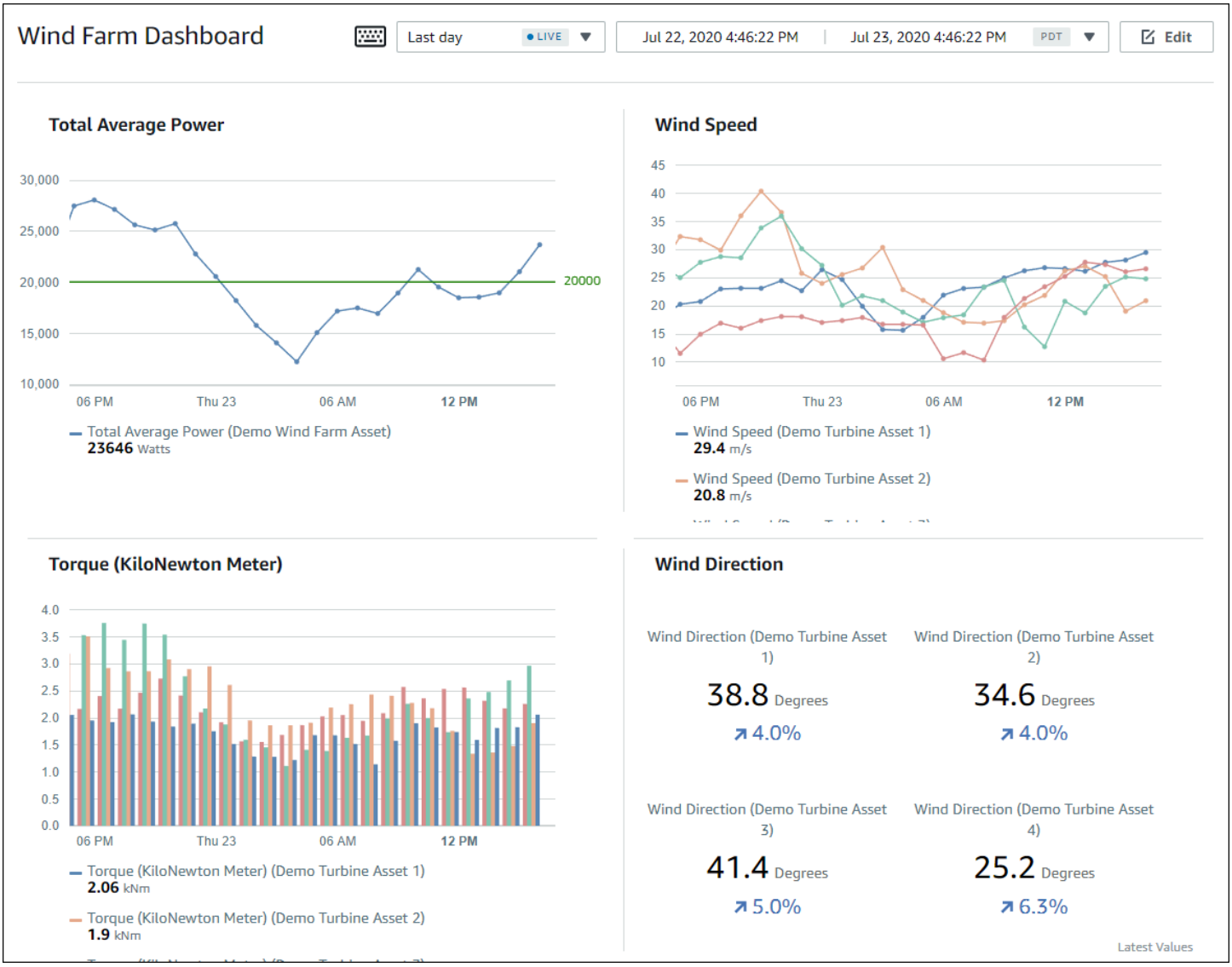
Para obter mais informações outras formas de ingerir dados, consulte Ingestão de dados para AWS IoT SiteWise.

Monitorando dados com AWS IoT SiteWise Monitor

Você pode usar AWS IoT SiteWise para monitorar os dados de seus processos, dispositivos e equipamentos criando portais web SiteWise Monitor. SiteWise O Monitor é um recurso AWS IoT SiteWise que você pode usar para criar portais na forma de um aplicativo web gerenciado. Depois, você poderá usar esses portais para visualizar e compartilhar os dados operacionais. É possível criar projetos com painéis para visualizar dados de seus processos, dispositivos e equipamentos conectados à AWS IoT.

Especialistas em domínio, como engenheiros de processo, podem usar esses portais para obter insights sobre seus dados operacionais rapidamente, entender o comportamento do dispositivo e do equipamento.

O exemplo de painel a seguir exibe dados de um parque eólico.



Como AWS IoT SiteWise captura dados ao longo do tempo, você pode usar o SiteWise Monitor para visualizar dados operacionais ao longo do tempo ou os últimos valores relatados em momentos específicos. Isso permite descobrir insights que poderiam ser difíceis de encontrar.

SiteWise Monitore as funções

Quatro funções interagem com o SiteWise Monitor:

AWS administrador

O AWS administrador usa o AWS IoT SiteWise console para criar portais. O administrador da AWS também pode atribuir administradores do portal e adicionar usuários do portal.

Posteriormente, os administradores do portal atribuem usuários do portal aos projetos como proprietários ou visualizadores. O AWS administrador trabalha exclusivamente no AWS console.

Administrador de portal

Cada portal do SiteWise Monitor tem um ou mais administradores do portal. Os administradores de portal usam-no para criar projetos que contenham coleções de ativos e painéis. Em seguida, o administrador de portal atribui ativos e proprietários a cada projeto. Ao controlar o acesso ao projeto, administradores do portal especificam quais ativos os proprietários e visualizadores do projeto podem ver.

Proprietário de projeto

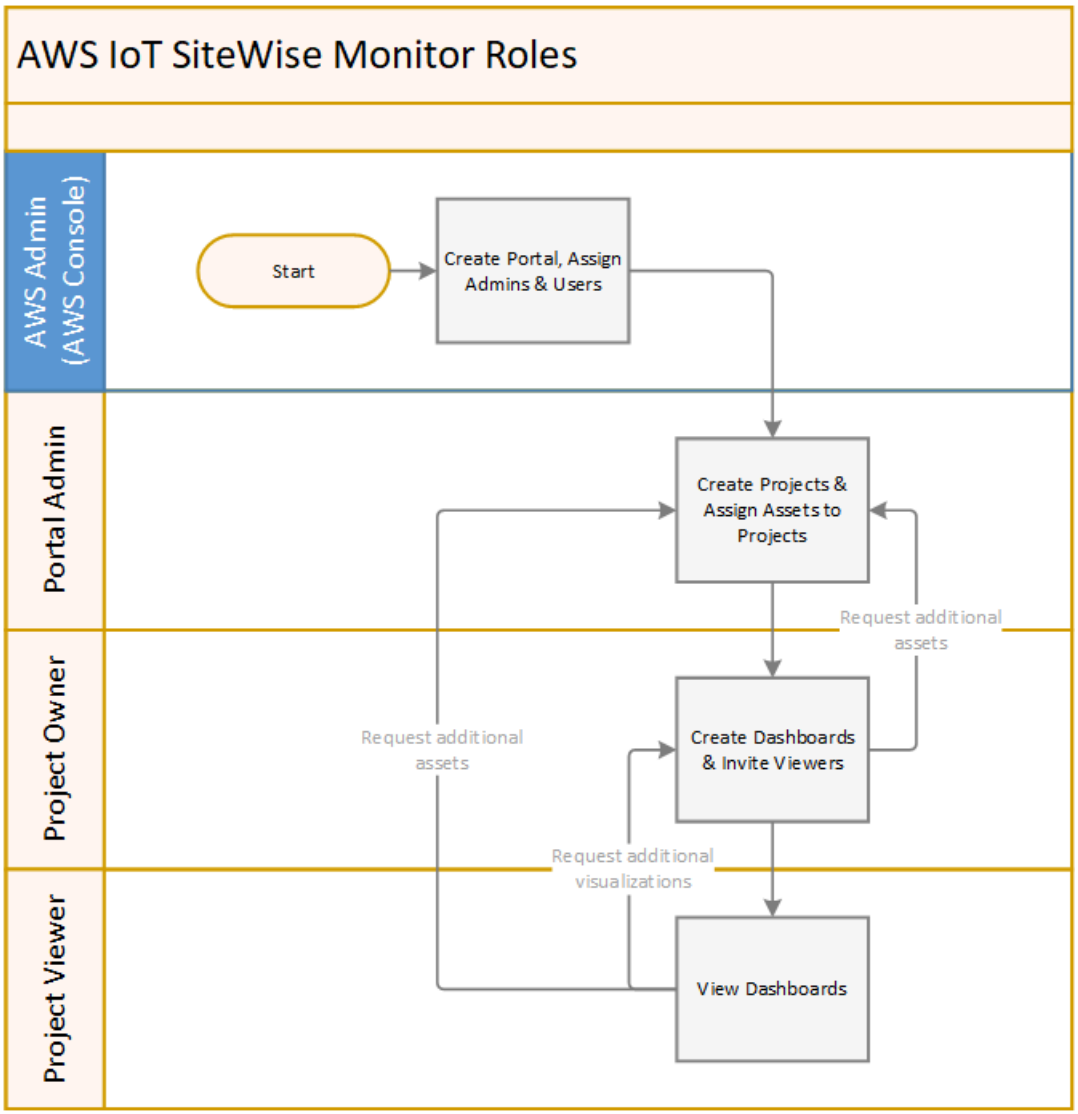
Cada projeto do SiteWise Monitor tem proprietários. Proprietários de projeto criam visualizações na forma de painéis para representar dados operacionais de forma consistente. Quando os painéis estiverem prontos para compartilhar, o proprietário de projeto pode convidar visualizadores. Os proprietários de projeto também podem atribuir outros proprietários a ele. Os proprietários do projeto podem definir limites e configurações de notificação para alarmes.

Visualizador de projeto

Cada projeto do SiteWise Monitor tem espectadores. Os visualizadores do projeto podem conectar-se ao portal para visualizar os painéis criados pelos proprietários do projeto. Em cada painel, os visualizadores do projeto podem ajustar os prazos para entender melhor os dados operacionais. Os visualizadores do projeto só podem visualizar painéis nos projetos aos quais tiverem acesso. Os visualizadores do projeto podem reconhecer e adiar os alarmes.

A depender da sua organização, a mesma pessoa pode desempenhar várias funções.

A imagem a seguir ilustra como essas quatro funções interagem no portal SiteWise Monitor.



É possível gerenciar quem tem acesso aos dados usando o AWS IAM Identity Center ou IAM. Seus usuários de dados podem fazer login no SiteWise Monitor a partir de um navegador de desktop ou celular usando suas credenciais do IAM Identity Center ou do IAM.

Federação do SAML

O Centro de Identidade do IAM e o IAM são compatíveis com federação de identidades com SAML (Security Assertion Markup Language) 2.0. O SAML 2.0 é um padrão aberto que muitos provedores de identidade externos (IdPs) usam para autenticar usuários e passar suas informações de identidade e segurança aos provedores de serviços (SPs). Normalmente, os SPs são aplicativos ou serviços. A federação SAML permite que os administradores e usuários do portal SiteWise Monitor entrem nos portais atribuídos com credenciais externas, como nomes de usuário e senhas corporativos.

Você pode configurar o IAM Identity Center e o IAM para usar a federação baseada em SAML para acessar seus portais do SiteWise Monitor.

IAM Identity Center

Seus administradores e usuários do portal podem entrar no portal de AWS acesso com seus nomes de usuário e senhas corporativos. Eles podem então navegar até os portais de SiteWise monitoramento atribuídos. O IAM Identity Center usa certificados para configurar uma relação de confiança SAML entre seu provedor de identidade e. AWS Para obter mais informações, consulte o perfil SCIM e implementação do SAML 2.0 no Guia do usuário do AWS IAM Identity Center .

IAM

Seus administradores e usuários do portal podem solicitar credenciais de segurança temporárias para acessar seus portais SiteWise Monitor atribuídos. Você cria uma identidade de provedor de identidade SAML no IAM para configurar uma relação de confiança entre seu provedor de identidade e. AWS Para obter mais informações, consulte Como usar a federação baseada em SAML para acesso à API AWS, no Guia do usuário do IAM.

Seus administradores e usuários do portal podem entrar no portal da sua empresa e selecionar a opção de ir para o console AWS de gerenciamento. Eles podem então navegar até os portais de SiteWise monitoramento atribuídos. O portal da sua empresa lida com a troca de confiança entre seu provedor de identidade AWS e. Para obter mais informações, consulte Como permitir que usuários federados do SAML 2.0 acessem o AWS Management Console no Guia do usuário do IAM.

> **Note**
>
> Ao adicionar usuários ou administradores ao portal, evite criar políticas do IAM que restrinjam as permissões do usuário, como IP limitado. Quaisquer políticas anexadas com permissões restritas não poderão se conectar ao AWS IoT SiteWise portal.

SiteWise Conceitos de monitoramento

Para usar o SiteWise Monitor, você deve estar familiarizado com os seguintes conceitos:

Portal

Um AWS IoT SiteWise Monitor portal é um aplicativo da web que você pode usar para visualizar e compartilhar seus AWS IoT SiteWise dados. Um portal tem um ou mais administradores e contém zero ou mais projetos.

Projeto

Cada portal do SiteWise Monitor contém um conjunto de projetos. Cada projeto tem uma subconjunto dos seus ativos AWS IoT SiteWise associado a ele. Os proprietários do projeto criam um ou mais painéis para fornecer uma maneira consistente de visualização dos dados associados a esses ativos. Os proprietários do projeto podem convidar visualizadores para o projeto, a fim de permitir que eles visualizem os ativos e os painéis no projeto. O projeto é a unidade básica de compartilhamento dentro do SiteWise Monitor. Os proprietários do projeto podem convidar usuários que receberam acesso ao portal pelo AWS administrador. Um usuário deve ter acesso a um portal antes que um projeto desse portal possa ser compartilhado com esse usuário.

Ativo

Quando os dados AWS IoT SiteWise do seu equipamento industrial são ingeridos, seus dispositivos, equipamentos e processos são representados como ativos. Cada ativo tem propriedades e alarmes associados a ele. O administrador do portal atribui conjuntos de ativos a cada projeto.

Propriedade

As propriedades são dados de séries temporais associados aos ativos. Por exemplo, uma peça de equipamento pode ter um número de série, um local, uma marca, um modelo e uma data de instalação. Ela também pode ter valores de séries temporais para disponibilidade, desempenho, qualidade, temperatura, pressão e assim por diante.

Alarme

Os alarmes monitoram as propriedades para identificar quando o equipamento está fora de sua faixa operacional. Cada alarme define um limite e uma propriedade a ser monitorada. Quando a propriedade excede o limite, o alarme fica ativo e indica que você ou alguém da sua equipe deve resolver o problema. Os proprietários do projeto podem personalizar os limites e configurações de notificação para alarmes. Os espectadores do projeto podem reconhecer e adiar os alarmes, além de deixar uma mensagem com detalhes sobre o alarme ou a ação realizada para resolvê-lo.

Painel

Cada projeto contém um conjunto de painéis. Os painéis fornecem um conjunto de visualizações para os valores de um de ativos. Os proprietários do projeto criam os painéis e as visualizações contidas neles. Quando um proprietário de projeto está pronto para compartilhar o conjunto de painéis, o proprietário pode convidar visualizadores para o projeto e lhes conceder acesso a todos os painéis do projeto. Se você quiser um conjunto de visualizadores diferente para painéis diferentes, será necessário dividir os painéis entre projetos. Quando visualizam os painéis, os espectadores podem personalizar o intervalo de tempo para analisar dados específicos.

Visualização

Em cada painel, os proprietários de projeto decidem como exibir as propriedades e alarmes dos ativos associados ao projeto. A disponibilidade pode ser representada como um gráfico de linhas, enquanto outros valores podem ser exibidos como gráficos de barras ou como indicadores-chave de desempenho (KPIs). Os alarmes são melhor exibidos como grades de status e cronogramas de status. Os proprietário do projeto personalizam cada visualização para fornecer a melhor compreensão sobre os dados desse ativo.

Começando com AWS IoT SiteWise Monitor

Se você for o AWS administrador da sua organização, crie portais a partir do AWS IoT SiteWise console. Conclua as etapas a seguir para criar um portal para que os membros da sua organização possam visualizar seus AWS IoT SiteWise dados:

1. Configurar e criar um portal
2. Adicionar administradores do portal e enviar e-mails de convite
3. Adicionar usuários ao portal

Depois de criar um portal, o administrador do portal pode visualizar seus AWS IoT SiteWise ativos e atribuí-los aos projetos no portal. Os proprietários do projeto poderão então criar painéis para visualizar as propriedades dos ativos que ajudam os visualizadores do projeto a entender como seus dispositivos, processos e equipamentos estão funcionando.

> **Note**
>
> Ao adicionar usuários ou administradores ao portal, evite criar políticas AWS Identity and Access Management (IAM) que restrinjam as permissões do usuário, como IP limitado.

Quaisquer políticas anexadas com permissões restritas não poderão se conectar ao AWS IoT SiteWise portal.

Você pode seguir um tutorial que aborda as etapas necessárias para configurar um portal com um projeto, painéis e vários usuários para um cenário específico usando dados de um parque de energia eólica. Para ter mais informações, consulte Visualizando e compartilhando dados de parques eólicos no Monitor SiteWise .

Tópicos

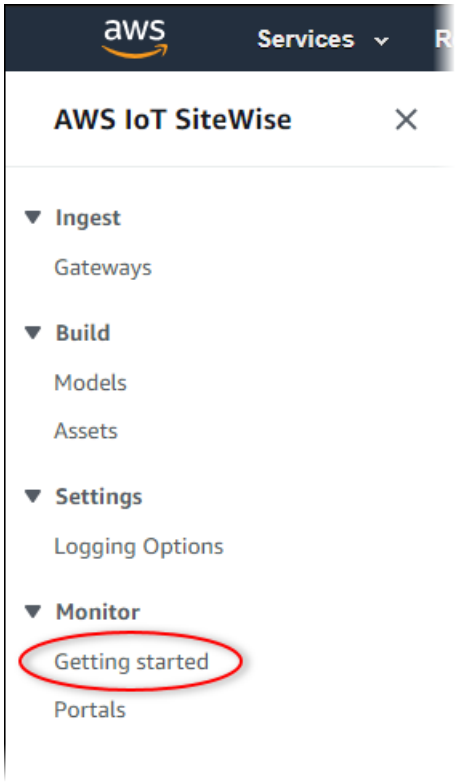
- Criar um portal
- Configurar seu portal
- Convidar administradores
- Adicionar usuários ao portal

Criar um portal

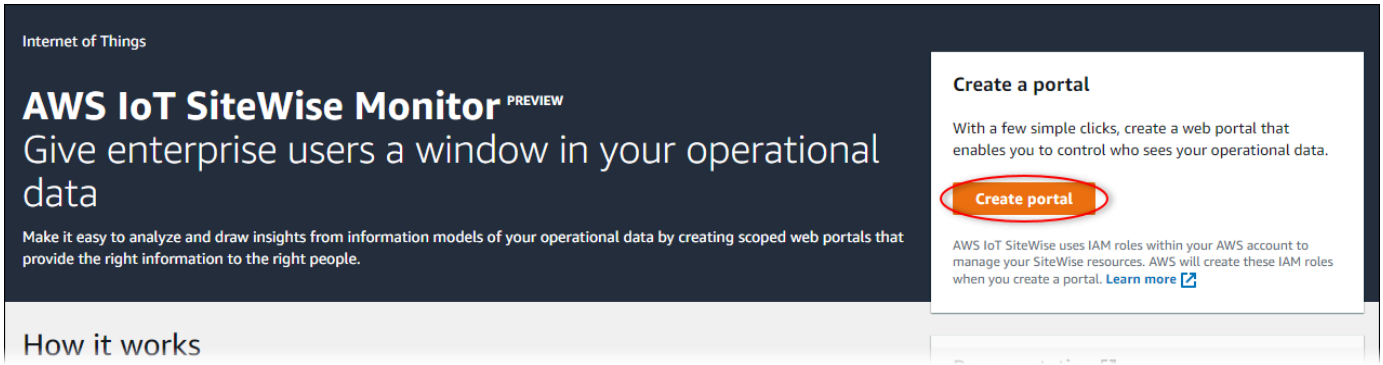
Você cria um portal SiteWise Monitor no AWS IoT SiteWise console.

Como criar um portal

1. Faça login no AWS IoT SiteWise console.
2. No painel de navegação, escolha Monitor, Conceitos básicos.



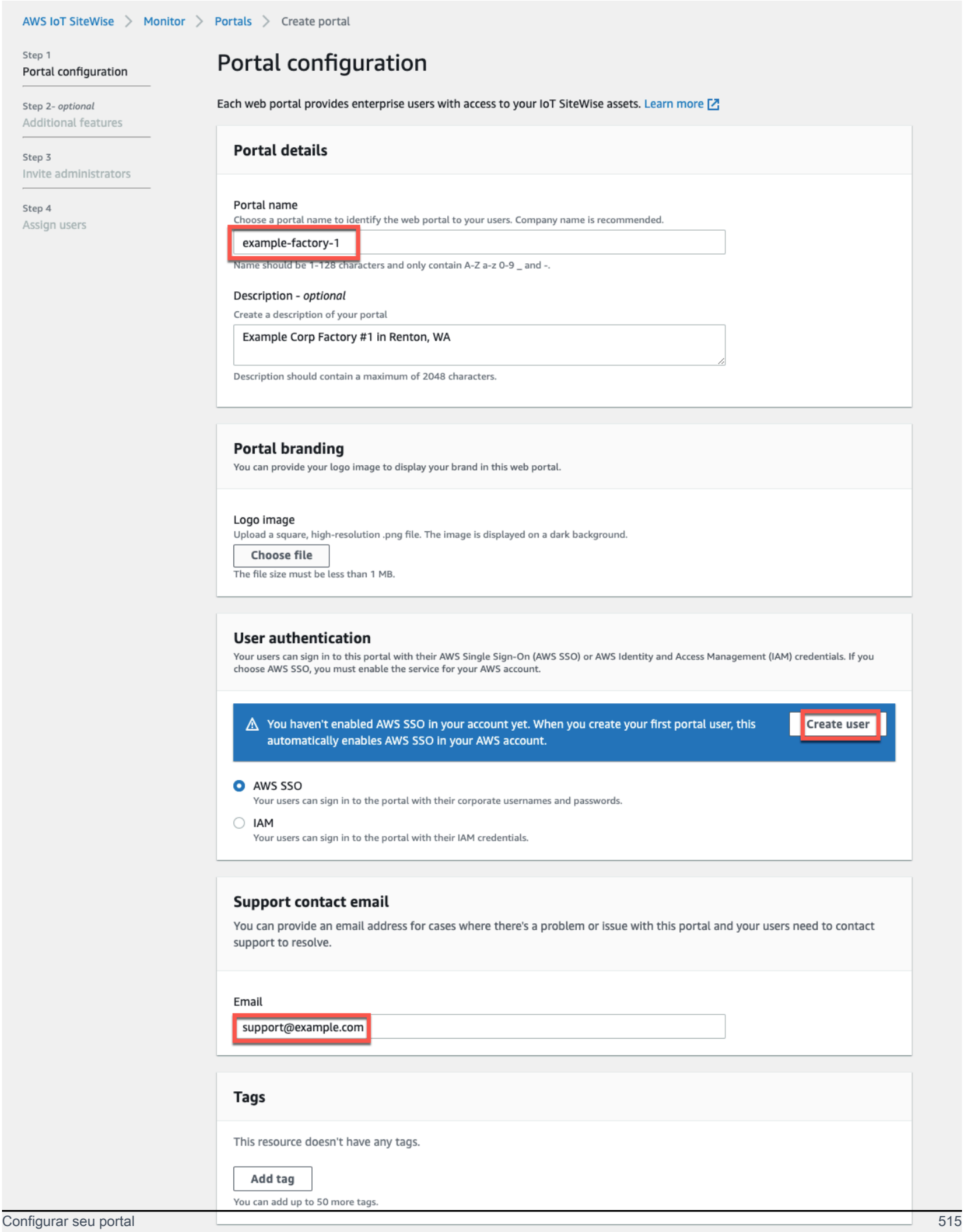
3. Escolha Criar Portal.



Depois, forneça algumas informações básicas para configurar o portal.

Configurar seu portal

Os usuários usam portais para visualizar seus dados. Você pode personalizar o nome, a descrição, a marca, a autenticação de usuário, o e-mail do contato de suporte e as permissões de um 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

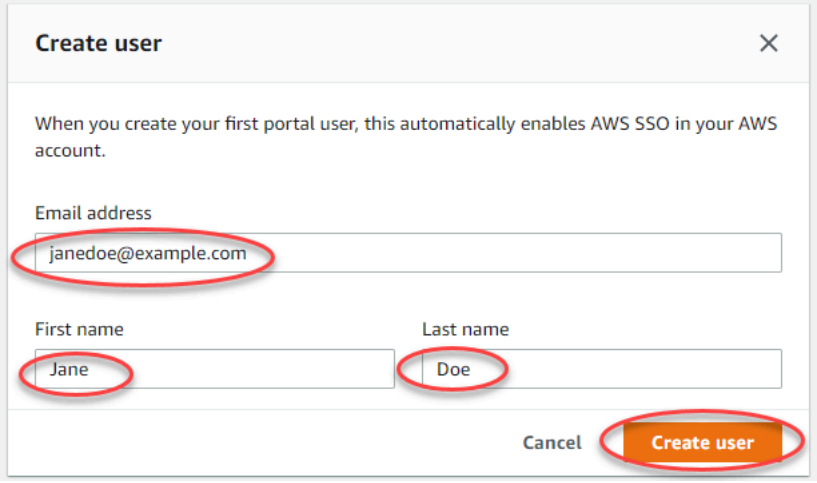
Como configurar um portal

1. Insira um nome para o portal.
2. (Opcional) Insira uma descrição para o portal. Se você tiver vários portais, use descrições significativas para ajudar a controlar o que cada portal contém.
3. (Opcional) Faça upload de uma imagem para exibir sua marca no portal. Escolha uma imagem quadrada no formato PNG. Se você fizer upload de uma imagem que não é quadrada, o portal reduzirá a imagem a um quadrado.
4. Escolha uma das seguintes opções:
   - Escolha Centro de identidade do IAM se os usuários do portal entrarem neste portal com seus nomes de usuário e senhas corporativas.

     Se você não habilitou o Centro de identidade do IAM em sua conta, faça o seguinte:

     a. Selecione Criar usuário.

     b. Na página Criar usuário, para criar o primeiro portal, insira o endereço de e-mail, nome e sobrenome do usuário e, então, escolha Criar usuário.



> **Note**
>
> - AWS ativa automaticamente o IAM Identity Center em sua conta quando você cria o primeiro usuário do portal.
> - Você pode configurar o Centro de identidade do IAM em apenas uma região de cada vez. SiteWise O Monitor se conecta à região que você configurou para o IAM Identity Center. Isso significa que você usa uma região para

acessar o Centro de identidade do IAM, mas pode criar portais em qualquer região.

- Escolha IAM se seus usuários do portal entrarem neste portal com as credenciais do IAM.

> **Important**
>
> Usuários ou perfis devem ter a permissão de `iotsitewise:DescribePortal` para entrar no portal.

5. Insira um endereço de e-mail que os usuários do portal possam contatar se tiverem um problema com o portal e precisarem de ajuda para solucioná-lo.
6. (Opcional) Adicione tags ao seu portal. Para ter mais informações, consulte Marcando seus recursos AWS IoT SiteWise.
7. Escolha uma das seguintes opções:
   - Escolha Criar e usar um novo perfil de serviço. Por padrão, o SiteWise Monitor cria automaticamente uma função de serviço para cada portal. Essa função permite que seus usuários do portal acessem seus AWS IoT SiteWise recursos. Para ter mais informações, consulte Usando funções de serviço para AWS IoT SiteWise Monitor.
   - Escolha Usar um perfil existente e escolha o perfil de serviço alvo.
8. Escolha Avançar
9. (Opcional) Habilitar alarmes para seu portal. Para ter mais informações, consulte Habilitar alarmes para seus portais.
10. Escolha Criar. AWS IoT SiteWise criará seu portal.

> **Note**
>
> Se fechar o console, você poderá concluir o processo de configuração adicionando administradores e usuários. Para ter mais informações, consulte Adicionar ou remover administradores do portal. Se não quiser manter o portal, exclua-o para que ele não use recursos. Para ter mais informações, consulte Excluir um portal.

A coluna de Status pode ser um dos valores a seguir:

- CREATING - AWS IoT SiteWise está processando sua solicitação para criar o portal. O processo pode demorar vários minutos para ser concluído.
- ATUALIZANDO - AWS IoT SiteWise está processando sua solicitação para atualizar o portal. O processo pode demorar vários minutos para ser concluído.
- PENDING - AWS IoT SiteWise está aguardando a conclusão da propagação do registro DNS. O processo pode demorar vários minutos para ser concluído. Você pode excluir o portal enquanto o status estiver PENDENTE.
- EXCLUIR - AWS IoT SiteWise está processando sua solicitação para excluir o portal. O processo pode demorar vários minutos para ser concluído.
- ATIVO: quando o portal se torna ativo, os usuários do portal podem acessá-lo.
- FALHOU - AWS IoT SiteWise não foi possível processar sua solicitação para criar, atualizar ou excluir o portal. Se você habilitou AWS IoT SiteWise o envio de registros para o Amazon CloudWatch Logs, você pode usar esses registros para solucionar problemas. Para obter mais informações, consulte Monitoramento AWS IoT SiteWise com CloudWatch registros.

Uma mensagem será exibida quando o portal for criado.

Depois, convide um ou mais administradores de portal para o portal. Até agora, você criou um portal, mas ninguém pode acessá-lo.

Convidar administradores

Para começar a usar seu novo portal, é necessário atribuir um administrador do portal. O administrador do portal cria projetos, escolhe proprietários de projetos e atribui ativos a projetos. Os administradores do portal podem ver todos os seus AWS IoT SiteWise ativos.

Com base no serviço de autenticação do usuário, selecione uma das opções a seguir:

IAM Identity Center

Se você estiver usando o SiteWise Monitor pela primeira vez, você pode escolher o usuário que você criou anteriormente para ser o administrador do portal. Se quiser adicionar outro usuário como administrador do portal, você pode criar um usuário do Centro de identidade do IAM a partir desta página. Como alternativa, é possível conectar um provedor de identidade externo ao Centro de identidade do IAM. Para mais informações, consulte o Guia do usuário do AWS IAM Identity Center.

Como convidar administradores

1. Marque as caixas de seleção para os usuários que você deseja como administradores do portal. Isso adiciona os usuários à lista de Administradores do Portal.

   > **Note**
   >
   > Se você usa o Centro de identidade do IAM como seu repositório de identidades e está conectado à sua conta de gerenciamento AWS Organizations , pode escolher Criar usuário para criar um usuário do Centro de identidade do IAM. O Centro de identidade do IAM envia ao novo usuário um e-mail para que ele defina sua senha. Você pode então atribuir o usuário ao portal como administrador. Para obter mais informações, consulte Gerenciar identidades no Centro de identidade do IAM.

2. (Opcional) Escolha Enviar convite para os usuários selecionados. Seu cliente de e-mail será aberto e um convite será colocado no corpo da mensagem.

   É possível personalizar o e-mail antes de enviá-lo para os administradores do portal. Também é possível enviar o e-mail para os administradores do portal mais tarde. Se você estiver testando o SiteWise Monitor pela primeira vez e adicionando seu novo usuário ou função do IAM Identity Center ou IAM como administrador do portal, você não precisa enviar um e-mail para si mesmo.
3. Se adicionar um usuário que não queira como administrador, desmarque a caixa de seleção desse usuário.
4. Quando terminar de convidar administradores do portal, escolha Próximo.

IAM

Você pode escolher um usuário para ser o administrador do portal. Se quiser adicionar outro usuário ou perfil como administrador do portal, você pode criar um usuário ou perfil no console do IAM. Para obter mais informações, consulte Criar um usuário do IAM na sua conta da AWS e Criar perfis do IAM no Guia do usuário do IAM.

Como convidar administradores

1. Faça o seguinte:

- Escolha usuários do IAM para adicionar um usuário do IAM como seu administrador do portal.
- Escolha perfis do IAM para adicionar um perfil do IAM como administrador do portal.

2. Marque as caixas de seleção para os usuários ou perfis que você deseja como administradores do portal. Isso adiciona os usuários ou perfis à lista de Administradores do Portal.
3. Se adicionar um usuário ou perfil que não queira como administrador, desmarque a caixa de seleção desse usuário ou perfil.
4. Quando terminar de convidar administradores do portal, escolha Próximo.

> **Important**
>
> Usuários ou perfis devem ter a permissão de `iotsitewise:DescribePortal` para entrar no portal.

> **Note**
>
> Se você usa o Centro de identidade do IAM como seu repositório de identidades e está conectado à sua conta de gerenciamento AWS Organizations , pode escolher Criar usuário para criar um usuário do Centro de identidade do IAM. O Centro de identidade do IAM envia ao novo usuário um e-mail para que ele defina sua senha. Você pode então atribuir o usuário ao portal como administrador. Para obter mais informações, consulte Gerenciar identidades no Centro de identidade do IAM.

É possível alterar a lista de administradores do portal posteriormente. Para ter mais informações, consulte Adicionar ou remover administradores do portal.

> **Note**
>
> Como somente um administrador de portal pode criar projetos e atribuir ativos a eles, é necessário especificar pelo menos um administrador do portal.

Como última etapa, adicione usuários que podem acessar o novo portal.

Adicionar usuários ao portal

Você controla quais usuários têm acesso aos portais. Em cada portal, os administradores do portal criam um ou mais projetos e atribuem usuários do portal como proprietários ou visualizadores para cada projeto. Cada proprietário do projeto pode convidar usuários adicionais do portal para serem proprietários ou visualizadores do projeto.

Com base no serviço de autenticação do usuário, selecione uma das opções a seguir:

IAM Identity Center

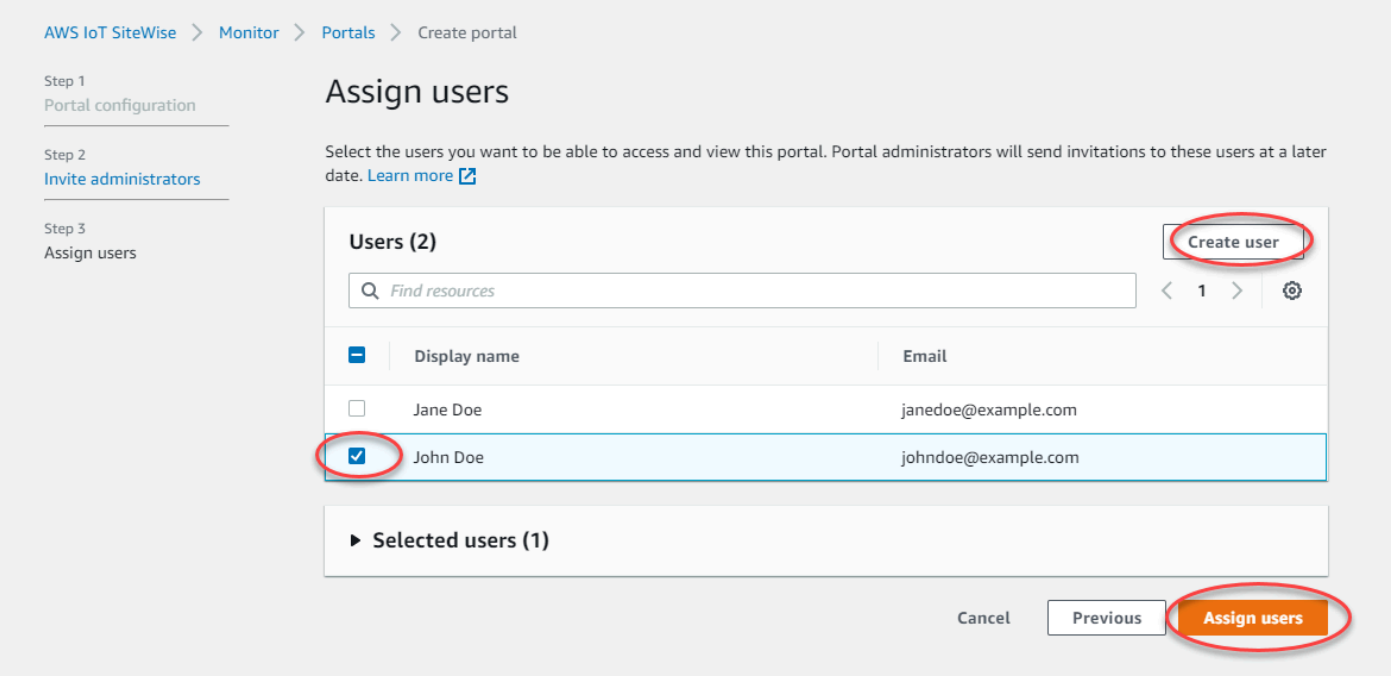
Caso queira adicionar um usuário à lista Usuários, execute as etapas a seguir.

Como adicionar usuários do portal

1. Escolha Atribuir usuários para adicionar esses usuários ao portal. Isso adiciona os usuários à lista de Usuários do portal. Se você estiver utilizando o SiteWise Monitor pela primeira vez, você não precisa adicionar seu administrador do portal como um usuário do portal.

   > **Note**
   >
   > Se você usa o Centro de identidade do IAM como seu repositório de identidades e está conectado à sua conta de gerenciamento AWS Organizations , pode escolher Criar usuário para criar um usuário do Centro de identidade do IAM. O Centro de identidade do IAM envia ao novo usuário um e-mail para que ele defina sua senha. Você pode então atribuir o usuário ao portal como usuário. Para obter mais informações, consulte Gerenciar identidades no Centro de identidade do IAM.

2. Se você adicionar um usuário que não quer que tenha acesso ao portal, desmarque a caixa de seleção desse usuário.
3. Quando terminar de selecionar os usuários, escolha Compartilhar.



IAM

Caso veja o usuário ou perfil que deseja adicionar à lista usuários do IAM ou perfis do IAM, execute as etapas a seguir.

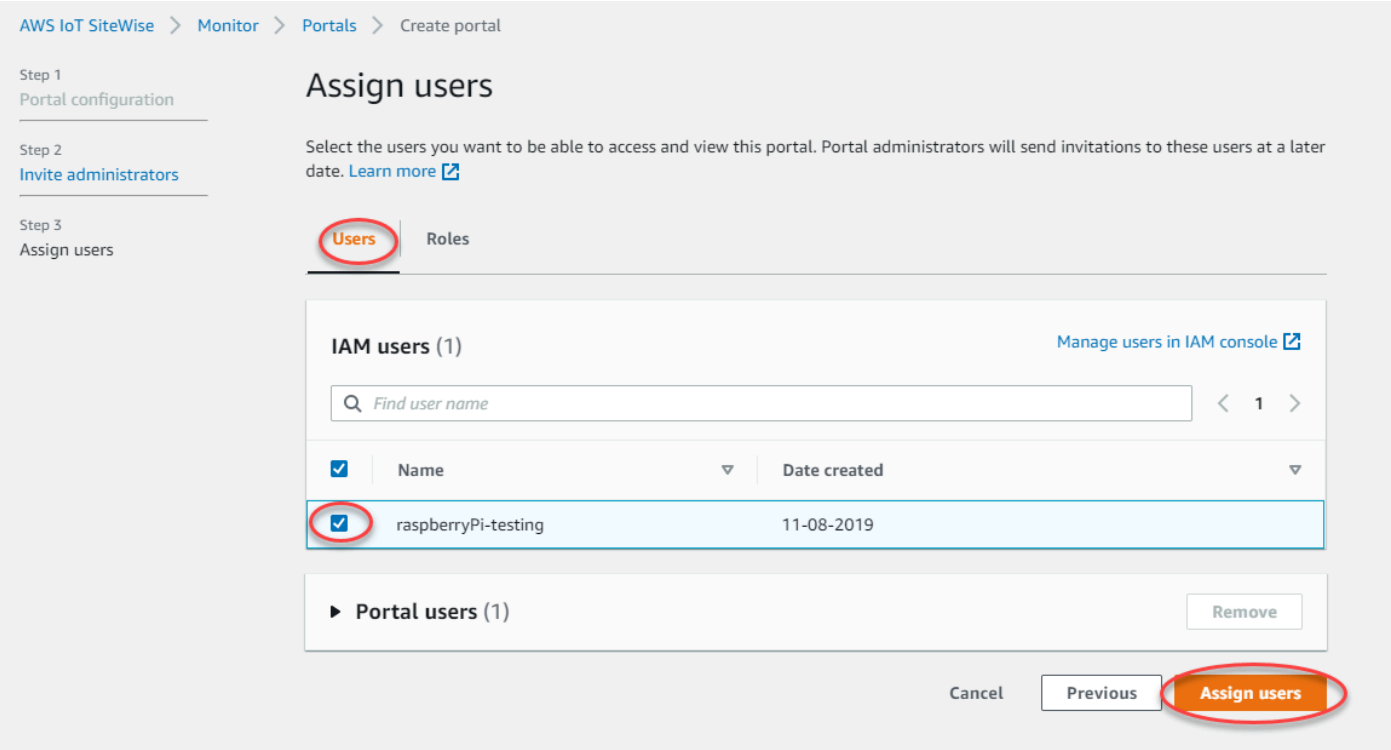
Como adicionar usuários do portal

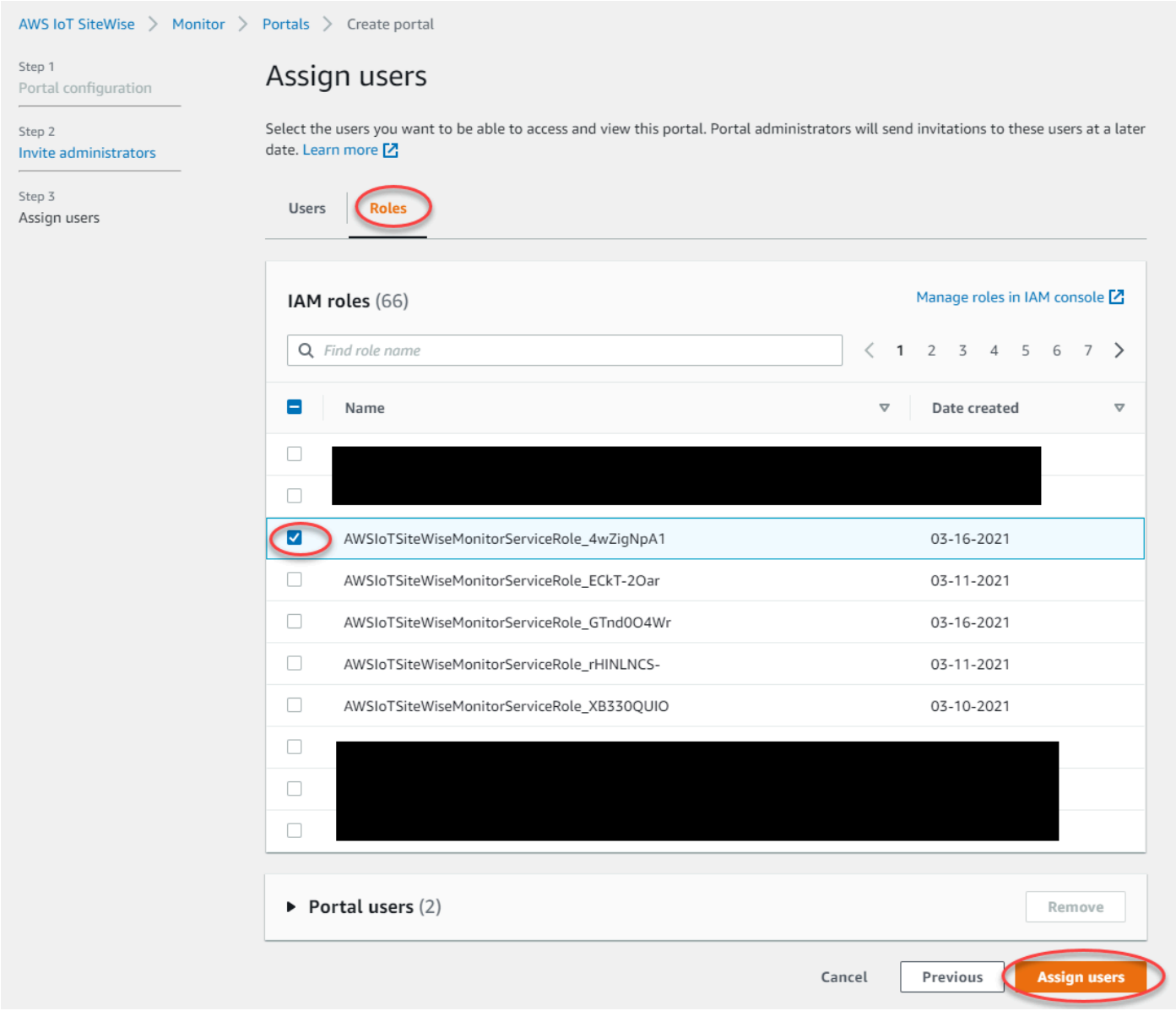
1. Execute as seguintes opções:

   - Escolha usuários do IAM para adicionar um usuário do IAM como seu usuário do portal.
   - Escolha perfis do IAM para adicionar um perfil do IAM como usuário do portal.

   Se você estiver utilizando o SiteWise Monitor pela primeira vez, você não precisa adicionar seu administrador do portal como um usuário do portal.
2. Marque as caixas de seleção para os usuários ou perfis que você deseja como usuários do portal. Isso adiciona os usuários ou perfis à lista de Usuários do portal.
3. Se você adicionar um usuário que não quer que tenha acesso ao portal, desmarque a caixa de seleção desse usuário.
4. Quando terminar de selecionar os usuários, escolha Compartilhar.

> **Important**
>
> Usuários ou perfis devem ter a permissão de `iotsitewise:DescribePortal` para entrar no portal.





Parabéns! Você criou com êxito um portal, atribuiu administradores de portal e atribuiu usuários que poderão usar o portal quando forem convidados. Agora os administradores do portal podem criar projetos e adicionar ativos a esses projetos. Depois, os proprietários do projeto podem criar painéis para visualizar os dados de cada ativo do projeto.

É possível alterar a lista de usuários do portal posteriormente. Para ter mais informações, consulte Adicionar ou remover usuários do portal.

Se precisar fazer alterações no portal, consulte Administrando seus portais do SiteWise Monitor.

Para começar no portal, consulte Introdução no Guia de Aplicação do SiteWise Monitor.

Criando painéis (AWS Command Line Interface)

Ao definir visualizações (ou widgets) em painéis usando a AWS CLI, você deve especificar as seguintes informações no documento JSON `dashboardDefinition`. Essa definição é um parâmetro das UpdateDashboardoperações CreateDashboarde.

`widgets`

Uma lista de estruturas de definição de widget que contêm as seguintes informações:

`type`

O tipo de widget. O AWS IoT SiteWise fornece os seguintes tipos de widget:

- `sc-line-chart`: um gráfico de linhas. Para obter mais informações, consulte Gráficos de linhas no Guia de aplicativo do AWS IoT SiteWise Monitor.
- `sc-scatter-chart`: um gráfico de dispersão. Para obter mais informações, consulte Gráficos de dispersão no Guia de aplicativo do AWS IoT SiteWise Monitor.
- `sc-bar-chart`: um gráfico de barras. Para obter mais informações, consulte Gráficos de barras no Guia de aplicativo do AWS IoT SiteWise Monitor.
- `sc-status-grid`: um widget de status que mostra o valor mais recente das propriedades do ativo como uma grade. Para obter mais informações, consulte Widgets de status no Guia do aplicativo do AWS IoT SiteWise Monitor.
- `sc-status-timeline`: um widget de status que mostra o valor mais recente das propriedades do ativo como uma linha do tempo. Para obter mais informações, consulte Widgets de status no Guia do aplicativo do AWS IoT SiteWise Monitor.
- `sc-kpi`: uma visualização do indicador chave de desempenho (KPI). Para obter mais informações, consulte Widgets de KPI no Guia do aplicativo do AWS IoT SiteWise Monitor.
- `sc-table`: um widget de tabela. Para obter mais informações, consulte Widgets de tabela no Guia do aplicativo do AWS IoT SiteWise Monitor.

`title`

O título do widget.

`x`

A posição horizontal do widget, começando à esquerda da grade. Esse valor se refere à posição do widget na grade do painel.

`y`

A posição vertical do widget, começando pelo topo da grade. Esse valor se refere à posição do widget na grade do painel.

`width`

A largura do widget, expressa em número de espaços na grade do painel.

`height`

A altura do widget, expressa em número de espaços na grade do painel.

`metrics`

Uma lista de estruturas de métricas em que cada uma define um fluxo de dados para este widget. Cada estrutura na lista deve conter as seguintes informações:

`label`

Um rótulo a ser exibido para essa métrica.

`type`

O tipo de fonte de dados para esta métrica. O AWS IoT SiteWise fornece os seguintes tipos de métrica:

- `iotsitewise`: o painel obtém dados da propriedade de um ativo no AWS IoT SiteWise. Se você escolher essa opção, deverá definir `assetId` e `propertyId` para essa métrica.

`assetId`

(Opcional) O ID de um ativo no AWS IoT SiteWise.

Esse campo será obrigatório se você escolher `iotsitewise` para `type` nessa métrica.

`propertyId`

(Opcional) O ID de uma propriedade de ativo no AWS IoT SiteWise.

Esse campo será obrigatório se você escolher `iotsitewise` para `type` nessa métrica.

`analysis`

(Opcional) Uma estrutura que define a análise, como linhas de tendência, a ser exibida para o widget. Para obter mais informações, consulte Configurar linhas de tendência em Guia do aplicativo AWS IoT SiteWise Monitor. Você pode adicionar uma linha de tendência de cada tipo por propriedade no widget. A estrutura de análise contém as seguintes informações:

`trends`

(Opcional) Uma lista de estruturas de tendência, cada uma definindo uma análise de tendência para esse widget. Cada estrutura na lista contém as seguintes informações:

`type`

O tipo de linha de tendência. Escolha a seguinte opção:

- `linear-regression`— Exibir uma linha de regressão linear. SiteWise O monitor usa o método dos mínimos quadrados para calcular a regressão linear.

`annotations`

(Opcional) Uma estrutura de anotações que define limites para o widget. Para obter mais informações, consulte Configurar limites em Guia do aplicativo do AWS IoT SiteWise Monitor. Você pode adicionar até seis anotações por widget. A estrutura de anotações contém as seguintes informações:

`y`

(Opcional) Uma lista de estruturas de anotação, cada uma definindo um limite horizontal para esse widget. Cada estrutura na lista contém as seguintes informações:

`comparisonOperator`

O operador de comparação para o limite. Escolha uma das seguintes opções:

- `LT`: destaque propriedades que tenham pelo menos um ponto de dados menor que `value`.
- `GT`: destaque propriedades que tenham pelo menos um ponto de dados maior que `value`.
- `LTE`: destaque propriedades que tenham pelo menos um ponto de dados menor ou igual a `value`.
- `GTE`: destaque propriedades que tenham pelo menos um ponto de dados maior ou igual a `value`.

- `EQ`: destaque propriedades que tenham pelo menos um ponto de dados igual a `value`.

`value`

O valor limite para comparar os pontos de dados com o `comparisonOperator`.

`color`

(Opcional) O código hexadecimal de 6 dígitos da cor limite. A visualização exibe legendas de propriedades nesta cor para propriedades com pelo menos um ponto de dados que atenda à regra de limite. Padrões do preto (`#000000`).

`showValue`

(Opcional) Se deve ou não mostrar o valor do limite nas margens do widget. Padronizado como `true`.

`properties`

(Opcional) Um dicionário simples de propriedades para o widget. Os membros dessa estrutura dependem do contexto. AWS IoT SiteWise fornece os seguintes widgets que usam `properties`:

- Gráficos de linhas, gráficos de dispersão e gráficos de barras têm a seguinte propriedade:

  `colorDataAcrossThresholds`

  (Opcional) Se deve ou não alterar a cor dos dados que ultrapassam os limites desse widget. Quando você ativa essa opção, os dados que ultrapassam um limite aparecem na cor que você escolher. Padronizado como `true`.

- As grades de status têm a seguinte propriedade:

  `labels`

  (Opcional) Uma estrutura que define os rótulos a serem exibidos na grade de status. A estrutura dos rótulos contém as seguintes informações:

  `showValue`

  (Opcional) Se deve ou não exibir a unidade e o valor de cada propriedade do ativo nesse widget. Padronizado como `true`.

Example Exemplo de definição de painel

O exemplo a seguir define um painel de uma carga útil armazenada em um arquivo JSON.

```
aws iotsitewise create-dashboard \
  --project-id a1b2c3d4-5678-90ab-cdef-eeeeeEXAMPLE \
  --dashboard-name "Wind Farm Dashboard" \
  --dashboard-definition file://dashboard-definition.json
```

O exemplo de JSON a seguir para `dashboard-definition.json` define o painel com os seguintes widgets de visualização:

- Um gráfico de linhas que visualiza a potência total do parque eólico no canto superior esquerdo do painel. Esse gráfico de linhas inclui um limite que indica quando o parque eólico gera menos energia do que a produção mínima esperada. Esse gráfico de linhas também inclui uma linha de tendência de regressão linear.
- Um gráfico de barras que visualiza a velocidade do vento para quatro turbinas no canto superior direito do painel.

> **Note**
>
> Esse exemplo representa visualizações de gráfico de linhas e de barras em um painel. Este painel é semelhante ao painel de exemplo do parque eólico.

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

Habilitar alarmes para seus portais

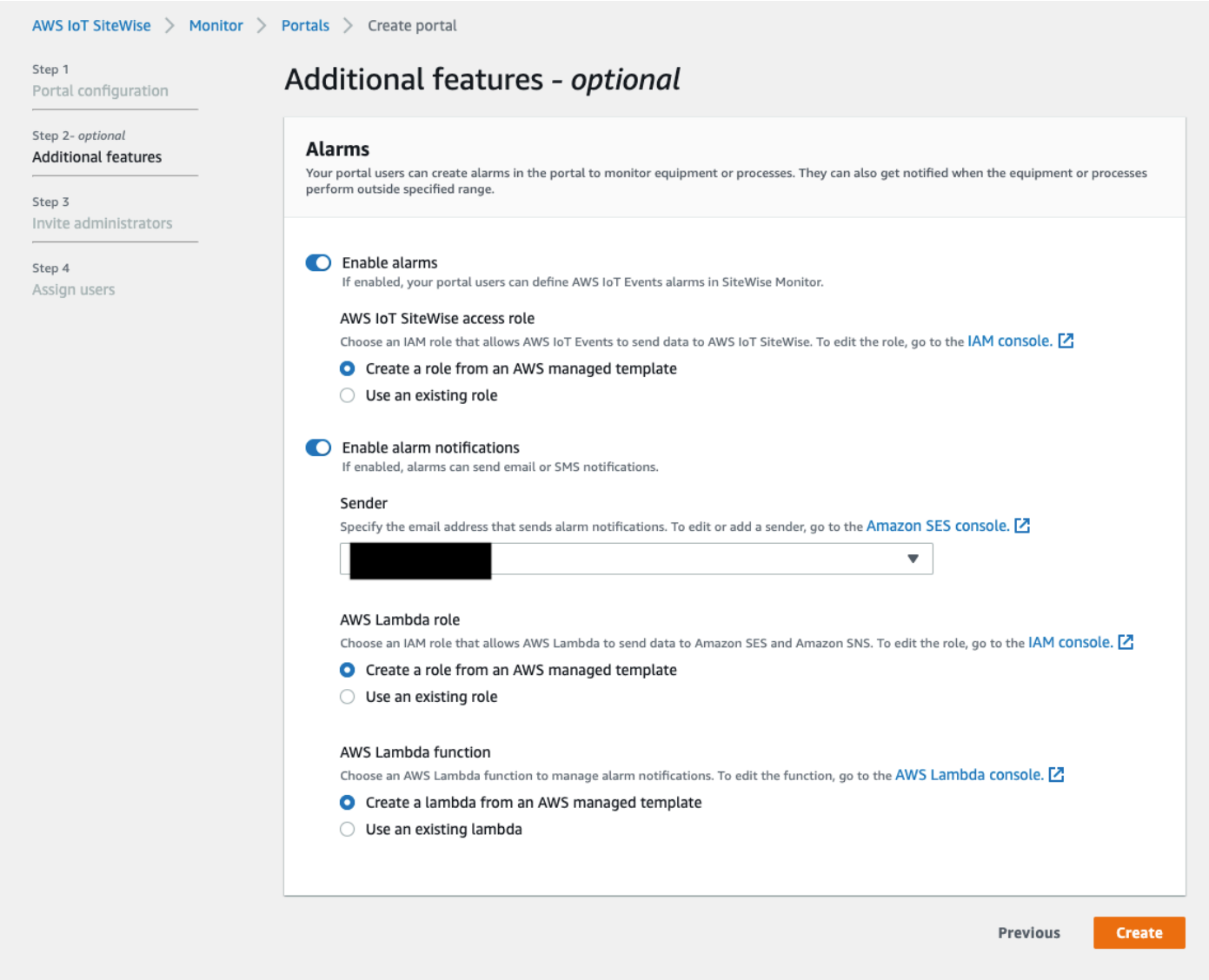
Você pode ativar o recurso de alarmes suportado por seus portais AWS IoT Events para que os administradores do portal possam criar, editar e excluir modelos de AWS IoT Events alarme em seus SiteWise portais do Monitor. Os proprietários do projeto podem configurar alarmes. Os visualizadores do projeto podem ver os detalhes do alarme. Esta seção explica como você pode usar o AWS IoT SiteWise console para ativar o recurso de alarmes em seus portais.

Important

- Você não pode criar alarmes externos em seus portais.
- Se quiser enviar notificações de alarme, você deve escolher o Centro de identidade do IAM para o serviço de autenticação do usuário.
- O recurso de notificações de alarme não está disponível na China (Pequim) Região da AWS.

Ao configurar e criar um portal, você pode habilitar alarmes e notificações de alarme na Etapa 2 atributos adicionais. Com base no serviço de autenticação do usuário, selecione uma das opções a seguir:

IAM Identity Center



Para habilitar alarmes para um portal

1. (Opcional) Escolha Habilitar alarmes.

   - Para o perfil de acesso do AWS IoT SiteWise , use um perfil existente ou crie um perfil com as permissões necessárias. Esse perfil requer `iotevents:BatchPutMessage` permissão e um relacionamento de confiança que permita que `iot.amazonaws.com` e `iotevents.amazonaws.com` assumam o perfil.

2. (Opcional) Escolha Habilitar notificações de alarme.

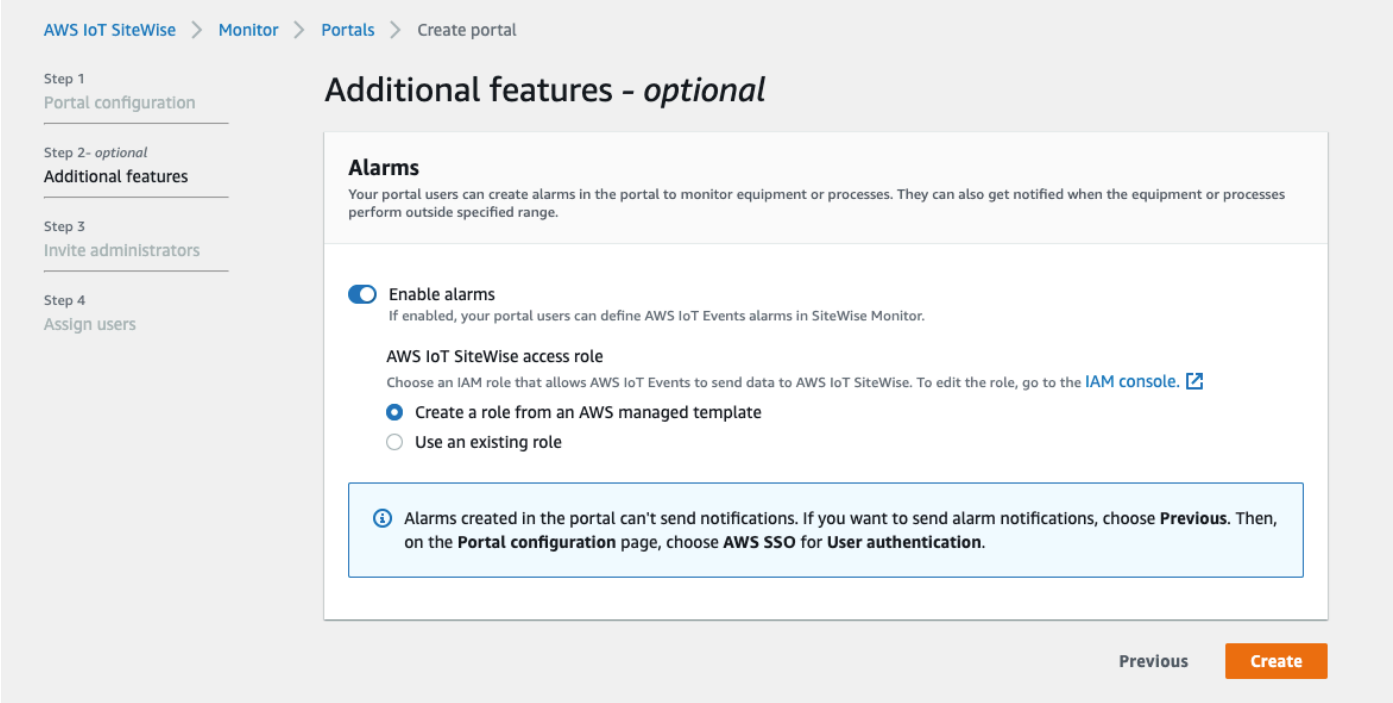
   a. Em Remetente, escolha o remetente.

> **Important**
>
> Você deve verificar o endereço de e-mail do remetente no Amazon SES. Para mais informações, consulte Verificar endereços de e-mail no Amazon SES no Guia do desenvolvedor do Amazon Simple Email Service.

b. Para o perfil AWS Lambda , use um perfil existente ou crie um perfil com as permissões necessárias. Esse perfil requer as permissões `lambda:InvokeFunction` e `sso-directory:DescribeUser` e um relacionamento de confiança que permita que `iotevents.amazonaws.com` e `lambda.amazonaws.com` assumam o perfil.

c. Para AWS Lambda funções, escolha uma função do Lambda existente ou crie uma função que gerencie notificações de alarme. Para obter mais informações, consulte Gerenciar notificações de alarme no Guia do desenvolvedor do AWS IoT Events .

IAM



Para habilitar alarmes para um portal

- (Opcional) Escolha Habilitar alarmes.

- Para o perfil de acesso do AWS IoT SiteWise , use um perfil existente ou crie um perfil com as permissões necessárias. Esse perfil requer `iotevents:BatchPutMessage` permissão e um relacionamento de confiança que permita que `iot.amazonaws.com` e `iotevents.amazonaws.com` assumam o perfil.

Para obter mais informações sobre alarmes no SiteWise Monitor, consulte Monitoramento com alarmes no Guia do AWS IoT SiteWise Aplicativo.

Habilitar seu portal na borda

Depois de habilitar seu portal na borda, esse portal estará disponível em todos os gateways do SiteWise Edge com o pacote de processamento de dados habilitado em sua conta.

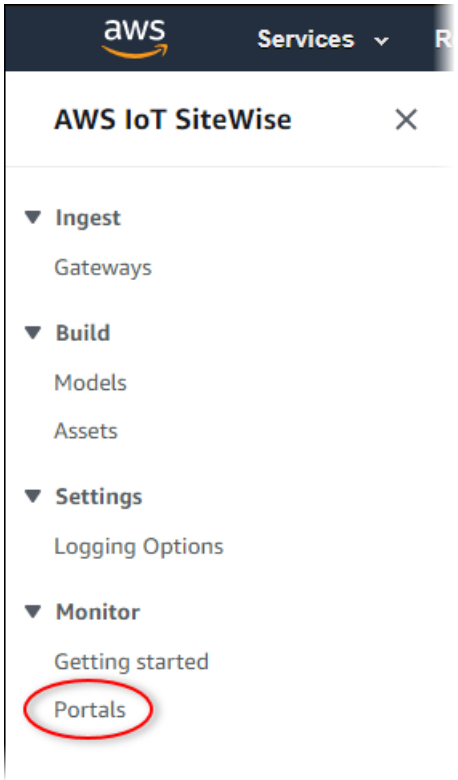
Para habilitar o portal na borda

1. Na seção Configuração de borda, ative Habilitar este portal na borda.
2. Escolha Criar.

Administrando seus portais do SiteWise Monitor

Talvez seja necessário atualizar os detalhes do portal, alterar administradores ou adicionar usuários aos seus portais. Esta seção explica como você pode concluir essas tarefas administrativas básicas para seus portais do SiteWise Monitor.

1. Faça login no AWS IoT SiteWise console.
2. No painel de navegação, escolha Monitorar, Portais.



3. Escolha um portal e selecione Visualizar detalhes (ou selecione o Nome do portal).
4. Você pode executar qualquer uma das seguintes tarefas administrativas:

   - Alterar o nome, a descrição, a marca, o e-mail de suporte e as permissões de um portal
   - Adicionar ou remover administradores do portal
   - Enviar convites por e-mail para administradores do portal
   - Adicionar ou remover usuários do portal
   - Excluir um portal

Para obter informações sobre como criar um portal, consulte Começando com AWS IoT SiteWise Monitor.

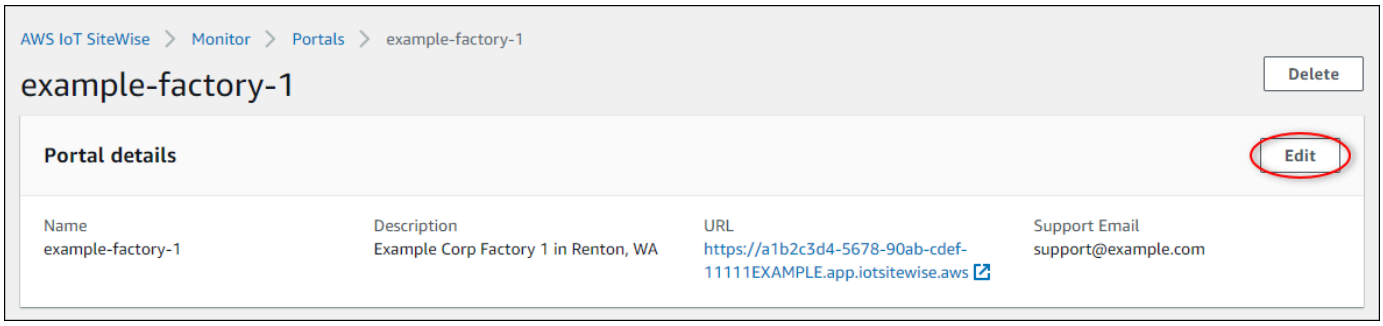
Tópicos

- Alterar o nome, a descrição, a marca, o e-mail de suporte e as permissões de um portal
- Adicionar ou remover administradores do portal
- Enviar convites por e-mail para administradores do portal
- Adicionar ou remover usuários do portal
- Excluir um portal

Alterar o nome, a descrição, a marca, o e-mail de suporte e as permissões de um portal

Você pode alterar o nome, a descrição, a marca, o e-mail de suporte e as permissões de um portal.

1. Na página de detalhes do portal, na seção Detalhes do portal escolha Editar.

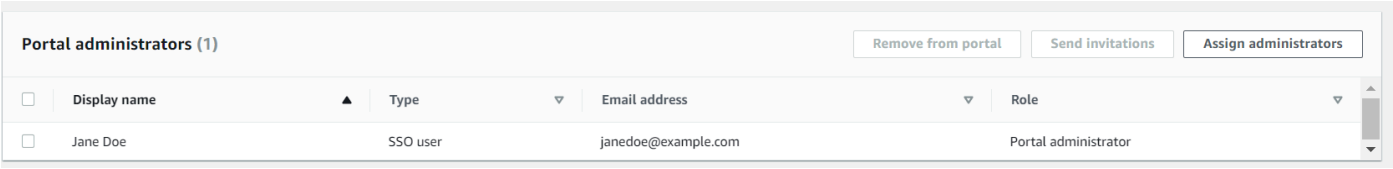


2. Atualize o Nome, a Descrição, a Marca do portal, o E-mail de contato do suporte ou as Permissões.
3. Ao terminar, escolha Salvar.

Adicionar ou remover administradores do portal

Em algumas etapas, é possível adicionar ou remover usuários como administradores de um portal. Com base no serviço de autenticação do usuário, selecione uma das opções a seguir.

IAM Identity Center

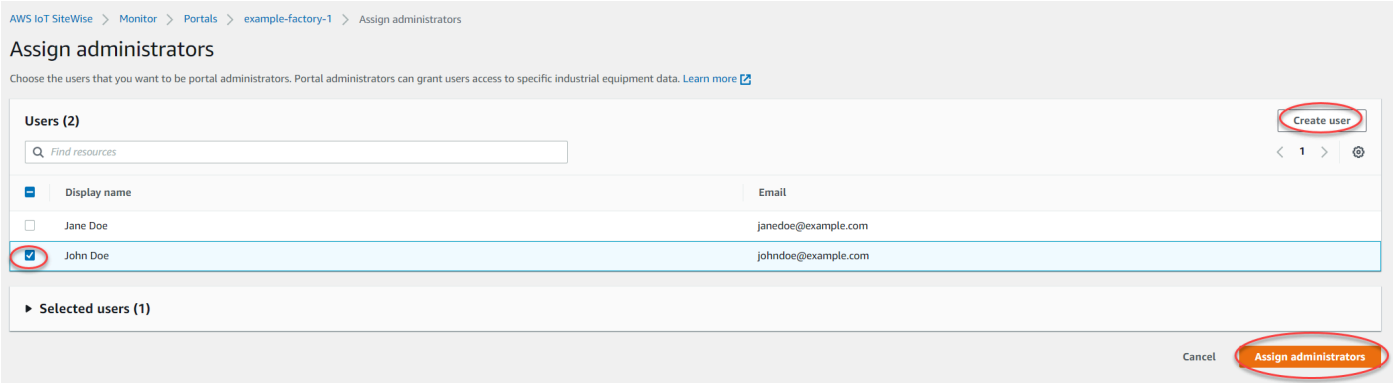


Como adicionar administradores do portal

1. Na página de detalhes do portal, na seção Administradores do portal, selecione Atribuir usuários.
2. Na página Atribuir administradores marque as caixas de seleção para os usuários a serem adicionados ao portal como administradores.

> **Note**
>
> Se você usa o Centro de identidade do IAM como seu repositório de identidades e está conectado à sua conta de gerenciamento AWS Organizations , pode escolher Criar usuário para criar um usuário do Centro de identidade do IAM. O Centro de identidade do IAM envia ao novo usuário um e-mail para que ele defina sua senha. Você pode então atribuir o usuário ao portal como administrador. Para obter mais informações, consulte Gerenciar identidades no Centro de identidade do IAM.

3. Escolha Atribuir administradores.

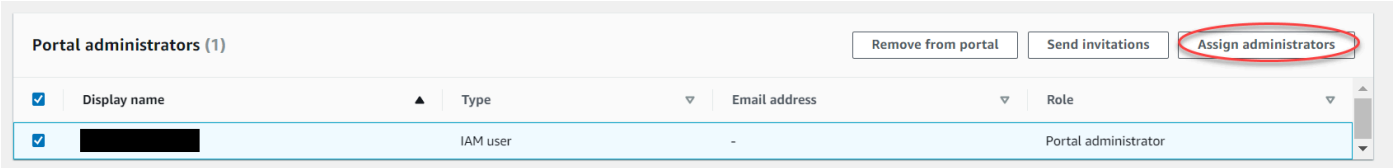


Como remover administradores do portal

- Na página de detalhes do portal, na seção Administradores do portal, marque a caixa de seleção dos usuários a serem removidos e escolha Remover do portal.

> **Note**
>
> Recomendamos que você selecione pelo menos um administrador do portal.

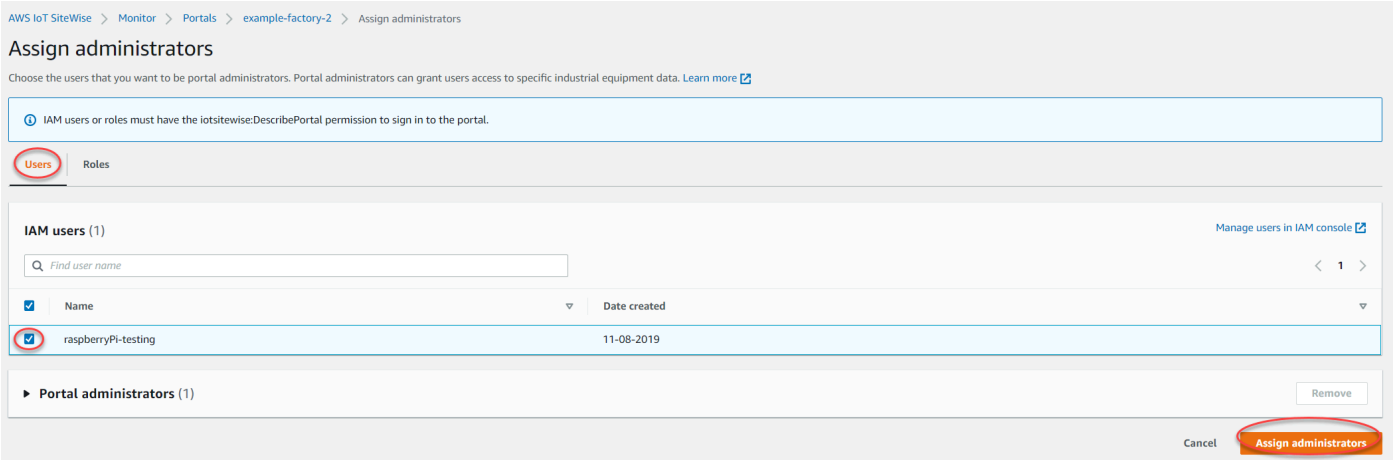
IAM

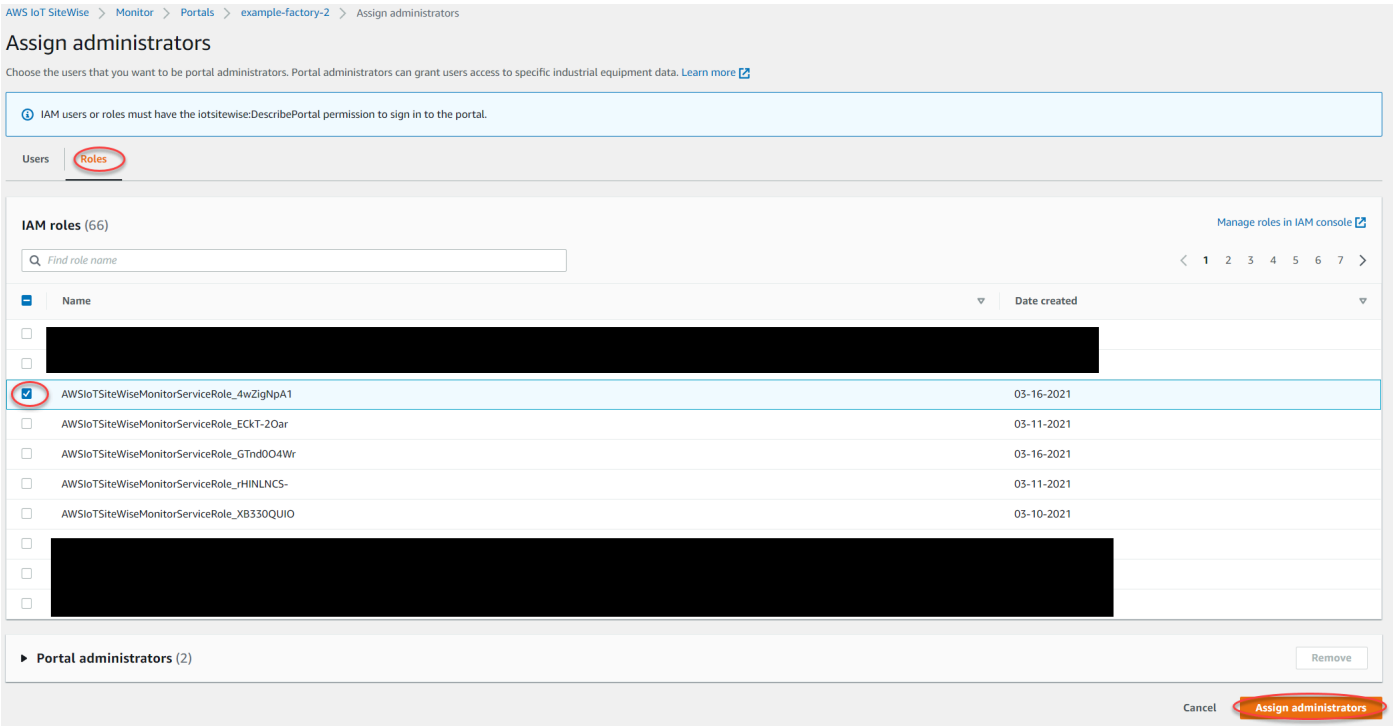


Como adicionar administradores do portal

1. Na página de detalhes do portal, na seção Administradores do portal, selecione Atribuir usuários.
2. Na página Atribuir administradores, faça o seguinte:
   - Escolha usuários do IAM se quiser adicionar um usuário do IAM como seu administrador do portal.
   - Escolha perfis do IAM se quiser adicionar um perfil do IAM como administrador do portal.
3. Marque as caixas de seleção para os usuários ou perfis que você deseja como administradores do portal. Isso adiciona os usuários ou perfis à lista de Administradores do Portal.
4. Escolha Atribuir administradores.

> **Important**
>
> Usuários ou perfis devem ter a permissão de `iotsitewise:DescribePortal` para entrar no portal.





Como remover administradores do portal

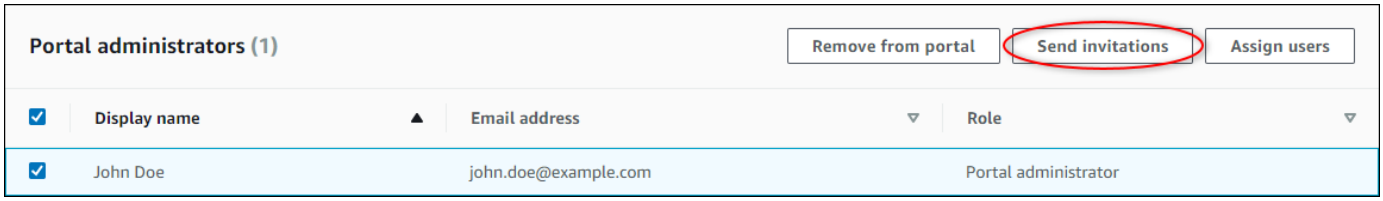
- Na página de detalhes do portal, na seção Administradores do portal, marque a caixa de seleção dos usuários a serem removidos e escolha Remover do portal.

> **Note**
>
> Não é recomendado deixar um portal sem administrador do portal.

Enviar convites por e-mail para administradores do portal

Você pode enviar convites por e-mail para administradores do portal.

1. Na página de detalhes do portal, na seção Administradores do portal marque as caixas de seleção dos administradores do portal.



2. Escolha Enviar convites. Seu cliente de e-mail será aberto e um convite será colocado no corpo da mensagem.

   É possível personalizar o e-mail antes de enviá-lo para os administradores do portal.

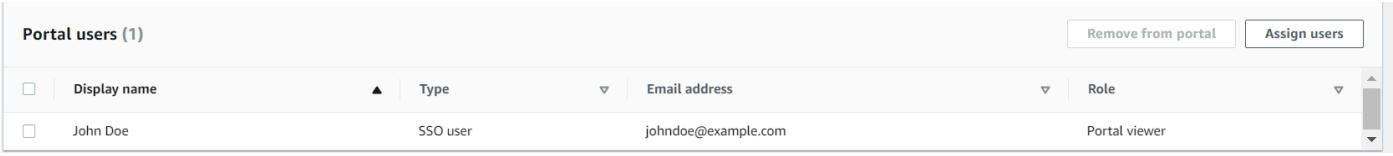
Adicionar ou remover usuários do portal

Você escolhe quais usuários têm acesso aos portais. Os usuários do portal aparecem na lista de usuários em um portal SiteWise Monitor. Nessa lista, os administradores do portal podem adicionar proprietários de projetos, e os proprietários de projetos podem adicionar visualizadores de projetos.

> **Note**
>
> Os administradores do portal e os usuários do portal poderão entrar em contato com você por meio do e-mail de suporte de um portal se precisarem e um usuário seja adicionado ou removido.

Com base no serviço de autenticação do usuário, selecione uma das opções a seguir.

IAM Identity Center



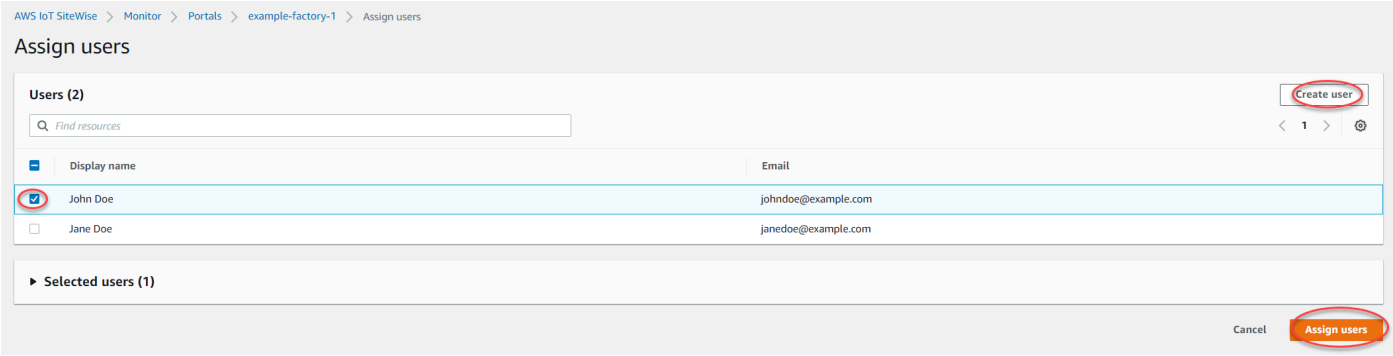
Como adicionar usuários do portal

1. Na página de detalhes do portal, na seção Usuários do portal, selecione Atribuir usuários.
2. Na página Atribuir usuários, marque a caixa de seleção dos usuários a serem adicionados ao portal.

   > **Note**
   >
   > Se você usa o Centro de identidade do IAM como seu repositório de identidades e está conectado à sua conta de gerenciamento AWS Organizations , pode escolher Criar usuário para criar um usuário do Centro de identidade do IAM. O Centro de identidade do IAM envia ao novo usuário um e-mail para que ele defina sua

senha. Você pode então atribuir o usuário ao portal como usuário. Para obter mais informações, consulte Gerenciar identidades no Centro de identidade do IAM.

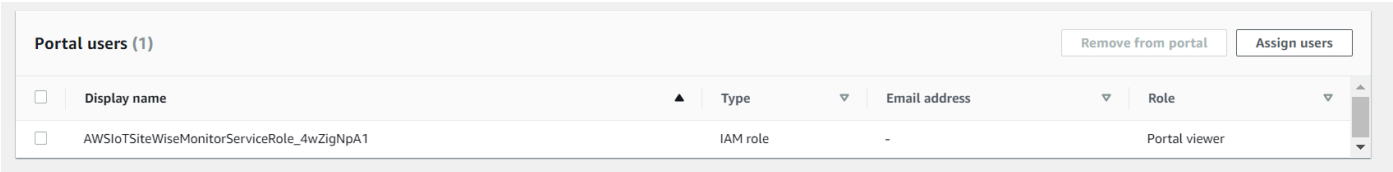
3. Escolha Atribuir usuários.



Como remover usuários do portal

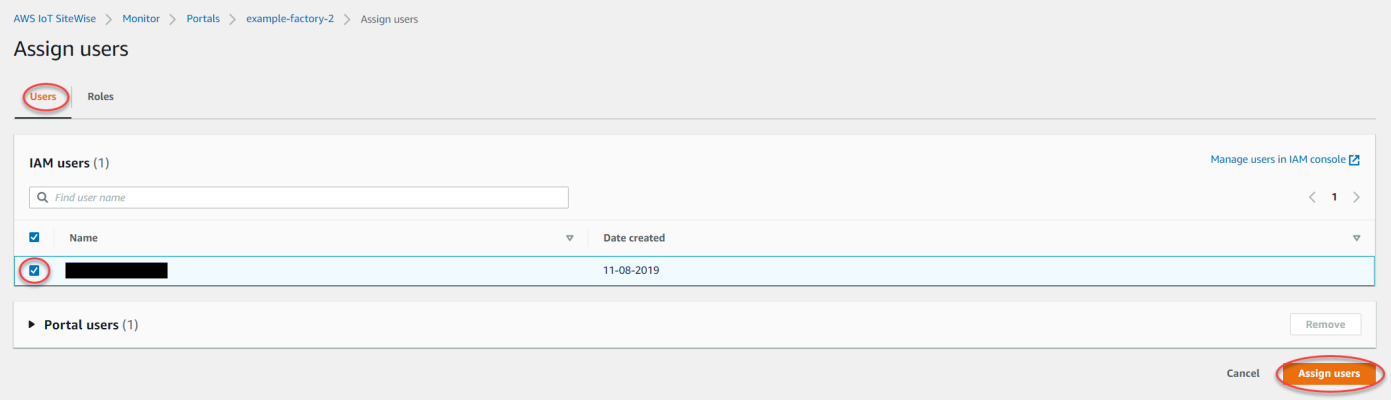
- Na página de detalhes do portal, na seção Usuários do portal, marque a caixa de seleção dos usuários a serem removidos do portal e selecione Remover do portal.

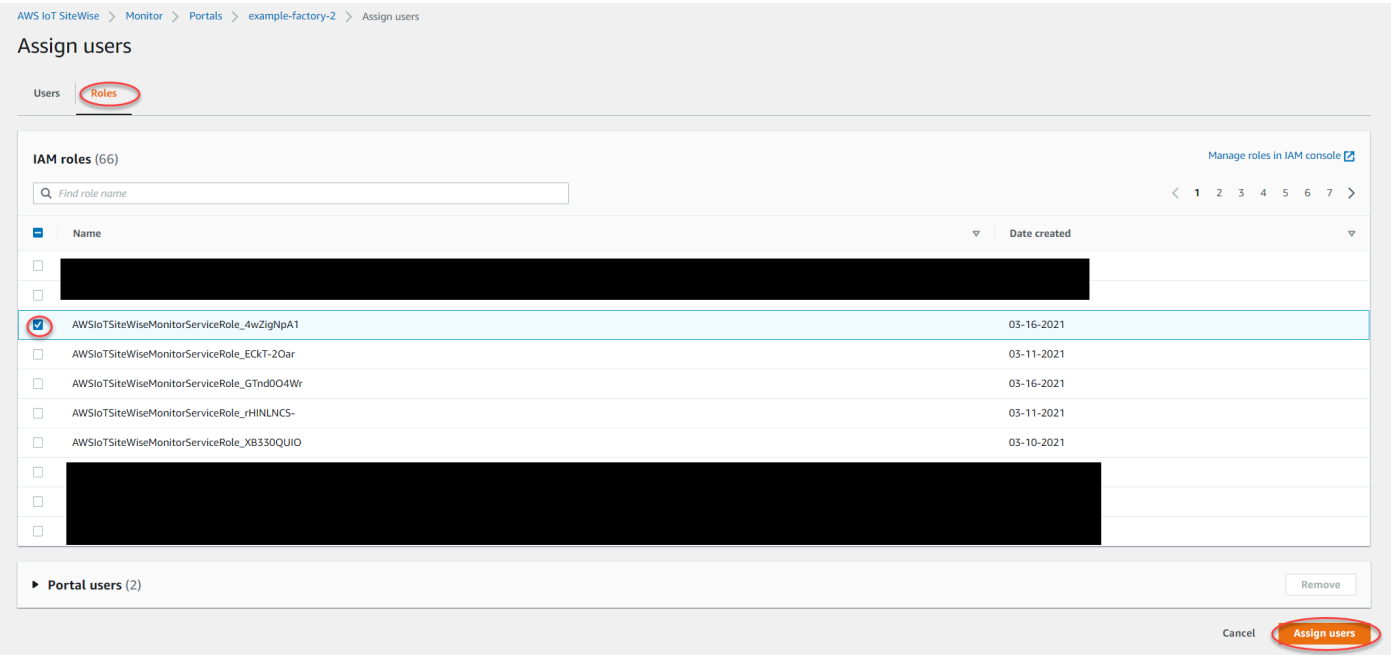
IAM



Como adicionar usuários do portal

1. Na página de detalhes do portal, na seção Usuários do portal, selecione Atribuir usuários.
2. Na página Atribuir usuários, faça o seguinte:
   - Escolha usuários do IAM para adicionar um usuário do IAM como seu usuário do portal.
   - Escolha perfis do IAM para adicionar um perfil do IAM como usuário do portal.
3. Marque as caixas de seleção para os usuários ou perfis que você deseja acrescentar como usuários do portal. Isso adiciona os usuários ou perfis à lista de Usuários do portal.
4. Escolha Atribuir usuários.





Como remover usuários do portal

- Na página de detalhes do portal, na seção Usuários do portal, marque a caixa de seleção dos usuários a serem removidos do portal e selecione Remover do portal.

> **Important**
>
> Usuários ou perfis devem ter a permissão de `iotsitewise:DescribePortal` para entrar no portal.

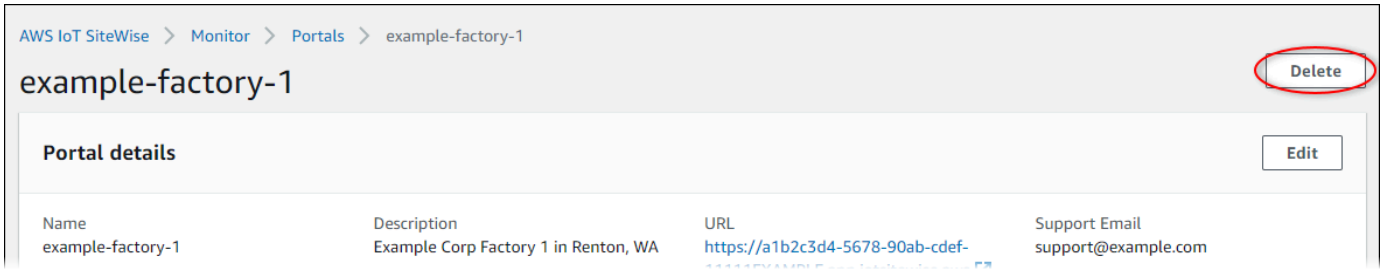
Excluir um portal

Você pode excluir um portal se ele foi criado para fins de teste ou se foi criada uma duplicata de um portal que já existe.

> **Note**
>
> Primeiro, é necessário excluir manualmente todos os painéis e projetos em um portal antes de excluí-lo. Para obter mais informações, consulte Excluindo projetos e Excluindo painéis no Guia de aplicativos do SiteWise Monitor.

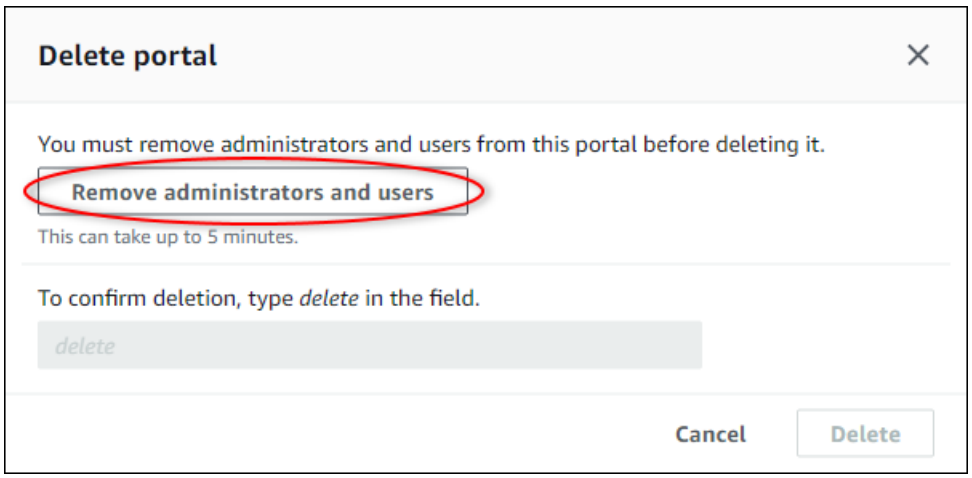
1. Na página de detalhes do portal, escolha Excluir.

   > **Important**
   >
   > Quando exclui um portal, você perde todos os projetos contidos no portal e todos os painéis em cada projeto. Essa ação não pode ser desfeita. Os dados de ativos não são afetados.

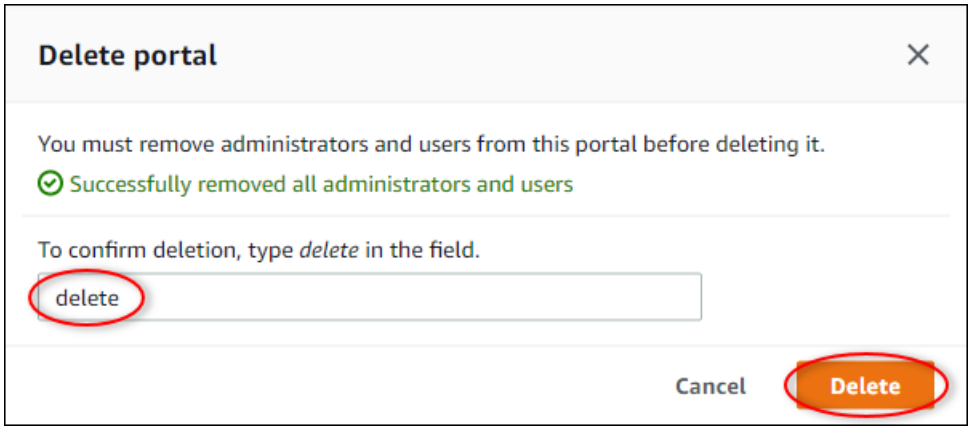


2. Na caixa de diálogo Excluir portais escolha Remover administradores e usuários.

   É necessário remover os administradores e usuários de um portal para poder excluí-lo. Se o portal não tiver administradores ou usuários, o botão não será exibido e você poderá prosseguir para a próxima etapa.



3. Se tiver certeza de que deseja excluir todo o portal, insira **`delete`** no campo para confirmar a exclusão.



4. Escolha Excluir.

Monitoramento de dados com o aplicativo de painel de IoT

O aplicativo de painel de IoT é um aplicativo de painel de código aberto onde você pode visualizar e interagir com dados operacionais. Você pode utilizar o AWS Cloud Development Kit (AWS CDK) para implantar o aplicativo de painel de IoT.

A seguir estão exemplos dos recursos personalizáveis de visualização de dados no aplicativo de painel de IoT:

- Support para várias propriedades em um gráfico de linha única.
- Pesquisa aprimorada de ativos e propriedades.

Clientes de manufatura, logística, energia e outros setores podem usar o aplicativo de painel de IoT para enfrentar desafios específicos, como monitorar o desempenho do equipamento, otimizar a eficiência operacional e tomar decisões baseadas em dados. Para obter mais informações, consulte o GitHub repositório do aplicativo de painel de IoT.

Consultar dados de AWS IoT SiteWise

Você pode usar as operações da AWS IoT SiteWise API para consultar os valores atuais, os valores históricos e os agregados de suas propriedades de ativos em intervalos de tempo específicos.

Use esses recursos para obter informações sobre seus dados. Por exemplo, descubra todos os seus ativos com um determinado valor de propriedade ou crie uma representação personalizada dos seus dados. Você também pode usar operações de API para desenvolver soluções de software que se integrem aos dados industriais armazenados em seus AWS IoT SiteWise ativos. Também é possível explorar os dados de ativos em tempo real no AWS IoT SiteWise Monitor. Para saber como configurar o SiteWise Monitor, consulteMonitorando dados com AWS IoT SiteWise Monitor.

As operações descritas nesta seção retornam objetos de valor de propriedade que contêm estruturas de timestamp, qualidade e valor (TQV):

- O `timestamp` contém o horário Unix epoch atual em segundos, com correção em nanossegundos.
- `quality` contém uma das seguintes strings, que indicam a qualidade do ponto de dados:
  - `GOOD` – os dados não são afetados por nenhum problema.
  - `BAD` – os dados são afetados por um problema, como a falha do sensor.
  - `UNCERTAIN` – os dados são afetados por um problema, como a imprecisão do sensor.
- O `value` contém um dos campos a seguir, a depender do tipo de propriedade:
  - `booleanValue`
  - `doubleValue`
  - `integerValue`
  - `stringValue`

Tópicos

Consultando valores de propriedade do ativo atual

Este tutorial mostra duas maneiras de obter o valor atual de uma propriedade do ativo. Você pode usar o AWS IoT SiteWise console ou usar a API no AWS Command Line Interface (AWS CLI).

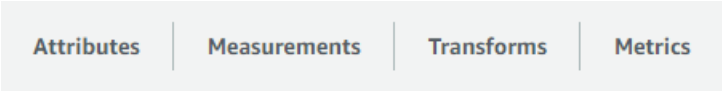
Tópicos

Consulte o valor atual de uma propriedade do ativo (console)

Você pode usar o AWS IoT SiteWise console para visualizar o valor atual de uma propriedade do ativo.

Como obter o valor atual de uma propriedade de ativo (console)

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Ativos.
3. Escolha o ativo com a propriedade a ser consultada.
4. Escolha o ícone de seta para expandir uma hierarquia de ativos e encontrar seu ativo.
5. Escolha a guia do tipo de propriedade. Por exemplo, escolha Medições para visualizar o valor atual de uma propriedade de medição.



6. Encontre a propriedade a ser visualizada. O valor atual aparece na coluna Valor mais recente.

Consulte o valor atual de uma propriedade do ativo (AWS CLI)

Você pode usar o AWS Command Line Interface (AWS CLI) para consultar o valor atual de uma propriedade do ativo.

Use a GetAssetPropertyValueoperação para consultar o valor atual de uma propriedade do ativo.

Para identificar uma propriedade do ativo, especifique uma das seguintes opções:

- O `assetId` fim `propertyId` da propriedade do ativo para a qual os dados são enviados.

- O `propertyAlias`, que é um alias de fluxo de dados (por exemplo, `/company/windfarm/3/turbine/7/temperature`). Para usar esta opção, primeiro você deve definir o apelido da propriedade do seu ativo. Para definir aliases de propriedades, consulteMapeamento de fluxos de dados industriais para propriedades de ativos.

Para obter o valor atual de uma propriedade do ativo (AWS CLI)

- Execute o seguinte comando para obter o valor atual da propriedade de ativo. Substitua *`asset-id`* pela ID do ativo e *`property-id`* pela ID da propriedade.

```
aws iotsitewise get-asset-property-value \
  --asset-id asset-id \
  --property-id property-id
```

A operação retornará uma resposta contendo o TQV atual da propriedade, no formato a seguir:

```
{
  "propertyValue": {
    "value": {
      "booleanValue": Boolean,
      "doubleValue": Number,
      "integerValue": Number,
      "stringValue": "String"
    },
    "timestamp": {
      "timeInSeconds": Number,
      "offsetInNanos": Number
    },
    "quality": "String"
  }
}
```

Consultar valores históricos de propriedade de ativos

Você pode usar a GetAssetPropertyValueHistoryoperação AWS IoT SiteWise da API para consultar os valores históricos de uma propriedade do ativo.

Para identificar uma propriedade do ativo, especifique uma das seguintes opções:

- O `assetId` fim `propertyId` da propriedade do ativo para a qual os dados são enviados.
- O `propertyAlias`, que é um alias de fluxo de dados (por exemplo, `/company/windfarm/3/turbine/7/temperature`). Para usar esta opção, primeiro você deve definir o apelido da propriedade do seu ativo. Para definir aliases de propriedades, consulteMapeamento de fluxos de dados industriais para propriedades de ativos.

Passe os seguintes parâmetros para refinar seus resultados:

- `startDate` — O início exclusivo do intervalo a partir do qual é possível consultar dados históricos, expressos em segundos, em tempo Unix epoch.
- `endDate` — O final inclusivo do intervalo a partir do qual a consulta de dados históricos é feita, expresso em segundos, no tempo Unix epoch.
- `maxResults` – O número máximo de resultados a serem retornados em uma solicitação. Remete ao padrão de `20` resultados.
- `nextToken` – Um token de paginação retornado de uma chamada anterior a essa operação.
- `timeOrdering` — A ordem a ser aplicada aos valores retornados: `ASCENDING` ou `DESCENDING`.
- `qualities` – A qualidade sob a qual pautar e filtrar os resultados: `GOOD`, `BAD`, ou `UNCERTAIN`.

Tópicos

- Consulte o histórico de valores de uma propriedade do ativo (AWS CLI)

Consulte o histórico de valores de uma propriedade do ativo (AWS CLI)

Para consultar o histórico de valores de uma propriedade do ativo (AWS CLI)

1. Execute o seguinte comando para obter o histórico de valores da propriedade de ativo: Esse comando consulta o histórico da propriedade em um intervalo específico de 10 minutos. Substitua *`asset-id`* pela ID do ativo e *`property-id`* pela ID da propriedade. Substitua os parâmetros de data pelo intervalo a ser consultado.

```
aws iotsitewise get-asset-property-value-history \
  --asset-id asset-id \
  --property-id property-id \
  --start-date 1575216000 \
  --end-date 1575216600
```

A operação retorna uma resposta que contém os TQVs históricos da propriedade no seguinte formato:

```
{
  "assetPropertyValueHistory": [
    {
      "value": {
        "booleanValue": Boolean,
        "doubleValue": Number,
        "integerValue": Number,
        "stringValue": "String"
      },
      "timestamp": {
        "timeInSeconds": Number,
        "offsetInNanos": Number
      },
      "quality": "String"
    }
  ],
  "nextToken": "String"
}
```

2. Se existirem mais entradas de valor, você poderá passar o token de paginação do `nextToken` campo para uma chamada subsequente para a GetAssetPropertyValueHistoryoperação.

Consultando agregados de propriedades de ativos

AWS IoT SiteWise calcula automaticamente valores agregados de propriedades de ativos, que são um conjunto de métricas básicas calculadas em vários intervalos de tempo. AWS IoT SiteWise calcula os seguintes agregados a cada minuto, hora e dia para suas propriedades de ativos:

- média – A média (meio) dos valores de uma propriedade ao longo de um intervalo de tempo.
- contagem O número de pontos de dados para uma propriedade em um intervalo de tempo.
- máximo – O máximo de valores de uma propriedade ao longo de um intervalo de tempo.
- mínimo – O mínimo de valores de uma propriedade ao longo de um intervalo de tempo.
- desvio padrão – O desvio padrão dos valores de uma propriedade ao longo de um intervalo de tempo.
- soma – A soma dos valores de uma propriedade em um intervalo de tempo.

Para propriedades não numéricas, como cadeias de caracteres e booleanos, AWS IoT SiteWise calcula somente o agregado de contagem.

Você também pode calcular métricas personalizadas para os dados dos ativos. Com as propriedades métricas, você define agregações específicas para sua operação. As propriedades métricas oferecem funções de agregação e intervalos de tempo adicionais que não são pré-computados para a API. AWS IoT SiteWise Para ter mais informações, consulte Agregando dados de propriedades e outros ativos (métricas).

Tópicos

- Agregados para uma propriedade de ativo (API)
- Agregados para uma propriedade de ativo ()AWS CLI

Agregados para uma propriedade de ativo (API)

Você pode usar a AWS IoT SiteWise API para obter agregados para uma propriedade de ativo.

Use a GetAssetPropertyAggregatesoperação para consultar agregados de uma propriedade do ativo.

Para identificar uma propriedade do ativo, especifique uma das seguintes opções:

- O `assetId` fim `propertyId` da propriedade do ativo para a qual os dados são enviados.
- O `propertyAlias`, que é um alias de fluxo de dados (por exemplo, `/company/windfarm/3/turbine/7/temperature`). Para usar esta opção, primeiro você deve definir o apelido da propriedade do seu ativo. Para definir aliases de propriedades, consulteMapeamento de fluxos de dados industriais para propriedades de ativos.

Você também deve definir os seguintes parâmetros necessários:

- `aggregateTypes` – A lista de agregados a recuperar. Você pode especificar qualquer opção entre `AVERAGE`, `COUNT`, `MAXIMUM`, `MINIMUM`, `STANDARD_DEVIATION` e `SUM`.
- `resolution` – O intervalo de tempo durante o qual é necessário recuperar a métrica: `1m` (1 minuto), `1h` (1 hora) ou `1d` (1 dia).
- `startDate` — O início exclusivo do intervalo a partir do qual é possível consultar dados históricos, expressos em segundos, em tempo Unix epoch.
- `endDate` — O final inclusivo do intervalo a partir do qual a consulta de dados históricos é feita, expresso em segundos, no tempo Unix epoch.

Defina também qualquer um dos seguintes parâmetros para refinar os resultados:

- `maxResults` – O número máximo de resultados a serem retornados em uma solicitação. Remete ao padrão de `20` resultados.
- `nextToken` – Um token de paginação retornado de uma chamada anterior a essa operação.
- `timeOrdering` — A ordem a ser aplicada aos valores retornados: `ASCENDING` ou `DESCENDING`.
- `qualities` – A qualidade sob a qual pautar e filtrar os resultados: `GOOD`, `BAD`, ou `UNCERTAIN`.

> **Note**
>
> A GetAssetPropertyAggregatesoperação retorna um TQV com um formato diferente das outras operações descritas nesta seção. A estrutura `value` contém um campo para cada um dos `aggregateTypes` na solicitação. O `timestamp` contém a hora na qual a agregação ocorreu, em segundos, no horário Unix epoch.

Agregados para uma propriedade de ativo ()AWS CLI

Para consultar agregados para uma propriedade do ativo ()AWS CLI

1. Execute o seguinte comando para obter os agregados para a propriedade de ativo: Este comando consulta média e soma, com resolução de 1 hora para um intervalo específico de 1 hora. Substitua *`asset-id`* pela ID do ativo e *`property-id`* pela ID da propriedade. Substitua os parâmetros pelos agregados e intervalo a ser consultado.

   ```
   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
   ```

   A operação retorna uma resposta contendo os TQVs históricos da propriedade no formato a seguir: A resposta inclui apenas os agregados solicitados.

   ```
   {
     "aggregatedValues": [
   ```

```
    {
      "timestamp": Number,
      "quality": "String",
      "value": {
        "average": Number,
        "count": Number,
        "maximum": Number,
        "minimum": Number,
        "standardDeviation": Number,
        "sum": Number
      }
    }
  ],
  "nextToken": "String"
}
```

2. Se existirem mais entradas de valor, você poderá passar o token de paginação do `nextToken` campo para uma chamada subsequente para a GetAssetPropertyAggregatesoperação.

AWS IoT SiteWise linguagem de consulta

Com a operação da ExecuteQueryAPI de recuperação de AWS IoT SiteWise dados, você pode recuperar informações sobre definições estruturais declarativas e os dados de série temporal associados a elas, a partir do seguinte:

- modelos
- ativos
- medidas
- métricas
- transforma-se
- agregados

Isso pode ser feito com instruções de consulta semelhantes a SQL, em uma única solicitação de API.

> **Note**
>
> Esse recurso está disponível em todas as regiões em que ambos AWS IoT SiteWise AWS IoT TwinMaker estão disponíveis, exceto AWS GovCloud (Oeste dos EUA).

Tópicos

Pré-requisitos

AWS IoT SiteWise requer permissões de integração para que AWS IoT TwinMaker possa organizar e modelar dados industriais.

Antes de recuperar informações sobre modelos, ativos, medições, métricas, transformações e agregados, certifique-se de que os seguintes pré-requisitos sejam atendidos:

- Funções vinculadas ao serviço para ambas AWS IoT SiteWise e AWS IoT TwinMaker configuração em seu. Conta da AWS Para obter mais informações sobre funções vinculadas a serviços, consulte Usando funções vinculadas a serviços no Guia do Usuário do IAM.
- Uma AWS IoT SiteWise integração habilitada para sua função do IAM. Para ter mais informações, consulte Integração do AWS IoT SiteWise e do AWS IoT TwinMaker.
- Um AWS IoT TwinMaker espaço de trabalho com ID `IoTSiteWiseDefaultWorkspace` em sua conta na região. Para obter mais informações, consulte Utilização do IoTSiteWiseDefaultWorkspace no Guia do usuário do AWS IoT TwinMaker .
- Os modos de preços de pacote padrão ou em camadas estão habilitados. AWS IoT TwinMaker Para obter mais informações, consulte Alternar os modos de AWS IoT TwinMaker preços no Guia AWS IoT TwinMaker do usuário.

Referência da linguagem de consulta

AWS IoT SiteWise suporta uma linguagem de consulta avançada para trabalhar com seus dados. Os tipos de dados, operadores, funções e construções disponíveis são descritos nos tópicos a seguir.

Consulte Consultas de exemplo para escrever consultas com a linguagem de AWS IoT SiteWise consulta.

Tópicos

- Operadores lógicos
- Operadores de comparação
- Consultas de exemplo

Entendendo as visualizações

Esta seção fornece informações para ajudá-lo a entender as visualizações AWS IoT SiteWise, como metadados do processo e dados de telemetria.

As tabelas a seguir fornecem os nomes das visualizações e as descrições das visualizações.

Modelo de dados

Exibir nome	Descrição da visualização
asset	Contém informações sobre a derivação do ativo e do modelo.
propriedade_ativo	Contém informações sobre a estrutura da propriedade do ativo.
série raw_time_series	Contém os dados históricos da série temporal.
série_valor_tempo_mais recente	Contém o valor mais recente da série temporal.
agregados_pré-computados	Contém os valores agregados da propriedade do ativo calculados automaticamente. Eles são um conjunto de métricas básicas calculadas em vários intervalos de tempo.

As visualizações a seguir listam os nomes das colunas para consultas junto com os dados de amostra.

Visualizar: ativo

id_do ativo	nome_do_ativo	descrição_do_ativo	id_modelo_de_ativo
88898498-0b8b-42b5-bf57-16180bc3d3a0	WindTurbine A	WindTurbine Ativo A	17847250-5bf0-4f74-b775-cc03f05e7cb8

id_do ativo	nome_do_ativo	descrição_do_ativo	id_modelo_de_ativo
17847250-5bf0-4f74-b775-cc03f05e7cb8	Modelo de ativos de turbina eólica	Representa uma turbina em um parque eólico.	

Exibir: asset_property

id_do_propriedade	id_do ativo	nome_do_propriedade	tipo_dados_de_propriedade	alias de propriedade_de_propriedade	id_de_modelo_composto do ativo
b29be434-b000-4d74-b809-75287d83bcd6	88898498-0b8b-42b5-bf57-16180bc3d3a0	temperatura do motor	Double	`Rochester 2/44///Line-5/Bus-2/Machine-5/Temperature`	
3b458f00-24e7-458a-b4e8-c6026eff654a	88898498-0b8b-42b5-bf57-16180bc3d3a0	direção do vento	Double	`/company/windfarm/3/turbine/7/winddirection`	2f458n00-56e7-458h-b4e8-c6026eff985g

Visualização: RAW_TIME_SERIES

id_do ativo	id_do_propriedade	alias de propriedade_de_propriedade	timestamp do evento	qualidade	valor_booleano	valor_int	valor_duplo	valor_string
88898498-0b8b-42b5-bf57-161	b29be434-b000-4d74-b809-752	`Rochester 2/44/// Line-5/`	1575219600	BOM			115,0	

id_do ativo	id_do_pro priedade	alias de proprieda de_de_pro priedade	timestamp do evento	qualidade	valor_boo leano	valor_int	valor_dup lo	valor_str ing
80bc3d3a	87d83bcd	Bus-2/ Machine -5/ Temper ature						
88898498 0b8b-42b5 - bf57-161 80bc3d3a	3b458f00- 24e7-458a -b4e8- c60 26eff654a	/ company, windfarr 3/ turbine /7/ winddi rection	15752193 7	BOM			348,75	

> **Note**
>
> Você deve incluir uma cláusula de filtro na `event_timestamp` coluna para consultar a `raw_time_series` exibição. Esse é um filtro obrigatório e a consulta falhará sem ele.
>
> Example consulta
>
> ```
> SELECT event_timestamp, double_value FROM raw_time_series WHERE event_timestamp
>  > 1234567890
> ```

Exibir: LATEST_VALUE_TIME_SERIES

id_do ativo	id_do_propriedade	alias de propriedade_de_propriedade	timestamp do evento	qualidade	valor_booleano	valor_int	valor_duplo	valor_string
88898498-0b8b-42b5-bf57-16180bc3d3a	3b458f00-24e7-458a-b4e8-c6026eff654a	/company/windfarm/3/turbine/7/winddirection	1575219600	BOM			355,39	

Exibir: precomputed_aggregates

id_do ativo	id_do_propriedade	alias de propriedade_de_propriedade	timestamp do evento	resolução	valor_soma	valor_contagem	valor_medio	valor_maximo	valor_minimo	stdev_value
888984-0b8b-42-bf57-1680bc3d	b29be4-b000-4c-b809-7587d83b	Rochester/44//Line-5/Bus-2/Machine-5/Temperature	1575215200	15 minutos	1105,48	15	73,4	80,6	68	3.64

Tipos de dados compatíveis

AWS IoT SiteWise a linguagem de consulta oferece suporte aos seguintes tipos de dados.

Visualizar: ativo

Tipo de dados	Descrição
`STRING`	Uma sequência de caracteres de comprimento máximo de 1024 bytes.
`INTEGER`	Um inteiro assinado de 32 bits com um intervalo de. `-2,147,483,648 to 2,147,483,647`
`DOUBLE`	Um número de ponto flutuante com alcance `-10^100 to 10^100` e precisão `IEEE 754` dupla.
`BOOLEAN`	`true` ou `false`.

> **Note**
>
> Os dados de precisão dupla não são exatos. Alguns valores não são convertidos exatamente e não representarão todos os números reais devido à precisão limitada. Os dados de ponto flutuante na consulta podem não ter o mesmo valor representado internamente. O valor é arredondado se a precisão de um número de entrada for muito alta.

Recupere dados com uma instrução SELECT

A `SELECT` instrução é usada para recuperar dados de uma ou mais visualizações. AWS IoT SiteWise suporta uma das visões `JOIN` implícitas. Você pode listar as visualizações a serem unidas (na `FROM` cláusula da `SELECT` declaração) usando vírgulas para separá-las.

Example

Use a seguinte `SELECT` declaração:

```
SELECT select_expr [, ...]
[ FROM from_item [, ...] ]
[ WHERE [LIKE condition ESCAPE condition] ]
```

No exemplo anterior, a `LIKE` cláusula especifica as condições de pesquisa e filtragem usando curingas. AWS IoT SiteWise suporta `percentage (%)` como personagem curinga.

Example para usar `%` em uma condição:

```
Prefix search: String%
Infix search: %String%
Suffix search: %String
```

Example para pesquisar um ativo:

```
SELECT asset_name, asset_description FROM asset WHERE asset_name LIKE 'Wind%'
```

Example para pesquisar um ativo usando uma condição ESCAPE:

```
SELECT asset_name, asset_description FROM asset WHERE asset_name LIKE 'room\%' ESCAPE
 '\'
```

Operadores lógicos

AWS IoT SiteWise suporta os seguintes operadores lógicos.

Operadores lógicos

Operador	Descrição	Exemplo
`AND`	`TRUE`se ambos os valores forem verdadeiros	a `AND` b

Se a ou b for`FALSE`, a expressão anterior será avaliada como falsa. Para que um `AND` operador seja avaliado como verdadeiro, tanto a quanto b devem ser verdadeiros.

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 comparação

AWS IoT SiteWise suporta os seguintes operadores de comparação.

Operadores lógicos

Operador	Descrição
<	Menor que
>	Maior que
<=	Menor ou igual a
>=	Maior ou igual a
=	Igual
!=	Not equal

Consultas de exemplo

Filtragem de metadados

O exemplo a seguir é para filtragem de metadados com uma `SELECT` instrução com a linguagem 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%'
```

Filtragem de valores

Veja a seguir um exemplo de filtragem de valores usando uma `SELECT` instrução com a linguagem 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
```

Interagindo com outros serviços AWS

AWS IoT SiteWise pode publicar dados de ativos no agente de mensagens de publicação e assinatura do AWS IoT MQTT, para que você possa interagir com seus dados de ativos de outros serviços. AWS AWS IoT SiteWise atribui a cada propriedade do ativo um tópico MQTT exclusivo que você pode usar para rotear seus dados de ativos para outros AWS serviços usando as regras AWS IoT principais. Por exemplo, você pode configurar as regras AWS IoT principais para realizar as seguintes tarefas:

- Identificar falhas no equipamento e notificar o pessoal adequado enviando dados para o AWS IoT Events.
- Criar um histórico dos dados de ativos selecionados para uso em soluções de software externas enviando dados para o Amazon DynamoDB.
- Gerar relatórios semanais acionando uma função do AWS Lambda.

Você pode seguir um tutorial que percorre as etapas necessárias para configurar uma regra que armazena valores de propriedade no DynamoDB. Para ter mais informações, consulte Publicar atualizações de valor de propriedade no Amazon DynamoDB.

Para obter mais informações sobre como configurar uma regra, consulte Rules no AWS IoT Developer Guide.

Você também pode voltar a consumir dados de outros AWS serviços AWS IoT SiteWise. Para ingerir dados por meio da ação de AWS IoT SiteWise regra, consulteIngestão de dados usando regras AWS IoT Core.

Tópicos

- Noções básicas sobre os tópicos MQTT das propriedades de ativos
- Trabalhar com notificações de propriedades de ativos
- Exporte dados para o Amazon S3 com notificações de propriedades de ativos
- Integração com o Grafana
- Integração do AWS IoT SiteWise e do AWS IoT TwinMaker
- Detecção de anomalias em equipamentos com o Amazon Lookout for Equipment

Noções básicas sobre os tópicos MQTT das propriedades de ativos

Cada propriedade de ativo tem um caminho de tópico MQTT exclusivo no formato a seguir.

```
$aws/sitewise/asset-models/assetModelId/assets/assetId/properties/propertyId
```

> **Note**
>
> AWS IoT SiteWise não suporta o caractere curinga do filtro de tópicos # (de vários níveis) no mecanismo de regras AWS IoT principais. Use o caractere curinga + (de nível único). Por exemplo, use o filtro de tópico a seguir para fazer a correspondência de todas as atualizações de um modelo de ativo específico.
>
> ```
> $aws/sitewise/asset-models/assetModelId/assets/+/properties/+
> ```
>
> Para saber mais sobre caracteres curinga de filtro de tópico, consulte Tópicos no Guia do desenvolvedor da Core AWS IoT .

Trabalhar com notificações de propriedades de ativos

Você pode ativar as notificações de propriedades para publicar atualizações de dados de ativos e AWS IoT Core, em seguida, executar consultas nos seus dados. Com notificações de propriedades de ativos, AWS IoT SiteWise fornece um AWS CloudFormation modelo que você pode usar para exportar AWS IoT SiteWise dados para o Amazon S3.

> **Note**
>
> Os dados do ativo são enviados AWS IoT Core sempre que são recebidos AWS IoT SiteWise, independentemente de o valor ter sido alterado.

Tópicos

- Habilitar notificações de propriedade de ativos (console)
- Habilitando notificações de propriedades de ativos (AWS CLI)
- Consultar mensagens de notificação de propriedade de ativos

Habilitar notificações de propriedade de ativos (console)

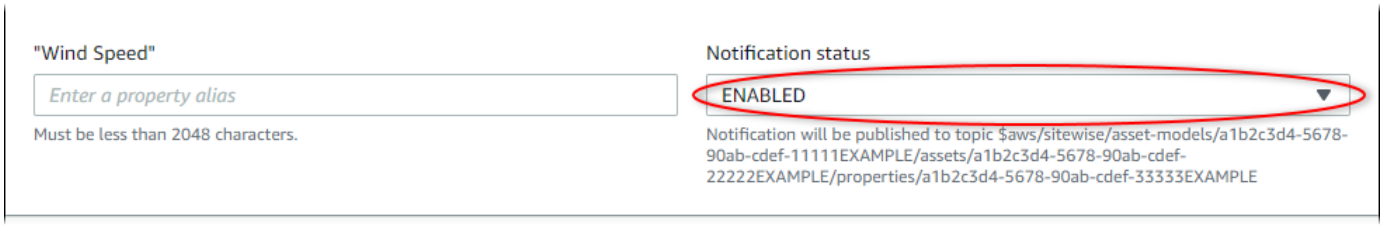
Por padrão, AWS IoT SiteWise não publica atualizações de valores de propriedades. Você pode usar o AWS IoT SiteWise console para ativar as notificações para uma propriedade do ativo.

Como habilitar ou desabilitar notificações de propriedade de um ativo (console)

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Ativos.
3. Escolha o ativo para habilitar as notificações de uma propriedade.

> **Tip**
>
> Você pode escolher o ícone de seta para expandir uma hierarquia de ativos para localizar seu ativo.

4. Selecione a opção Editar.
5. Para o Status da notificação da propriedade de ativo, escolha HABILITADO.



   Você também pode escolher DESABILITADO para desabilitar notificações para a propriedade do ativo.

6. Selecione Salvar.

Habilitando notificações de propriedades de ativos (AWS CLI)

Por padrão, AWS IoT SiteWise não publica atualizações de valores de propriedades. Você pode usar o AWS Command Line Interface (AWS CLI) para ativar ou desativar as notificações de uma propriedade do ativo.

Para executar este procedimento, é necessário saber quais são o `assetId` do ativo e o `propertyId` da propriedade. Você também pode usar o ID externo. Se você criou um ativo e não

o conheceassetId, use a ListAssetsAPI para listar todos os ativos de um modelo específico. Use a DescribeAssetoperação para visualizar as propriedades do seu ativo, incluindo IDs de propriedade.

Use a UpdateAssetPropertyoperação para ativar ou desativar as notificações de uma propriedade do ativo. Especifique os seguintes parâmetros:

- `assetId` – a ID do ativo.
- `propertyId` – a ID da propriedade do ativo.
- `propertyNotificationState` – o estado de notificação do valor da propriedade: `ENABLED` ou `DISABLED`.
- `propertyAlias` – o alias da propriedade. Especifique o alias existente da propriedade ao atualizar o estado da notificação. Se você omitir esse parâmetro, o alias existente da propriedade será removido.

Como habilitar ou desabilitar notificações para a propriedade de um ativo (CLI)

1. Execute o seguinte comando para recuperar o alias da propriedade de ativo. Substitua *`asset-id`* pela ID do ativo e *`property-id`* pela ID da propriedade.

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

   A operação retorna uma resposta que contém os detalhes da propriedade do ativo no formato a seguir. O alias da propriedade está em `assetProperty.alias` no 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. Execute o seguinte comando para habilitar notificações para a propriedade de ativo. Substitua *property-alias* pelo alias da propriedade da resposta do comando anterior ou omita `--property-alias` para atualizar a propriedade sem um alias.

```
aws iotsitewise update-asset-property \
  --asset-id asset-id \
  --property-id property-id \
  --property-notification-state ENABLED \
  --property-alias property-alias
```

   Você também pode passar `--property-notification-state DISABLED` para desabilitar notificações para a propriedade de ativo.

Consultar mensagens de notificação de propriedade de ativos

Para consultar notificações de propriedades de ativos, crie AWS IoT Core regras compostas por instruções SQL.

AWS IoT SiteWise publica atualizações de dados de propriedades de ativos no AWS IoT Core no seguinte 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 estrutura na `values` lista é uma estrutura timestamp-quality-value (TQV).

- O `timestamp` contém o horário Unix epoch atual em segundos, com correção em nanossegundos.
- `quality` contém uma das seguintes strings, que indicam a qualidade do ponto de dados:
  - `GOOD` – os dados não são afetados por nenhum problema.
  - `BAD` – os dados são afetados por um problema, como a falha do sensor.
  - `UNCERTAIN` – os dados são afetados por um problema, como a imprecisão do sensor.
- O `value` contém um dos campos a seguir, a depender do tipo de propriedade:
  - `booleanValue`
  - `doubleValue`
  - `integerValue`
  - `stringValue`

Para analisar valores fora da matriz `values`, é necessário usar consultas complexas de objetos aninhados nas instruções SQL das regras. Para obter mais informações, consulte NConsultas de objeto aninhado no AWS IoT Guia do desenvolvedor ou consulte o Publicar atualizações de valor de propriedade no Amazon DynamoDB tutorial para ver um exemplo específico de análise de mensagens de notificação de propriedade de ativos.

Example Exemplo de consulta para extrair a matriz de valores

A instrução a seguir demonstra como consultar a matriz de valores de propriedade atualizados para uma propriedade específica de tipo duplo em todos os ativos com essa propriedade.

```
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'
```

A instrução de consulta de regra anterior produz dados no formato a seguir.

```
{
  "windspeed": [
    26.32020195042838,
    26.282584572975477,
    26.352566977372508,
    26.283084346171442,
    26.571883739599322,
    26.60684140743005,
    26.628738636715045,
    26.273486932802125,
    26.436379105473964,
    26.600590095377303
  ]
}
```

Example Exemplo de consulta para extrair um único valor

A instrução a seguir demonstra como consultar o primeiro valor da matriz de valores de propriedade para uma propriedade específica de tipo duplo em todos os ativos com essa propriedade.

```
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'
```

A instrução de consulta de regra anterior produz dados no formato a seguir.

```
{
  "windspeed": 26.32020195042838
}
```

> **Important**
>
> Essa instrução de consulta de regra ignora atualizações de valor diferentes da primeira em cada lote. Cada lote pode conter até 10 valores. Se você precisar incluir os valores restantes, deverá configurar uma solução mais complexa para gerar valores de propriedade do ativo para outros serviços. Por exemplo, você pode configurar uma regra com uma AWS Lambda ação para republicar cada valor na matriz em outro tópico e configurar outra regra para consultar esse tópico e publicar cada valor na ação de regra desejada.

Exporte dados para o Amazon S3 com notificações de propriedades de ativos

Você pode exportar dados recebidos AWS IoT SiteWise para um bucket do Amazon S3 em sua conta. Você pode fazer backup de seus dados em um formato que permite criar relatórios históricos ou analisar os dados com métodos complexos.

> **Note**
>
> AWS IoT SiteWise também oferece suporte ao armazenamento de nível frio que permite salvar dados em um bucket Amazon S3 gerenciado pelo cliente. Para obter mais informações sobre os níveis de armazenamento compatíveis, consulte Gerenciando o armazenamento de dados.

AWS IoT SiteWise fornece esse recurso como um AWS CloudFormation modelo. Quando você cria uma pilha a partir do modelo, AWS CloudFormation cria os AWS recursos necessários para transmitir dados de entrada AWS IoT SiteWise para um bucket do S3.

Em seguida, o bucket do S3 recebe todos os dados da propriedade do ativo enviados das mensagens de atualização do valor da AWS IoT SiteWise propriedade. O bucket do S3 também recebe seus metadados de ativos, que incluem nomes de ativos e propriedades e outras informações.

Para obter mais informações sobre como habilitar mensagens de atualização de valor de propriedade para as propriedades do ativo para exportação para o Amazon S3, consulte Interagindo com outros serviços AWS.

Esse recurso armazena seus dados de propriedade de ativos e metadados de ativos no formato Apache Parquet no Amazon S3. O Parquet é um formato de dados colunar que economiza espaço e permite consultas mais rápidas em comparação com formatos orientados por linha, como o JSON.

> **Note**
>
> Quando esse recurso recupera metadados de ativos, ele oferece suporte a até aproximadamente 1.500 propriedades de ativos. Essa limitação se aplica somente aos metadados de ativos. Essa limitação não se aplica ao número de ativos compatíveis quando o recurso exporta dados de propriedade de ativos.

O nome de cada recurso inclui um prefixo que você pode personalizar ao criar a pilha. Os recursos incluem:

- Um bucket do Amazon S3
- AWS Lambda funções
- Uma AWS IoT Core regra
- AWS Identity and Access Management funções
- Um stream do Amazon Data Firehose
- Um AWS Glue banco de dados

Para obter uma lista completa, consulte Recursos criados usando o modelo.

> **Important**
>
> Você será cobrado pelos recursos que esse AWS CloudFormation modelo cria e consome. Essas cobranças incluem armazenamento e transferência de dados para vários AWS serviços.

Tópicos

Crie a AWS CloudFormation pilha

Você deve criar uma pilha AWS CloudFormation para exportar seus dados de ativos para o Amazon S3.

Para exportar dados para o Amazon S3

1. Abra o Modelo do AWS CloudFormation e faça login no AWS Management Console.
2. Na página Create stack (Criar pilha) escolha Next (Próximo) na parte inferior da página.
3. Na página Especificar detalhes da pilha, insira um BucketNamepara o bucket do S3 que esse modelo cria para receber dados do ativo. O nome do bucket deve ser exclusivo globalmente. Para obter mais informações, consulte as Regras para nomear buckets no Manual do usuário do Amazon Simple Storage Service.
4. (Opcional) Altere qualquer um dos outros parâmetros do modelo:
   - GlobalResourcePrefix – um prefixo para nomes de recursos globais, como funções do IAM criados usando esse modelo.
   - LocalResourcePrefix – um prefixo para nomes de recursos criados usando esse modelo na região atual.

   > **Note**
   >
   > Se você criar esse modelo várias vezes, talvez seja necessário alterar os parâmetros de nome do bucket e prefixo do recurso para evitar conflitos de nome de recurso.
5. Escolha Avançar.
6. Na página Configurar opções de pilha, selecione Avançar.
7. Na parte inferior da página, marque a caixa de seleção que indica I acknowledge that AWS CloudFormation might create IAM resources (Reconheço que o [2] pode criar recursos do IAM).
8. Selecione Criar pilha.

   A pilha leva alguns minutos para ser criada. Se a pilha falhar ao ser criada, sua conta pode ter permissões insuficientes ou você pode ter inserido um nome de bucket que já existe. Use as etapas a seguir para excluir a pilha e tente novamente:

   a. Escolha Delete (Excluir) no canto superior direito.

A pilha leva alguns minutos para ser excluída.

> **Note**
>
> AWS CloudFormation não exclui buckets ou grupos de CloudWatch registros do S3. Você pode excluir esses recursos nos consoles desses serviços.

b. Se a pilha não puder ser excluída, escolha Delete (Excluir) novamente.

c. Se a pilha não for excluída novamente, siga as etapas no AWS CloudFormation console para ignorar os recursos que não foram excluídos e tente novamente.

9. Depois que a AWS CloudFormation pilha for criada com sucesso, siga o próximo procedimento para explorar os dados da propriedade do seu ativo no Amazon S3.

> **Important**
>
> Depois de criar a pilha, você pode ver os novos recursos em sua AWS conta. O recurso pode parar de funcionar corretamente se você os excluir ou modificar. É recomendável não modificar esses recursos, a menos que você queira parar de enviar dados para o bucket ou queira personalizar esse recurso.

Visualize seus dados no Amazon S3

Depois de criar o recurso, você pode exibir seus dados de propriedades de ativos e metadados de ativos no .

> **Note**
>
> Os metadados de ativos são atualizados a cada seis horas. Pode ser necessário aguardar até seis horas para ver os metadados de ativos aparecerem no bucket do S3.

Esse recurso armazena dados de propriedades de ativos nas colunas a seguir, onde cada linha contém um ponto de dados:

- type – o tipo de notificação de propriedade (`PropertyValueUpdate`).
- asset_id – o ID do ativo que recebeu um ponto de dados.

- asset_property_id – o ID da propriedade que recebeu um ponto de dados para o ativo.
- time_in_seconds – o horário em que os dados foram recebidos, expresso em segundos no tempo epoch do Unix.
- offset_in_nanos – deslocamento em nanossegundos de `timeInSeconds`.
- asset_property_quality – a qualidade do ponto de dados: `GOOD`, `UNCERTAIN` ou `BAD`.
- asset_property_value – o valor do ponto de dados.
- asset_property_data_type –o tipo de dados da propriedade do ativo: `boolean`, `double` `integer`, ou `string`.

Esse recurso armazena metadados de ativos nas seguintes colunas, onde cada linha contém uma propriedade do ativo:

- asset_id – o ID do ativo.
- asset_name – o nome do ativo.
- asset_model_id – o ID do modelo do ativo.
- asset_property_id – o ID da propriedade do ativo.
- asset_property_name – o nome da propriedade do ativo.
- asset_property_data_type – o tipo de dados da propriedade do ativo: `BOOLEAN`, `DOUBLE`, `INTEGER`, or `STRING`.
- asset_property_unit – a unidade da propriedade do ativo.
- asset_property_alias – o alias da propriedade do ativo.

Para visualizar seus AWS IoT SiteWise dados no Amazon S3

1. Navegue até o console do Amazon S3.
2. Na lista de buckets, escolha o bucket com o nome escolhido quando você criou o modelo.
3. No bucket, escolha uma das seguintes pastas:
   - `asset-property-updates`— Essa pasta contém dados de propriedades de ativos exportados de AWS IoT SiteWise.
   - `asset-metadata`— Essa pasta contém detalhes do ativo exportados de AWS IoT SiteWise.
4. Escolha o objeto que deseja visualizar.
5. Na página do objeto, faça o seguinte:

a. Escolha a guia Select from (Selecionar de).

   Neste painel, você pode visualizar registros de arquivos Parquet.

b. Em File format (Formato do arquivo), escolha Parquet.

c. Escolha Show file preview (Mostrar visualização do arquivo) para mostrar o conteúdo do arquivo no formato JSON.

> **Note**
>
> Se novos dados não aparecerem no bucket, verifique se você habilitou as notificações de atualização de valor das propriedades do ativo. Para ter mais informações, consulte Interagindo com outros serviços AWS.

Para obter mais informações sobre como analisar os dados de ativos armazenados no bucket do S3, consulte Analise os dados exportados com o Amazon Athena.

Analise os dados exportados com o Amazon Athena

Depois de ter seus dados de propriedade de ativos no Amazon S3, você pode usar vários AWS serviços para gerar relatórios ou analisar e consultar seus dados:

- Execute consultas SQL em seus dados usando o Amazon Athena.
- Execute análise de big data usando Amazon EMR.
- Pesquise e analise seus dados usando o Amazon OpenSearch Service.

Você pode encontrar outros AWS serviços que podem interagir com seus dados no Amazon S3 listados em Analytics no. AWS Management Console

> **Note**
>
> A pilha cria um AWS Glue banco de dados para formatar os dados da propriedade do ativo. Não é possível consultar esse banco de dados para obter dados de ativos. Siga as etapas desta seção para criar um AWS Glue banco de dados que você possa consultar.

Neste tutorial, você aprende como configurar os pré-requisitos para usar o Amazon Athena e como usar o Athena para executar consultas SQL em seus dados de ativos exportados. AWS IoT SiteWise Para consultar dados com o Athena, você deve primeiro preencher o AWS Glue Data Catalog com os dados do seu ativo. O Catálogo de Dados contém bancos de dados e tabelas, e o Athena pode acessar dados no Catálogo de Dados. Você pode criar um AWS Glue rastreador que atualize regularmente o Catálogo de Dados com seus dados de ativos exportados.

Tópicos

Como configurar um rastreador para preencher o AWS Glue Data Catalog

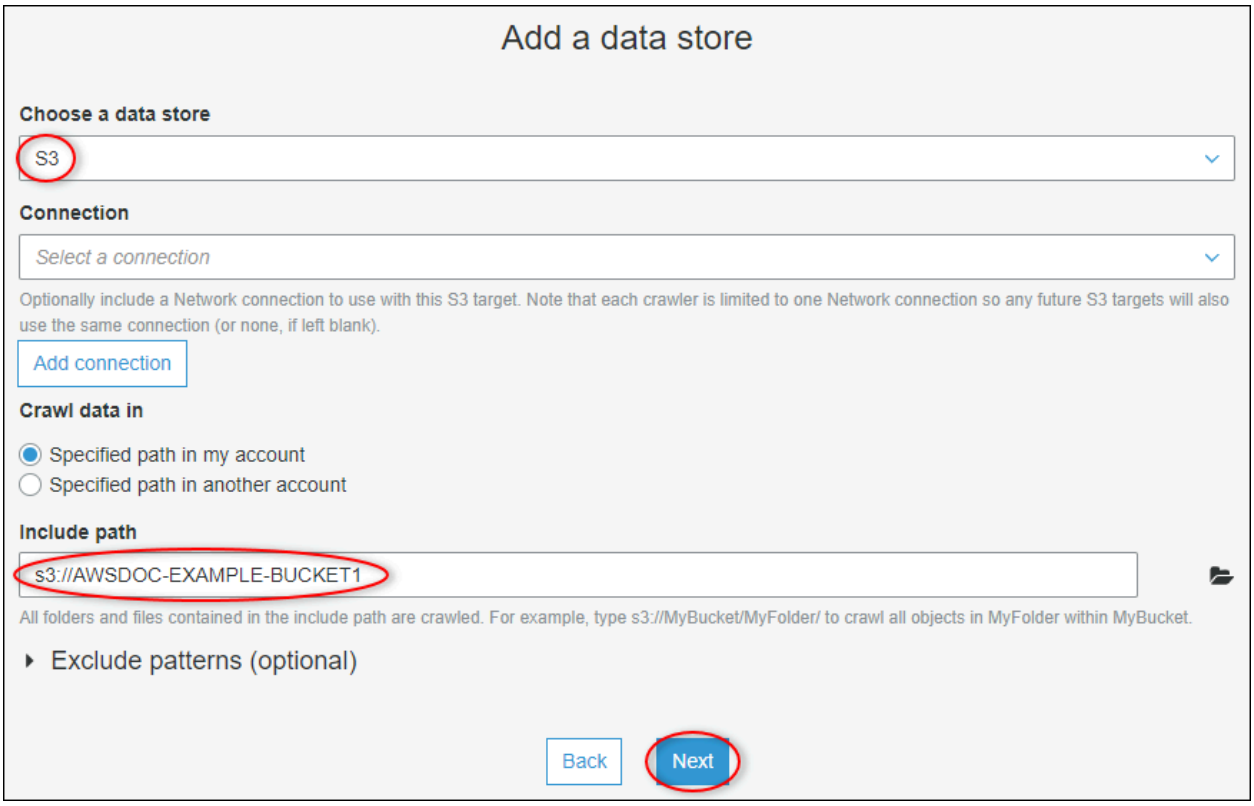
AWS Glue rastreadores rastreiam armazenamentos de dados para preencher tabelas no. AWS Glue Data Catalog Neste procedimento, você cria e executa um AWS Glue rastreador para seu bucket do S3 que contém dados de ativos exportados. O rastreador cria uma tabela para atualizações de propriedades de ativos e uma tabela para metadados de ativos. Depois, você poderá executar consultas SQL nessas tabelas com o Athena. Para obter mais informações, consulte Populating the AWS Glue Data Catalog and Defining crawlers (Preencher e Definir rastreadores) no AWS Glue Developer Guide.

Para criar um AWS Glue rastreador

1. Navegue até o console do AWS Glue.
2. No painel de navegação, escolha Rastreadores.
3. Escolha Adicionar crawler.
4. Na página Adicionar rastreador, faça o seguinte:
    a. Insira um nome para o rastreador, como **`IoTSiteWiseDataCrawler`** e depois, escolha Próximo.
    b. Em Tipo de origem do rastreador, escolha Armazenamentos de dados e depois, escolha Próximo.
    c. Na página Adicionar um armazenamento de dados, faça o seguinte:
        i. Em Escolher um armazenamento de dados, escolha S3.

ii. Em Incluir caminho, insira **`s3://DOC-EXAMPLE-BUCKET1`** para adicionar o bucket de dados de ativos como um armazenamento de dados. Substitua DOC-EXAMPLE-BUCKET1 pelo nome do bucket que você escolheu ao criar a pilha.

iii. Escolha Próximo.



d. Na página Adicionar outra página de armazenamento de dados, escolha Não e depois, escolha Próximo.

e. Na página Choose an IAM role (Escolher um perfil do IAM), faça o seguinte:

i. Para criar uma nova função de serviço que permita AWS Glue acessar o bucket do S3, escolha Criar uma função do IAM.

ii. Insira um sufixo para o nome da função, como **`IoTSiteWiseDataCrawler`**.

iii. Escolha Próximo.

f. Em Frequência, escolha Por hora e depois, escolha Próximo. O rastreador atualiza as tabelas com novos dados em todas as execuções, portanto, é possível escolher uma frequência adequada para o seu caso de uso.

g. Na página Configurar saída do rastreador, faça o seguinte:

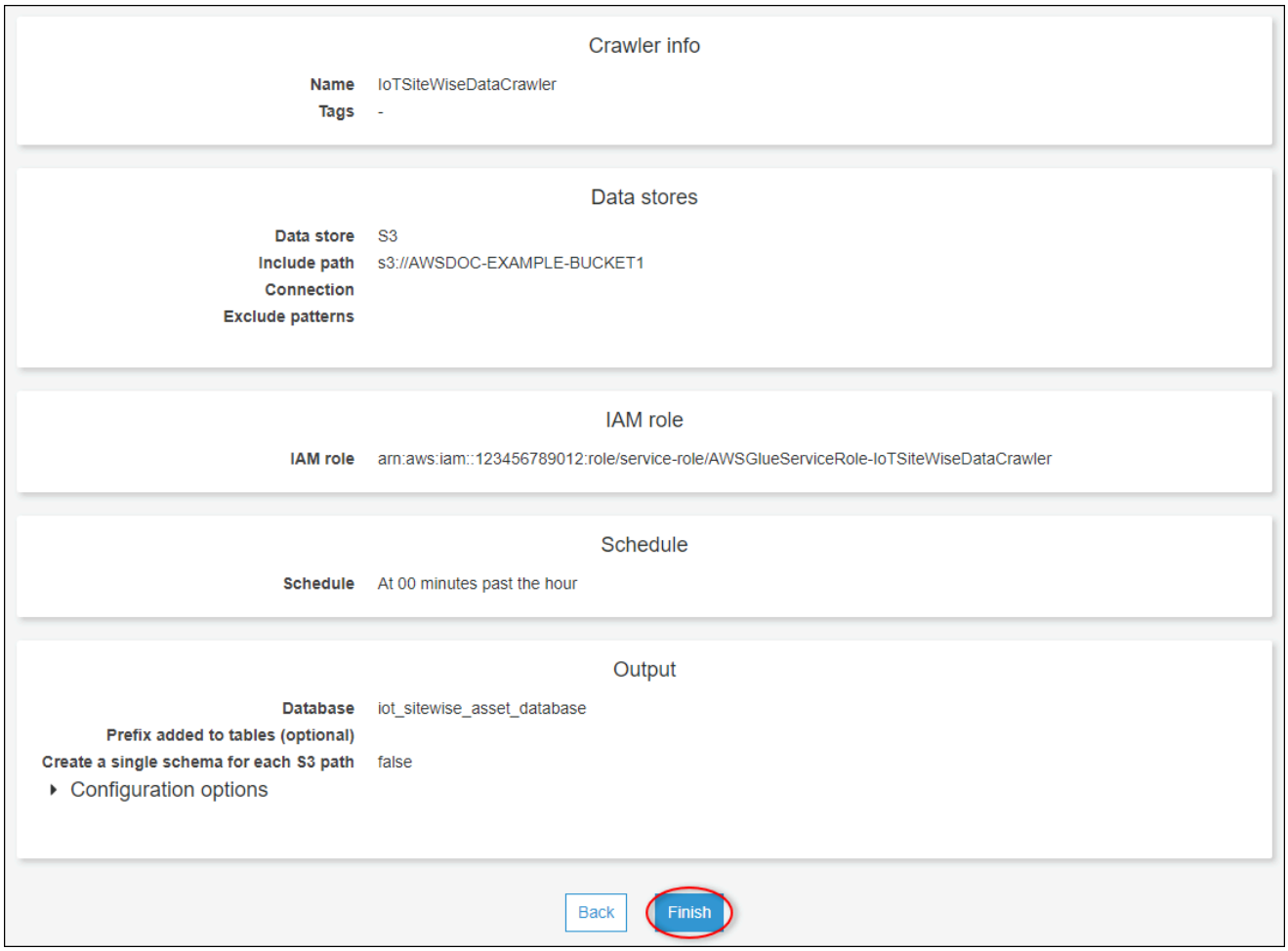
i. Escolha Adicionar banco de dados para criar um AWS Glue banco de dados para seus dados de ativos.

ii. Insira um nome para o banco de dados, como **`iot_sitewise_asset_database`**.

iii. Escolha Criar.

iv. Escolha Próximo.

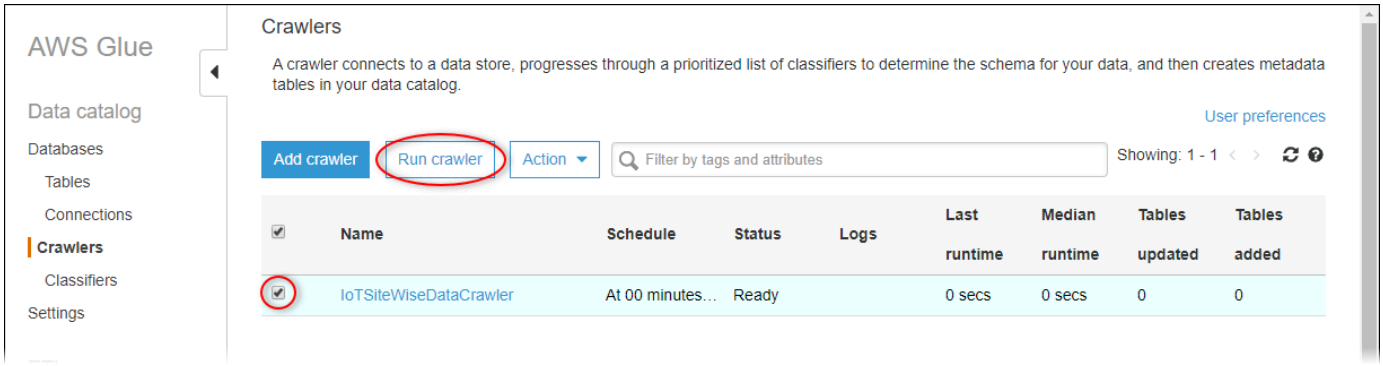
h. Revise os detalhes do rastreador e depois escolha Concluir.



Por padrão, o novo rastreador não é executado imediatamente. É necessário executá-lo manualmente ou aguardar até que ele seja executado no agendamento configurado.

Como executar um rastreador

1. Na página Rastreadores, marque a caixa de seleção para o novo rastreador e escolha Executar rastreador.



2. Aguarde até que o rastreador termine e apresente um status Pronto.

   O rastreador pode levar alguns minutos para ser executado e o status é atualizado automaticamente.

3. No painel de navegação, selecione Tabelas.

   Você verá duas novas tabelas: asset_metadata e asset_property_updates.

Consulta de dados com o Athena

Athena descobre automaticamente suas tabelas de dados de ativos no. AWS Glue Data Catalog Para executar consultas na interseção dessas tabelas, crie uma exibição, que é uma tabela de dados lógica. Para obter mais informações, consulte Working with views (Trabalhando com visualizações) no Amazon Athena User Guide.

Depois de criar uma exibição que combine dados e metadados de propriedades de ativos, é possível executar consultas que geram valores de propriedades com ativos e nomes de propriedades anexados. Para obter mais informações, consulte Executar consultas SQL usando o Amazon Athena no Manual do usuário do Amazon Athena.

Como consultar dados de ativos com o Athena.

1. Navegue até o Athena console (console do Athena).

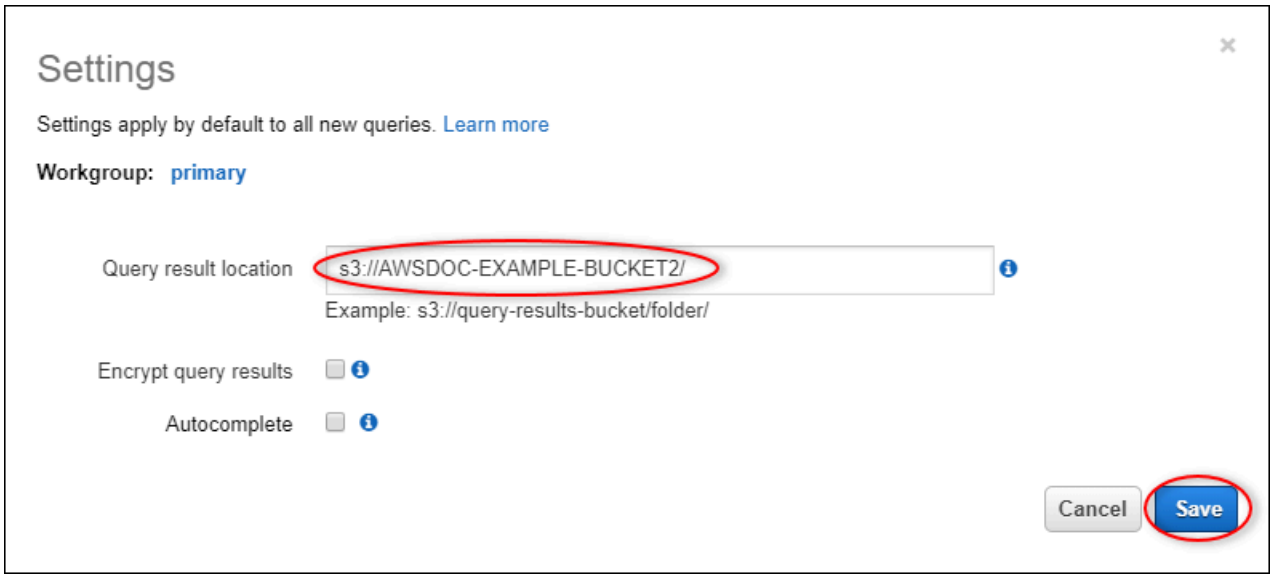
   Se a página Conceitos básicos for exibida, escolha Começar a usar.

2. Se você estiver usando o Athena pela primeira vez, execute os seguintes passos para configurar um bucket do S3 e obter os resultados da consulta. O Athena armazena os resultados de suas consultas nesse bucket.

> **Important**
>
> Use um bucket diferente do bucket de dados de ativos, para que o rastreador criado anteriormente não rastreie os resultados da consulta. Recomendamos criar um bucket para usar somente resultados de consultas do Athena. Para obter mais informações, consulte Como criar um bucket do S3? no Guia do usuário do Amazon Simple Storage Service.

a. Escolha Configurações.

b. Em Query result location (Local do resultado da consulta), insira o bucket do S3 para os resultados de consultas do Athena. O bucket deve terminar com /.

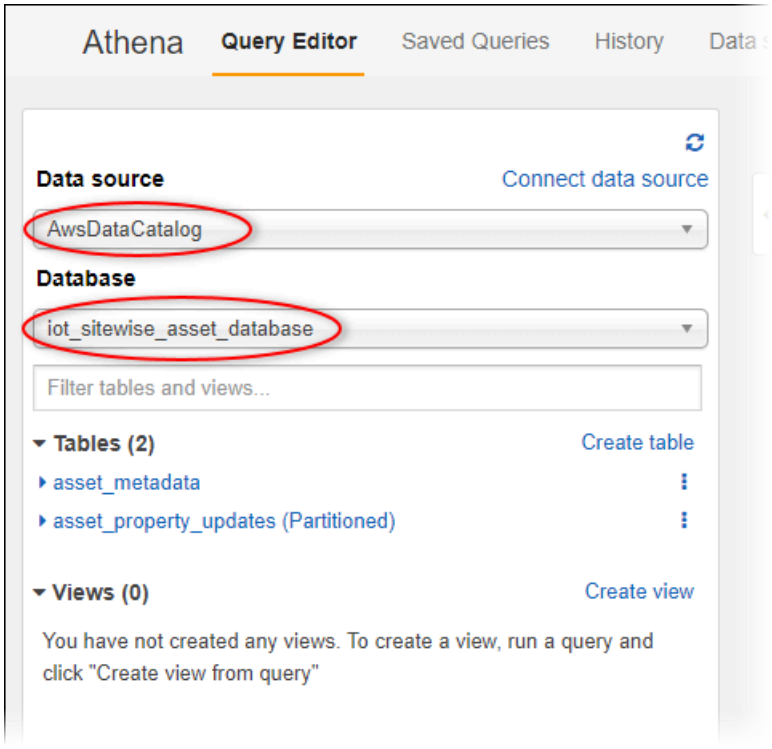


c. Escolha Salvar.

3. O painel esquerdo contém a fonte de dados que será consultada. Faça o seguinte:

a. Em Fonte de dados, escolha AwsDataCatalogusar AWS Glue Data Catalog o.

b. Em Banco de dados, escolha o AWS Glue banco de dados que você criou com o rastreador.



Você verá duas tabelas: asset_metadata e asset_property_updates.

4. Para criar uma exibição a partir da combinação de dados e metadados das propriedades de ativos, insira a seguinte consulta e depois escolha Executar 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") ) );
```

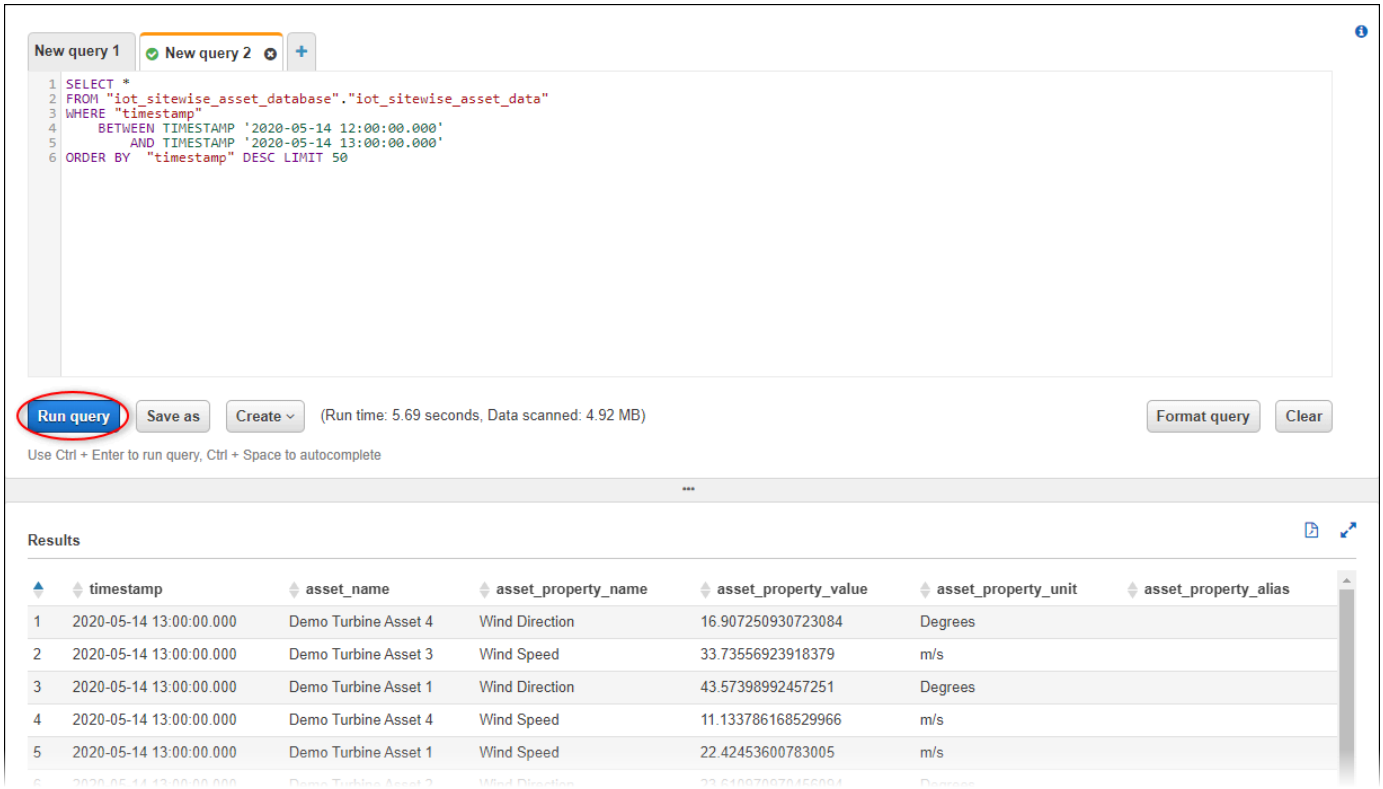
Essa consulta unirá as tabelas de dados e metadados da propriedade de ativos no ID do ativo e no ID da propriedade para criar uma exibição. É possível executar essa consulta várias vezes, pois ela substitui a exibição existente, caso já exista.

5. Escolha o ícone + para adicionar uma nova consulta.
6. Para exibir uma amostra dos dados de ativos, insira a seguinte consulta e escolha Executar consulta. Substitua os time stamps por um intervalo para o qual o bucket tenha dados.

```
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;
```

Essa consulta gera até 50 pontos de dados entre dois time stamps, exibindo as entradas mais recentes primeiro.

A saída da consulta pode ser semelhante aos seguintes resultados.



Agora você pode executar consultas úteis para seu AWS IoT SiteWise aplicativo. Para obter mais informações, consulte SQL reference for Amazon Athena no Guia do usuário do Amazon Athena.

Recursos criados usando o modelo

Quando você cria uma pilha a partir do modelo, AWS CloudFormation cria os seguintes recursos. A maioria dos nomes dos recursos inclui um prefixo que você pode personalizar ao criar a pilha.

Parâmetros de nomes de recursos

- `BucketName` – o nome do bucket do S3 criado usando esse modelo que recebe dados de ativos.
- `GlobalResourcePrefix` – um prefixo para nomes de recursos globais criados usando esse modelo. Padronizado como `sitewise-export-to-s3`.
- `LocalResourcePrefix` – um prefixo para nomes de recursos criados usando esse modelo na região atual. Padronizado como `sitewise_export_to_s3`.

Recursos criados pelo AWS CloudFormation modelo

Recurso	Descrição	Nome
Bucket do S3 para dados processados	Esse bucket contém duas pastas. Uma pasta recebe os dados nivelados e formatados do stream de entrega do Firehose e a outra pasta recebe os metadados do ativo.	`${BucketName}`
Banco de dados da AWS Glue	Esse banco de dados contém a AWS Glue tabela que essa pilha cria.	`${LocalResourcePrefix}_firehose_glue_database`
AWS Glue tabela	O stream de entrega do Firehose usa essa tabela para formatar dados no formato Parquet.	`${LocalResourcePrefix}_firehose_glue_table`
Função do AWS Lambda que transforma dados	Essa função nivela a matriz de valores nas mensagens de notificação do valor da propriedade enviadas de. AWS IoT SiteWise	`${LocalResourcePrefix}_lambda_transform_function`

Recurso	Descrição	Nome
Perfil do IAM para a transformação da função do Lambda.	Essa função permite que o Lambda armazene logs de execução da função de transformação.	`${GlobalResourcePrefix}-lambda-transform-role`
Política do IAM para a transformação do perfil da função do Lambda.	Essa política permite que o Lambda armazene logs de execução da função de transformação.	`${GlobalResourcePrefix}-lambda-transform-policy`
CloudWatch Registra o grupo de registros para a função de transformação	Esse grupo de logs contém logs da função de transformação.	`/aws/lambda/${LocalResourcePrefix}_lambda_transform_function`
Função do Lambda que coleta metadados de ativos	Essa função recupera detalhes sobre ativos AWS IoT SiteWise e armazena os detalhes em um bucket do Amazon S3 criado por essa pilha.	`${LocalResourcePrefix}_lambda_metadata_function`
Camada do Lambda para a função de metadados	Essa camada fornece um AWS SDK que contém AWS IoT SiteWise operações que a função de metadados usa.	`${LocalResourcePrefix}_lambda_metadata_layer`
Perfil do IAM para a função de metadados do Lambda.	Essa função permite que o Lambda recupere detalhes sobre os ativos em. AWS IoT SiteWise	`${GlobalResourcePrefix}-lambda-metadata-role`
Política do IAM para a função de metadados do Lambda.	Essa política permite que o Lambda recupere detalhes sobre os ativos em. AWS IoT SiteWise	`${GlobalResourcePrefix}-lambda-metadata-policy`

Recurso	Descrição	Nome
EventBridgeevento agendado para a função Lambda de metadados	Esse evento programad o executa os metadados do Lambda a cada 6 horas para atualizar o bucket de metadados do ativo.	`${LocalResourcePrefix}-metadata-event`
CloudWatch Grupo de registros para a função de metadados	Esse grupo de logs contém os logs da função de metadados.	`/aws/lambda/${LocalResourcePrefix}_lambda_metadata_function`
Regra do AWS IoT	Essa regra consulta mensagens de notificação de valor de propriedade e envia dados de ativos para um stream de entrega do Amazon Data Firehose.	`${LocalResourcePrefix}_iot_topic_rule`
Papel do IAM para a AWS IoT regra	Essa função permite enviar dados AWS IoT para o stream de entrega do Firehose.	`${GlobalResourcePrefix}-core-firehose-role`
Política do IAM para a função de AWS IoT regra	Essa política permite enviar dados AWS IoT para o stream de entrega do Firehose.	`${GlobalResourcePrefix}-core-firehose-policy`
Stream de entrega do Firehose	Esse fluxo de entrega consome dados da AWS IoT regra, nivela os dados com uma função Lambda e entrega os dados para o Amazon S3.	`${LocalResourcePrefix}_firehose_delivery_stream`

Recurso	Descrição	Nome
Perfil do IAM para o fluxo de entrega.	Essa função permite que o Firehose execute operações no bucket, na tabela AWS Glue , nas funções do Lambda e no grupo de registros de registros do S3. CloudWatch	`${GlobalResourcePrefix}-firehose-delivery-role`
CloudWatch Registra o grupo de registros para o stream de entrega	Esse grupo de registros contém um fluxo de registros ,`S3 Delivery`, que recebe registros sobre o fluxo de entrega do Firehose.	`/aws/kinesisfirehose/${LocalResourcePrefix}_firehose_delivery_stream`

Integração com o Grafana

O Grafana é uma plataforma de visualização de dados que você pode usar para visualizar e monitorar dados em painéis. Na versão 7.3.0 e posterior do Grafana, você pode usar o plug-in AWS IoT SiteWise para visualizar seus dados de ativos AWS IoT SiteWise nos painéis do Grafana. Você pode visualizar dados de várias AWS fontes (como AWS IoT SiteWise Amazon Timestream CloudWatch e Amazon) e outras fontes de dados com um único painel da Grafana.

Você tem duas opções para usar o plug-in AWS IoT SiteWise:

- Servidores locais do Grafana

  Você pode configurar o plug-in AWS IoT SiteWise em um servidor Grafana que você gerencia. Para obter mais informações sobre como adicionar e usar o plug-in, consulte o arquivo README da AWS IoT SiteWise fonte de dados no site. GitHub
- AWS Managed Service for Grafana

  Você pode usar o plug-in AWS IoT SiteWise no AWS Managed Service for Grafana (AMG). A AMG gerencia os servidores Grafana para você, de modo que seja possível visualizar seus dados sem precisar criar, empacotar ou implantar qualquer hardware ou qualquer outra infraestrutura do Grafana. Para obter mais informações, consulte os tópicos a seguir no AWSGuia do usuário do Managed Service for Grafana:

- O que é o Amazon Managed Service for Grafana (AMG)?
- Usando a fonte de dados AWS IoT SiteWise

Example Exemplo de painel do Grafana

O painel do Grafana a seguir visualiza o parque eólico de demonstração. Você pode acessar este painel de demonstração no site do Grafana Play.

Integração do AWS IoT SiteWise e do AWS IoT TwinMaker

A integração com AWS IoT TwinMaker concede acesso a funcionalidades robustasAWS IoT SiteWise, como `ExecuteQuery` API de recuperação de AWS IoT SiteWise dados e pesquisa

avançada de ativos no AWS IoT SiteWise console. Para integrar os serviços e usar esses recursos, você deve primeiro habilitar a integração.

Tópicos

Habilitar a integração

Os administradores podem usar as políticas de JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições. O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. Para obter mais informações sobre as ações compatíveis com AWS IoT SiteWise, consulte Ações definidas pelo AWS IoT SiteWise na Referência de autorização de serviço.

Para obter mais informações sobre funções AWS IoT TwinMaker vinculadas ao serviço, consulte Funções vinculadas ao serviço AWS IoT TwinMaker no Guia do usuário. AWS IoT TwinMaker

Antes de integrar AWS IoT SiteWise eAWS IoT TwinMaker, você deve conceder as seguintes permissões que permitem AWS IoT SiteWise a integração com um espaço de trabalho AWS IoT TwinMaker vinculado:

- `iotsitewise:EnableSiteWiseIntegration`— Permite AWS IoT SiteWise a integração com um AWS IoT TwinMaker espaço de trabalho vinculado. Essa integração permite AWS IoT TwinMaker ler todas as suas informações de modelagem AWS IoT SiteWise por meio de uma função AWS IoT TwinMaker vinculada ao serviço. Para habilitar essa permissão, adicione a seguinte política à sua função do IAM:

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

```
  ]
}
```

Integração do AWS IoT SiteWise e do AWS IoT TwinMaker

Para integrar AWS IoT SiteWise eAWS IoT TwinMaker, você deve ter o seguinte:

- AWS IoT SiteWisefunção vinculada ao serviço configurada em sua conta
- AWS IoT TwinMakerfunção vinculada ao serviço configurada em sua conta
- AWS IoT TwinMakerespaço de trabalho com ID `IoTSiteWiseDefaultWorkspace` em sua conta na região.

Para integrar usando o AWS IoT SiteWise console

Ao ver o AWS IoT TwinMaker banner Integração com o console, escolha Conceder permissão. Os pré-requisitos são criados em sua conta.

Para integrar usando o AWS CLI

Para integrar AWS IoT SiteWise e AWS IoT TwinMaker usar oAWS CLI, digite os seguintes comandos:

1. Ligue `CreateServiceLinkedRole` com um `AWSServiceName` dos`iotsitewise.amazonaws.com`.

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

2. Ligue `CreateServiceLinkedRole` com um `AWSServiceName` dos `iottwinmaker.amazonaws.com`.

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

3. Ligue `CreateWorkspace` com um `ID` dos`IoTSiteWiseDefaultWorkspace`.

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

Detecção de anomalias em equipamentos com o Amazon Lookout for Equipment

> **Note**
>
> A detecção de anomalias só está disponível nas regiões em que o Amazon Lookout for Equipment está disponível.

Você pode se integrar AWS IoT SiteWise ao Amazon Lookout for Equipment para obter informações sobre seu equipamento industrial por meio da detecção de anomalias e da manutenção preditiva de equipamentos industriais. O Lookout for Equipment é um serviço de aprendizado de máquina (ML) para monitorar equipamentos industriais que detecta o comportamento anormal do equipamento e identifica possíveis falhas. Com o Lookout for Equipment, você pode implementar programas de manutenção preditiva e identificar processos de equipamentos abaixo do ideal. Para obter mais informações sobre o Lookout for Equipment, consulte O que é o Amazon Lookout for Equipment? no Guia do usuário do Amazon Lookout for Equipment.

Quando você cria uma previsão para treinar um modelo de ML para detectar o comportamento anômalo do equipamento, AWS IoT SiteWise envia os valores das propriedades do ativo para a Lookout for Equipment para treinar um modelo de ML para detectar o comportamento anômalo do equipamento. Para definir uma definição de previsão em um modelo de ativo, você especifica as funções do IAM necessárias para que a Lookout for Equipment acesse seus dados e as propriedades para enviar à Lookout for Equipment e enviar dados processados para o Amazon S3. Para ter mais informações, consulte Criar modelos de ativo.

Para integrar AWS IoT SiteWise o Lookout for Equipment, você executará as seguintes etapas de alto nível:

- Adicione uma definição de previsão em um modelo de ativo que descreva quais propriedades você deseja rastrear. A definição de previsão é uma coleção reutilizável de medições, transformações e métricas que é usada para criar previsões sobre os ativos com base nesse modelo de ativo.
- Treine a previsão com base nos dados históricos que você fornece.
- Inferência de cronograma, que AWS IoT SiteWise informa com que frequência executar uma previsão específica.

Depois que a inferência é programada, o modelo Lookout for Equipment monitora os dados que recebe do seu equipamento e procura anomalias no comportamento do equipamento. Você pode visualizar e analisar os resultados no SiteWise Monitor, usando as operações da API AWS IoT SiteWise GET ou o console Lookout for Equipment. Você também pode criar alarmes usando detectores de alarme do modelo de ativos para alertá-lo sobre o comportamento anormal do equipamento.

Tópicos

Adicionando uma definição de previsão (console)

Para começar a enviar dados coletados pela AWS IoT SiteWise Lookout for Equipment, você deve adicionar AWS IoT SiteWise uma definição de previsão a um modelo de ativo.

Para adicionar uma definição de previsão a um modelo AWS IoT SiteWise de ativo

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, escolha Modelos e selecione o modelo de ativo ao qual você deseja adicionar a definição de previsão.
3. Escolha Previsões.
4. Escolha Adicionar definição de predição.
5. Defina detalhes sobre a definição da previsão.

    a. Insira um nome exclusivo e uma descrição para sua definição de previsão. Escolha o nome cuidadosamente, pois depois de criar a definição de previsão, você não poderá alterar o nome dela.

    b. Crie ou selecione uma função de permissões do IAM que permita AWS IoT SiteWise compartilhar seus dados de ativos com o Amazon Lookout for Equipment. A função deve ter

as seguintes políticas de IAM e confiança. Para obter ajuda na criação da função, consulte Criação de uma função usando políticas de confiança personalizadas (console).

Política do IAM

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "L4EPermissions",
            "Effect": "Allow",
            "Action": [
                "lookoutequipment:CreateDataset",
                "lookoutequipment:CreateModel",
                "lookoutequipment:CreateInferenceScheduler",
                "lookoutequipment:DescribeDataset",
                "lookoutequipment:DescribeModel",
                "lookoutequipment:DescribeInferenceScheduler",
                "lookoutequipment:ListInferenceExecutions",
                "lookoutequipment:StartDataIngestionJob",
                "lookoutequipment:StartInferenceScheduler",
                "lookoutequipment:UpdateInferenceScheduler",
                "lookoutequipment:StopInferenceScheduler"
            ],
            "Resource": [
                "arn:aws:lookoutequipment:Region:Account_ID:inference-
scheduler/IoTSiteWise_*",
                "arn:aws:lookoutequipment:Region:Account_ID:model/
IoTSiteWise_*",
                "arn:aws:lookoutequipment:Region:Account_ID:dataset/
IoTSiteWise_*"
            ]
        },
        {
            "Sid": "L4EPermissions2",
            "Effect": "Allow",
            "Action": [
                "lookoutequipment:DescribeDataIngestionJob"
            ],
            "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::Account_ID:role/Role_name"
        }
    ]
}
```

Política de confiança

```
{
    "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. Selecione Next (Próximo).

6. Selecione os atributos de dados (medidas, transformações e métricas) que você deseja enviar para a Lookout for Equipment.

   a. (Opcional) Selecione as medidas.

   b. (Opcional) Selecione as transformações.

   c. (Opcional) Selecione métricas.

   d. Selecione Next (Próximo).

7. Revise suas seleções. Para adicionar a definição de previsão ao modelo de ativo, na página de resumo, escolha Adicionar definição de previsão.

Você também pode editar ou excluir uma definição de predição existente que tenha previsões ativas anexadas.

Treinando uma previsão (console)

Depois de adicionar uma definição de previsão a um modelo de ativo, você pode treinar as previsões que estão em seus ativos.

Para treinar uma previsão em AWS IoT SiteWise

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, escolha Ativos e selecione o ativo que você deseja monitorar.

3. Escolha Previsões.
4. Selecione as previsões que você deseja treinar.
5. Em Ações, escolha Iniciar treinamento e faça o seguinte:

    a. Em Detalhes da previsão, selecione uma função de permissões do IAM que permita AWS IoT SiteWise compartilhar seus dados de ativos com o Lookout for Equipment. Se você precisar criar uma nova função, escolha Criar uma nova função.

    b. Em Configurações de dados de treinamento, insira um intervalo de tempo de dados de treinamento para selecionar quais dados usar para treinar a previsão.

    c. (Opcional) Selecione a taxa de amostragem dos dados após o pós-processamento.

    d. (Opcional) Para rótulos de dados, forneça um bucket e um prefixo do Amazon S3 que contenham seus dados de rotulagem. Para obter mais informações sobre rotulagem de dados, consulte Como rotular seus dados no Guia do usuário do Amazon Lookout for Equipment.

    e. Selecione Next (Próximo).
6. (Opcional) Se você quiser que a previsão fique ativa assim que o treinamento for concluído, em Configurações avançadas, selecione Ativar automaticamente a previsão após o treinamento e faça o seguinte:

    a. Em Dados de entrada, em Frequência de upload de dados, defina com que frequência os dados são carregados e, em Tempo de atraso de compensação, defina a quantidade de buffer a ser usada.

    b. Selecione Next (Próximo).
7. Revise os detalhes da previsão e escolha Salvar e começar.

Iniciando ou interrompendo a inferência sobre uma previsão (console)

> **Note**
>
> As cobranças do Lookout for Equipment se aplicam a inferências programadas com os dados transferidos AWS IoT SiteWise entre o Lookout for Equipment e o Lookout for Equipment. Para obter mais informações, consulte os preços do Amazon Lookout for Equipment.

Se você adicionou uma previsão b"lookoutequipment: CreateDataset “, mas não optou por ativá-la após o treinamento, você deve ativá-la para que ela comece a monitorar seus ativos.

Para iniciar a inferência para uma previsão

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, escolha Ativos e selecione o ativo ao qual a previsão é adicionada.
3. Escolha Previsões.
4. Selecione as previsões que você deseja ativar.
5. Em Ações, escolha Iniciar inferência e faça o seguinte:

    a. Em Dados de entrada, em Frequência de upload de dados, defina com que frequência os dados são carregados e, em Tempo de atraso de compensação, defina a quantidade de buffer a ser usada.

    b. Escolha Salvar e começar.

Para interromper a inferência de uma previsão

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, escolha Ativos e selecione o ativo ao qual a previsão é adicionada.
3. Escolha Previsões.
4. Selecione as previsões que você deseja interromper.
5. Em Ações, escolha Parar inferência.

Adicionando uma definição de previsão (CLI)

Para definir uma definição de previsão em um modelo de ativo novo ou existente, você pode usar o AWS Command Line Interface (AWS CLI). Depois de definir a definição de previsão no modelo de ativo, você treina e programa a inferência para uma previsão em um ativo AWS IoT SiteWise para fazer a detecção de anomalias com o Lookout for Equipment.

Pré-requisitos

Para concluir essas etapas, você deve ter um modelo de ativo e pelo menos um ativo criado. Para obter mais informações, consulte Criação de um modelo de ativo (AWS CLI) e Criação de um ativo (AWS CLI).

Se você é novato AWS IoT SiteWise, deve chamar a operação de `CreateBulkImportJob` API para importar valores de propriedades de ativos AWS IoT SiteWise, que serão usados para treinar o modelo. Para ter mais informações, consulte Criar um trabalho de importação em massa (AWS CLI).

Para adicionar uma definição de previsão

1. Crie um arquivo chamado `asset-model-payload.json`. Siga as etapas nessas outras seções para adicionar os detalhes do seu modelo de ativo para o arquivo, mas não envie a solicitação para criar ou atualizar o modelo de ativo.

   - Para obter mais informações sobre como criar um modelo de ativo, consulte Criação de um modelo de ativo (AWS CLI)
   - Para obter mais informações sobre como atualizar um modelo de ativo existente, consulte Atualizando um modelo de ativo ou componente (AWS CLI)

2. Adicione um modelo composto da Lookout for Equipment `assetModelCompositeModels` () ao modelo de ativo adicionando o código a seguir.

   - *`Property`*Substitua pela ID das propriedades que você deseja incluir. Para obter essas identidades, ligue `DescribeAssetModel`.
   - *`RoleARN`*Substitua pelo ARN de uma função do IAM que permite que a Lookout for Equipment acesse seus dados. 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. Crie o modelo de ativo ou atualize o modelo de ativo existente. Execute um destes procedimentos:

   - Para criar o modelo de ativo, execute o seguinte comando:

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

   - Para atualizar o modelo de ativo existente, execute o comando a seguir. *asset-model-id*Substitua pela ID do modelo de ativo que você deseja atualizar.

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

Depois de executar o comando, observe o `assetModelId` na resposta.

Treinando uma previsão e iniciando a inferência (CLI)

Agora que a definição de previsão está definida, você pode treinar ativos com base nela e iniciar a inferência. Se você quiser treinar sua previsão, mas não iniciar a inferência, vá para. Treinando uma previsão (CLI) Para treinar a previsão e iniciar a inferência sobre o ativo, você precisará do recurso `assetId` de destino.

Para treinar e iniciar a inferência da previsão

1. Execute o comando a seguir para encontrar o `assetModelCompositeModelId` abaixo`assetModelCompositeModelSummaries`. *`asset-model-id`*Substitua pela ID do modelo de ativo que você criou emAtualizando um modelo de ativo ou componente (AWS CLI).

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

2. Execute o comando a seguir para encontrar a `TrainingWithInference` ação. `actionDefinitionId` *`asset-model-id`*Substitua pela ID usada na etapa anterior e *`asset-model-composite-model-id`*substitua pela ID retornada na etapa 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. Crie um arquivo chamado `train-start-inference-prediction.json` e adicione o código a seguir, substituindo o seguinte:

   - *`asset-id`*com o ID do ativo de destino
   - *`action-definition-id`*com o ID da TrainingWithInference ação
   - *`StartTime`*com o início dos dados de treinamento, fornecidos em segundos de época
   - *`EndTime`*com o final dos dados de treinamento, fornecidos em segundos de época
   - *`TargetSamplingRate`*com a taxa de amostragem dos dados após o pós-processamento pela Lookout for Equipment. Os valores permitidos são:`PT1S | PT5S | PT10S | PT15S | PT30S | PT1M | PT5M | PT10M | PT15M | PT30M | PT1H`.

   ```
   {
     "targetResource": {
       "assetId": "asset-id"
   ```

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

4. Execute o comando a seguir para iniciar o treinamento e a inferência:

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

Treinando uma previsão (CLI)

Agora que a definição de previsão está definida, você pode treinar ativos com base nela. Para treinar a previsão do ativo, você precisará `assetId` do recurso de destino.

Para treinar a previsão

1. Execute o comando a seguir para encontrar o `assetModelCompositeModelId` abaixo`assetModelCompositeModelSummaries`. *`asset-model-id`*Substitua pela ID do modelo de ativo que você criou emAtualizando um modelo de ativo ou componente (AWS CLI).

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

2. Execute o comando a seguir para encontrar a `Training` ação. `actionDefinitionId` *`asset-model-id`*Substitua pela ID usada na etapa anterior e *`asset-model-composite-model-id`*substitua pela ID retornada na etapa 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. Crie um arquivo chamado `train-prediction.json` e adicione o código a seguir, substituindo o seguinte:

- *asset-id*com o ID do ativo de destino
- *action-definition-id*com o ID da ação de treinamento
- *StartTime*com o início dos dados de treinamento, fornecidos em segundos de época
- *EndTime*com o final dos dados de treinamento, fornecidos em segundos de época
- (Opcional) *BucketName* com o nome do bucket do Amazon S3 que contém seus dados de etiqueta
- (Opcional) *Prefix* com o prefixo associado ao bucket do Amazon S3.
- *TargetSamplingRate*com a taxa de amostragem dos dados após o pós-processamento pela Lookout for Equipment. Os valores permitidos são:`PT1S | PT5S | PT10S | PT15S | PT30S | PT1M | PT5M | PT10M | PT15M | PT30M | PT1H`.

> **Note**
>
> Inclua o nome e o prefixo do bucket, ou nenhum deles.

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

4. Execute o comando a seguir para iniciar o treinamento:

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

Antes de começar a inferência, o treinamento deve ser concluído. Para verificar o status do treinamento, faça o seguinte:

- No console, navegue até o ativo em que a previsão está ativada.

- A partir do AWS CLI, ligue `BatchGetAssetPropertyValue` usando o `propertyId` da `trainingStatus` propriedade.

Iniciando ou interrompendo a inferência sobre uma previsão (CLI)

Depois que a previsão for treinada, você poderá iniciar a inferência para fazer com que a Lookout for Equipment comece a monitorar seus ativos. Para iniciar ou interromper a inferência, você precisará do recurso `assetId` de destino.

Para iniciar a inferência

1. Execute o comando a seguir para encontrar o `assetModelCompositeModelId` abaixo`assetModelCompositeModelSummaries`. *`asset-model-id`*Substitua pela ID do modelo de ativo que você criou emAtualizando um modelo de ativo ou componente (AWS CLI).

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

2. Execute o comando a seguir para encontrar a `Inference` ação. `actionDefinitionId` *`asset-model-id`*Substitua pela ID usada na etapa anterior e *`asset-model-composite-model-id`*substitua pela ID retornada na etapa 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. Crie um arquivo chamado `start-inference.json` e adicione o código a seguir, substituindo o seguinte:

   - *`asset-id`*com o ID do ativo de destino
   - *`action-definition-id`*com o ID da ação inicial de inferência
   - *`Offset`*com a quantidade de buffer a ser usada
   - *`Frequency`*com a frequência com que os dados são carregados

   ```
   {
     "targetResource": {
       "assetId": "asset-id"
     },
   ```

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

4. Execute o comando a seguir para iniciar a inferência:

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

Para parar a inferência

1. Execute o comando a seguir para encontrar o `assetModelCompositeModelId` abaixo`assetModelCompositeModelSummaries`. *`asset-model-id`*Substitua pela ID do modelo de ativo que você criou em[Atualizando um modelo de ativo ou componente (AWS CLI)](#).

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

2. Execute o comando a seguir para encontrar a `Inference` ação. `actionDefinitionId` *`asset-model-id`*Substitua pela ID usada na etapa anterior e *`asset-model-composite-model-id`*substitua pela ID retornada na etapa 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. Crie um arquivo chamado `stop-inference.json` e adicione o código a seguir, substituindo o seguinte:

   - *`asset-id`*com o ID do ativo de destino
   - *`action-definition-id`*com o ID da ação inicial de inferência

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

```
}}
```

4. Execute o comando a seguir para interromper a inferência:

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

Gerenciando o armazenamento de dados

Você pode configurar AWS IoT SiteWise para salvar seus dados nos seguintes níveis de armazenamento:

Dados acessados com frequência (camada quente)

O nível de armazenamento quente é um armazenamento AWS IoT SiteWise gerenciado de séries temporais. O hot tier é mais eficaz para dados acessados com frequência, com baixa write-to-read latência. Os dados armazenados na camada quente são usados por aplicações industriais que precisam de acesso rápido aos valores mais recentes das medições em seu equipamento. Isso inclui aplicativos que visualizam métricas em tempo real com um painel interativo ou aplicativos que monitoram operações e lançam alarmes para identificar problemas de desempenho.

Por padrão, os dados ingeridos AWS IoT SiteWise são armazenados na camada ativa. Você pode definir um período de retenção para o nível quente, após o qual AWS IoT SiteWise move os dados no nível quente para o armazenamento no nível quente ou frio, com base na sua configuração. Para obter o melhor desempenho e a melhor relação custo-benefício, defina o período de retenção do Hot Tier para ser maior do que o tempo necessário para recuperar dados com frequência. Isso é usado para métricas, alarmes e cenários de monitoramento em tempo real. Se um período de retenção não for definido, seus dados serão armazenados indefinidamente no hot tier.

Nível quente

O nível de armazenamento aquecido é um nível AWS IoT SiteWise gerenciado que é eficaz para o armazenamento econômico de dados históricos. É melhor usá-lo para recuperar grandes volumes de dados com características de write-to-read latência média. Use a camada quente para armazenar dados históricos necessários para grandes cargas de trabalho. Por exemplo, ele é usado para recuperação de dados para análises, aplicativos de business intelligence (BI), ferramentas de geração de relatórios e treinamento de modelos de aprendizado de máquina (ML). Se você ativar o nível de armazenamento a frio, poderá definir um período de retenção do nível quente. Após o término do período de retenção, AWS IoT SiteWise exclui os dados do nível quente.

Dados acessados raramente (camada fria)

O nível de armazenamento a frio usa um bucket do Amazon S3 para armazenar dados que raramente são usados. Com a camada fria ativada, AWS IoT SiteWise replica as séries

temporais, incluindo medições, métricas, transformações e agregações e definições de modelos de ativos a cada 6 horas. A camada fria é usada para armazenar dados que toleram alta latência de leitura para relatórios e backups históricos.

Tópicos

Definir configurações de armazenamento

Você pode definir as configurações de armazenamento para optar pelo armazenamento gerenciado de nível quente e também para replicar dados para o nível frio. Para saber mais sobre o período de retenção dos níveis quente e quente, consulteImpacto da retenção de dados. Ao definir as configurações de armazenamento, faça o seguinte:

- Retenção de nível ativo — defina um período de retenção de quanto tempo seus dados são armazenados no nível ativo antes de serem excluídos e movidos para o armazenamento gerenciado em nível quente ou armazenamento em nível frio com base em suas configurações de armazenamento. AWS IoT SiteWise excluirá todos os dados do hot tier que existiam antes do término do período de retenção. Se você não definir um período de retenção, seus dados serão armazenados indefinidamente no hot tier.
- Retenção de nível quente — defina um período de retenção de quanto tempo seus dados são armazenados no nível quente antes de serem excluídos do AWS IoT SiteWise armazenamento e movidos para o armazenamento de nível frio gerenciado pelo cliente. AWS IoT SiteWise exclui todos os dados do nível de aquecimento que existiam antes do término do período de retenção. Se um período de retenção não for definido, seus dados serão armazenados indefinidamente no nível quente.

> **Note**
>
> Para melhorar o desempenho da consulta, defina um período de retenção de nível ativo com armazenamento de nível quente.

Impacto da retenção de dados no armazenamento de níveis quente e quente

- Quando você diminui o período de retenção do armazenamento da camada quente, os dados são movidos permanentemente da camada quente para a camada quente ou fria. Quando você diminui o período de retenção da camada quente, os dados são movidos para a camada fria e excluídos permanentemente da camada quente.
- Quando você aumenta o período de retenção do armazenamento de nível quente ou quente, a alteração afeta os dados enviados a AWS IoT SiteWise partir de então. AWS IoT SiteWise não recupera dados do armazenamento quente ou frio para preencher o nível quente. Por exemplo, se o período de retenção do armazenamento de camada ativa for inicialmente definido para 30 dias e depois aumentado para 60 dias, são necessários 30 dias para que o armazenamento de camada ativa contenha dados equivalentes a 60 dias.

Tópicos

Defina as configurações de armazenamento para o nível quente (console)

O procedimento a seguir mostra como definir as configurações de armazenamento para replicar dados para a camada quente no AWS IoT SiteWise console.

Para definir configurações de ingestão de dados no console:

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, em Configurações, selecione Armazenamento.
3. No canto superior direito, escolha Editar.
4. Na página Editar permissões, faça o seguinte:
5. Para configurações do Hot tier, faça o seguinte:

- Se você quiser definir um período de retenção de quanto tempo seus dados serão armazenados no nível ativo antes de serem excluídos e movidos para o armazenamento de nível quente gerenciado pelo serviço, escolha Ativar período de retenção.
- Para configurar um período de retenção, insira um número e escolha uma unidade. O período de retenção deve ser igual ou maior que 30 dias.

AWS IoT SiteWise exclui todos os dados no hot tier que sejam mais antigos do que o período de retenção. Caso não defina um período de retenção, seus dados serão armazenados indefinidamente.

6. (Recomendado) Para configurações de nível quente, faça o seguinte:

   - Para optar pelo armazenamento em camada quente, selecione Confirmo a opção de armazenamento em camada quente para optar pelo armazenamento em camada quente.
   - (Opcional) Para configurar um período de retenção, insira um número inteiro e escolha uma unidade. O período de retenção deve ser maior ou igual a 365 dias.

   AWS IoT SiteWise exclui dados no nível de aquecimento que existiam antes do período de retenção. Caso não defina um período de retenção, seus dados serão armazenados indefinidamente.

   > **Note**
   >
   > - Quando você opta pelo nível quente, a configuração é exibida apenas uma vez.
   > - Para definir a retenção do nível quente, você deve ter armazenamento no nível quente ou frio. Para eficiência de custos e recuperação de dados históricos, AWS IoT SiteWise recomenda que você armazene dados de longo prazo no nível quente.
   > - Para definir a retenção do nível quente, você deve ter armazenamento no nível frio.

7. Escolha Salvar para salvar suas configurações de armazenamento.

Na seção AWS IoT SiteWise de armazenamento, o armazenamento de nível quente está em um dos seguintes estados:

- Ativado — se seus dados existiam antes do período de retenção do nível quente, AWS IoT SiteWise mova os dados para o nível quente.”
- Desativado — O armazenamento de nível quente está desativado.

Definir as configurações de armazenamento para o nível quente (AWS CLI)

Você pode definir as configurações de armazenamento para mover dados para a camada quente usando os comandos AWS CLI e os seguintes.

Para evitar a substituição da configuração existente, recupere as informações atuais da configuração de armazenamento executando o seguinte comando:

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

Example resposta sem a configuração existente de camada fria

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

Example resposta com a configuração de camada fria 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"
}
```

Defina as configurações de armazenamento para o nível quente com AWS CLI

Execute o comando a seguir para definir as configurações de armazenamento. `file-name`Substitua pelo nome do arquivo que contém a configuração AWS IoT SiteWise de armazenamento.

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

Example AWS IoT SiteWise configuração com nível quente e quente

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

}
```

`hot-tier-retention-in-days`deve ser um número inteiro maior ou igual a 30 dias.

Example Retorno

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

Se você tiver o armazenamento de camada fria ativado, consulte[Defina as configurações de armazenamento com AWS CLI uma camada fria existente](#).

Defina as configurações de armazenamento com AWS CLI uma camada fria existente

Defina as configurações de armazenamento usando AWS CLI o armazenamento de camada fria existente

- Execute o comando a seguir para definir as configurações de armazenamento. Substitua *file-name* pelo nome do arquivo contendo a configuração de armazenamento AWS IoT SiteWise .

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

Example AWS IoT SiteWise configuração de armazenamento

- Substitua *bucket-name* pelo nome do bucket do Amazon S3.
- Substitua o *prefixo* pelo prefixo do Amazon S3.
- *aws-account-id*Substitua pelo ID AWS da sua conta.
- Substitua *role-name* pelo nome da função de acesso do Amazon S3 que AWS IoT SiteWise permite enviar dados para o Amazon S3.
- Substitua *hot-tier-retention-in-days* por um número inteiro maior ou igual a 30 dias.
- Substitua *warm-tier-retention-in-days* por um número inteiro maior ou igual a 365 dias.

> **Note**
>
> AWS IoT SiteWise excluirá todos os dados na camada quente que sejam mais antigos do que o período de retenção da camada fria. Caso não defina um período de retenção, seus dados serão armazenados 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 Retorno

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

Definir as configurações de armazenamento para o nível frio (console)

O procedimento a seguir mostra como definir as configurações de armazenamento para replicar dados para a camada fria no AWS IoT SiteWise console.

Para definir configurações de ingestão de dados no console:

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, em Configurações, selecione Armazenamento.
3. No canto superior direito, escolha Editar.
4. Na página Editar permissões, faça o seguinte:
   a. Em Configurações de armazenamento, escolha Ativar armazenamento em camada fria. O armazenamento de camada fria estará desabilitado por padrão.
   b. Em Localização do bucket do S3, insira o nome de um bucket existente do Amazon S3 e um prefixo.

> **Note**
>
> - O Amazon S3 usa o prefixo como nome de pasta para organizar os dados no bucket Amazon S3. O prefixo deve ter entre 1 e 255 caracteres e terminar com uma barra (/). Seus dados AWS IoT SiteWise serão salvos nessa pasta.
> - Se não tiver um bucket do Amazon S3, escolha Exibir e crie um no console do Amazon S3. Para obter mais informações, consulte Criar seu primeiro bucket do S3 no Guia do Usuário do Amazon S3.

c. Para Função de acesso S3, siga um destes procedimentos:

- Escolha Criar uma função a partir de um modelo AWS gerenciado, cria AWS automaticamente uma função do IAM que permite AWS IoT SiteWise enviar dados para o Amazon S3.
- Escolha Usar uma função existente e, em seguida, a função criada a partir da lista.

> **Note**
>
> - Você deve usar o mesmo nome do bucket do Amazon S3 na Localização do bucket do S3 da etapa anterior e política do IAM.
> - Certifique-se de que sua função tem as permissões do exemplo a seguir:
>
>   Example política de permissões:
>
> ```
> {
>       "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/*"
            ]
        }
    ]
}
```

Substitua *bucket-name* pelo nome do bucket do Amazon S3.

d. Para configurar o hot tier, consulte a Etapa 5 emDefina as configurações de armazenamento para o nível quente (console).

e. (Opcional) Para Integração AWS IoT Analytics , faça o seguinte:

   i. Se você quiser usar AWS IoT Analytics para consultar seus dados, escolha Armazenamento de AWS IoT Analytics dados ativado.

   ii. AWS IoT SiteWise gera um nome para seu armazenamento de dados ou você pode inserir um nome diferente.

   AWS IoT SiteWise cria automaticamente um armazenamento de dados AWS IoT Analytics para salvar seus dados. Para consultar os dados, você pode usar AWS IoT Analytics para criar conjuntos de dados. Para obter mais informações, consulte Como trabalhar com AWS IoT SiteWise dados no Guia AWS IoT Analytics do usuário.

f. Selecione Salvar.

Na seção Armazenamento do AWS IoT SiteWise , o Armazenamento em camada fria pode ser um dos seguintes valores:

- Ativado — AWS IoT SiteWise replica seus dados para o bucket do Amazon S3 especificado.
- Habilitar — AWS IoT SiteWise está processando sua solicitação para habilitar o armazenamento em camada fria. O processo pode demorar vários minutos para ser concluído.
- Enable_Failed — AWS IoT SiteWise não foi possível processar sua solicitação para ativar o armazenamento em camada fria. Se você habilitou AWS IoT SiteWise o envio de registros para o Amazon CloudWatch Logs, você pode usar esses registros para solucionar problemas. Para ter mais informações, consulte Monitoramento com Amazon CloudWatch Logs.
- Desativado — O armazenamento em camada fria está desativado.

Definir as configurações de armazenamento para o nível frio (AWS CLI)

O procedimento a seguir mostra como definir as configurações de armazenamento para replicar os dados na camada fria usando o AWS CLI.

Para definir as configurações de armazenamento usando AWS CLI

1. Para exportar dados para um bucket do Amazon S3 em sua conta, execute o comando a seguir para definir as configurações de armazenamento: Substitua *file-name* pelo nome do arquivo que contém a configuração AWS IoT SiteWise de armazenamento.

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

   Example AWS IoT SiteWise configuração de armazenamento

   - Substitua *bucket-name* pelo nome do bucket do Amazon S3.
   - Substitua o *prefixo* pelo prefixo do Amazon S3.
   - *aws-account-id*Substitua pelo ID AWS da sua conta.
   - Substitua *role-name* pelo nome da função de acesso do Amazon S3 que AWS IoT SiteWise permite enviar dados para o Amazon S3.
   - *retention-in-days*Substitua por um número inteiro maior ou igual a 30 dias.

   ```
   {
         "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

- Você deve usar o mesmo nome de bucket do Amazon S3 na configuração de AWS IoT SiteWise armazenamento e na política do IAM.
- Certifique-se de que sua função tem as permissões do exemplo a seguir:

  Example política de permissões:

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

  Substitua *bucket-name* pelo nome do bucket do Amazon S3.

Example Retorno

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

```
        "state": "UPDATE_IN_PROGRESS"
    }
}
```

> **Note**
>
> A atualização da configuração de armazenamento pode levar alguns minutos. AWS IoT SiteWise

2. Para obter as informações de configuração do repositório, use o seguinte comando:

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

Example Retorno

```
{
      "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 interromper a exportação de dados para o bucket do Amazon S3, execute o comando a seguir para definir configurações de armazenamento:

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

> **Note**
>
> Por padrão, seus dados são armazenados apenas na camada ativa do AWS IoT SiteWise.

Example Retorno

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

4. Para obter as informações de configuração do repositório, use o seguinte comando:

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

Example Retorno

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

(Opcional) Crie um armazenamento AWS IoT Analytics de dados (AWS CLI)

Um armazenamento AWS IoT Analytics de dados é um repositório escalável e consultável que recebe e armazena dados. Você pode usar o AWS IoT SiteWise console ou as AWS IoT Analytics APIs para criar um armazenamento AWS IoT Analytics de dados para salvar seus AWS IoT SiteWise dados. Para consultar os dados, você cria conjuntos de dados usando o. AWS IoT Analytics Para obter mais informações, consulte Trabalhando com dados AWS IoT SiteWise no Guia do Usuário AWS IoT Analytics .

As etapas a seguir são usadas AWS CLI para criar um armazenamento de dados em AWS IoT Analytics.

Para criar um armazenamento de dados, execute o comando a seguir: Substitua *file-name* pelo nome do arquivo que contém a configuração de armazenamento de dados.

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

> **Note**
>
> - Você deve especificar o nome de um bucket existente do Amazon S3. Se você não tiver um bucket do Amazon S3, crie um primeiro. Para obter mais informações, consulte Criar seu primeiro bucket S3 no Guia do usuário do Amazon S3.
> - Você deve usar o mesmo nome de bucket do Amazon S3 na configuração de AWS IoT SiteWise armazenamento, na política do IAM e na configuração do armazenamento de AWS IoT Analytics dados.

Example AWS IoT Analytics configuração do armazenamento de dados

Substitua *data-store-name*e *s3-bucket-name pelo nome do* seu armazenamento de AWS IoT Analytics dados e pelo nome do bucket do Amazon S3.

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

Example Retorno

```
{
```

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

Solucionar problemas de configurações de armazenamento

Use as informações a seguir para solucionar problemas com a configuração de armazenamento.

Problemas

- Erro: Bucket não existe
- Erro: acesso negado ao caminho do Amazon S3
- Erro: O ARN da função não pode ser presumido
- Erro: falha ao acessar o bucket entre regiões do Amazon S3

Erro: Bucket não existe

Solução: AWS IoT SiteWise não foi possível encontrar seu bucket do Amazon S3. Certifique-se de ter inserido o nome de um bucket existente do Amazon S3 na região atual.

Erro: acesso negado ao caminho do Amazon S3

Solução: AWS IoT SiteWise não foi possível acessar seu bucket do Amazon S3. Faça o seguinte:

- Certifique-se de usar o mesmo bucket do Amazon S3 especificado na política do IAM.
- Certifique-se de que sua função tem as permissões do exemplo a seguir:

  Example política de permissões

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

Substitua *bucket-name* pelo nome do bucket do Amazon S3.

Erro: O ARN da função não pode ser presumido

Solução: AWS IoT SiteWise não foi possível assumir a função do IAM em seu nome. Certifique-se de que seu perfil confia no seguinte serviço: `iotsitewise.amazonaws.com`. Para obter mais informações, consulte Não consigo presumir uma função em Guia do Usuário do IAM.

Erro: falha ao acessar o bucket entre regiões do Amazon S3

Solução: O bucket do Amazon S3 que você especificou está em uma região diferente AWS . Certifique-se de que seu bucket e AWS IoT SiteWise ativos do Amazon S3 estejam na mesma região.

Caminhos de arquivo e esquemas de dados salvos na camada fria

AWS IoT SiteWise armazena seus dados na camada fria replicando séries temporais, incluindo medições, métricas, transformações e agregados, além de definições de ativos e modelos de ativos. A seguir, descrevemos os caminhos de arquivo e os esquemas de dados enviados para a camada fria.

Tópicos

- Dados do equipamento (medições)
- Métricas, transformações e agregados

- Metadados de ativos
- Metadados de hierarquia de ativos
- Arquivos de índice de dados de armazenamento

Dados do equipamento (medições)

AWS IoT SiteWise exporta dados do equipamento (medições) para a camada fria uma vez a cada seis horas. Os dados brutos são salvos na camada fria no formato Apache AVRO (`.avro`).

Caminho do arquivo

AWS IoT SiteWise armazena dados do equipamento (medições) na camada fria usando o modelo a seguir.

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

Cada caminho de arquivo para dados brutos no Amazon S3 contém os seguintes componentes:

Componente do caminho	Descrição
`keyPrefix`	O prefixo do Amazon S3 que você especific ou na configuração de armazenamento. AWS IoT SiteWise O Amazon S3 usa o prefixo como nome de pasta no bucket.
`raw`	A pasta que armazena dados de séries temporais do equipamento (medições). A pasta `raw` é salva na pasta de prefixos.
`seriesBucket`	Um número hexadecimal entre 00 e ff. Esse número é derivado de `timeSeriesId` . Essa partição é usada para aumentar a taxa de transferência ao AWS IoT SiteWise gravar na camada fria. Ao usar o Amazon Athena para executar consultas, você pode usar a partição para particionamento refinado, a fim de melhorar o desempenho da consulta.

Componente do caminho	Descrição
	`seriesBucket` e `timeSeriesBucket` nos metadados do ativo são o mesmo número.
`startYear`	O ano do horário de início exclusivo associado aos dados de séries temporais.
`startMonth`	O mês do horário de início exclusivo associado aos dados de séries temporais.
`startDay`	O dia do mês do horário de início exclusivo associado aos dados de séries temporais.
`fileName`	O nome do arquivo usa o caractere sublinhado (_) como delimitador para separar: • O prefixo `raw`. • O valor `timeSeriesId` . • O carimbo de data e hora da época do horário de início exclusivo associado aos dados de séries temporais. • A qualidade dos dados. Valores válidos: `GOOD`, `BAD` e `UNCERTAIN` . Para obter mais informações, consulte AssetPropertyValor na referência AWS IoT SiteWise da API. O arquivo é salvo no formato `.avro` usando a compressão Rápida.

Example caminho do arquivo para dados brutos na camada fria

```
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

O esquema de dados brutos exportados para a camada fria contém os seguintes campos:

Nome do campo	Tipos suportados	Tipo padrão	Descrição
`seriesId`	`string`	N/A	A ID que identifica os dados de série temporais do equipamento (medições). Você pode usar esse campo para unir dados brutos e metadados de ativos em consultas.
`timeInSeconds`	`long`	N/D	O carimbo de data e hora, em segundos, no formato de época do Unix. Os dados fracionários de nanossegundos são fornecidos por `offsetInNanos` .
`offsetInNanos`	`long`	N/D	O deslocamento em nanossegundos de `timeInSeconds` .
`quality`	`string`	N/D	A qualidade do valor de série temporal.
`doubleValue`	`double` ou `null`	`null`	Dados de séries temporais tipo duplo (número de ponto flutuante).

Nome do campo	Tipos suportados	Tipo padrão	Descrição
`stringValue`	`string` ou `null`	`null`	Dados de séries temporais tipo string (sequência de caracteres).
`integerValue`	`int` ou `null`	`null`	Dados de séries temporais tipo inteiro (número inteiro).
`booleanValue`	`boolean` ou `null`	`null`	Dados de séries temporais tipo Booleanos (verdadeiro ou falso).
`jsonValue`	`string` ou `null`	`null`	Dados de séries temporais do tipo JSON (tipos de dados complexos armazenados como string).
`recordVersion`	`long` ou `null`	`null`	O número da versão para o registro. Você pode usar o número da versão para selecionar o registro mais recente. Os registros mais recentes têm números de versão maiores.

Example dados brutos na camada fria

```
{"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, transformações e agregados

AWS IoT SiteWise exporta métricas, transforma e agrega para o nível frio uma vez a cada seis horas. Métricas, transformações e agregados são salvos na camada fria, no formato Apache AVRO (`.avro`).

Caminho do arquivo

AWS IoT SiteWise armazena métricas, transformações e agregados na camada fria usando o modelo a seguir.

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

Cada caminho de arquivo para métricas, transformações e agregados no Amazon S3 contém os seguintes componentes:

Componente do caminho	Descrição
`keyPrefix`	O prefixo do Amazon S3 que você especific ou na configuração de armazenamento. AWS IoT SiteWise O Amazon S3 usa o prefixo como nome de pasta no bucket.
`agg`	A pasta que armazena dados de séries temporais das métricas. A pasta `agg` é salva na pasta de prefixos.

Componente do caminho	Descrição
`seriesBucket`	Um número hexadecimal entre 00 e ff. Esse número é derivado de `timeSeriesId` . Essa partição é usada para aumentar a taxa de transferência ao AWS IoT SiteWise gravar na camada fria. Ao usar o Amazon Athena para executar consultas, você pode usar a partição para particionamento refinado, a fim de melhorar o desempenho da consulta. `seriesBucket` e `timeSeriesBucket` nos metadados do ativo são o mesmo número.
`startYear`	O ano do horário de início exclusivo associado aos dados de séries temporais.
`startMonth`	O mês do horário de início exclusivo associado aos dados de séries temporais.
`startDay`	O dia do mês do horário de início exclusivo associado aos dados de séries temporais.

Componente do caminho	Descrição
`fileName`	O nome do arquivo usa o caractere sublinhado (_) como delimitador para separar: • O prefixo `raw`. • O valor `timeSeriesId` . • O carimbo de data e hora da época do horário de início exclusivo associado aos dados de séries temporais. • A qualidade dos dados. Valores válidos: `GOOD`, `BAD` e `UNCERTAIN` . Para obter mais informações, consulte AssetPropertyValor na referência AWS IoT SiteWise da API. O arquivo é salvo no formato `.avro` usando a compressão Rápida.

Example caminho do arquivo para métricas na camada fria

```
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

O esquema de métricas, transformações e agregados que são exportados para a camada fria contém os seguintes campos:

Nome do campo	Tipos suportados	Tipo padrão	Descrição
`seriesId`	`string`	N/D	A ID que identific a dados de séries temporais de equipamentos, métricas ou transform

Nome do campo	Tipos suportados	Tipo padrão	Descrição
			ações. Você pode usar esse campo para unir dados brutos e metadados de ativos em consultas.
`timeInSeconds`	`long`	N/D	O carimbo de data e hora, em segundos, no formato de época do Unix. Os dados fracionários de nanossegundos são fornecidos por `offsetInNanos` .
`offsetInNanos`	`long`	N/D	O deslocamento em nanossegundos de `timeInSeconds` .
`quality`	`string`	N/D	A qualidade pela qual filtram-se os dados de ativos.
`resolution`	`string`	N/D	O intervalo de tempo no qual agregam-se os dados.
`count`	`double` ou `null`	`null`	O número total de pontos de dados das variáveis fornecidas ao longo do intervalo de tempo atual.

Nome do campo	Tipos suportados	Tipo padrão	Descrição
`average`	`double` ou `null`	`null`	A média dos valores das variáveis fornecidas ao longo do intervalo de tempo atual.
`min`	`double` ou `null`	`null`	O valor mínimo dos valores das variáveis fornecidas ao longo do intervalo de tempo atual.
`max`	`boolean` ou `null`	`null`	O valor máximo das variáveis fornecidas ao longo do intervalo de tempo atual.
`sum`	`string` ou `null`	`null`	A soma dos valores das variáveis fornecidas ao longo do intervalo de tempo atual.
`recordVersion`	`long` ou `null`	`null`	O número da versão para o registro. Você pode usar o número da versão para selecionar o registro mais recente. Os registros mais recentes têm números de versão maiores.

Example Dados métricos na camada fria

```
{"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}
```

Metadados de ativos

Quando você ativa AWS IoT SiteWise a exportação de dados para a camada fria pela primeira vez, os metadados do ativo são exportados para a camada fria. Após a configuração inicial, AWS IoT SiteWise exporta metadados do ativo para a camada somente quando você altera as definições do modelo do ativo ou as definições do ativo. Os metadados do ativo são salvos na camada fria no formato JSON () delimitado por nova linha. `.ndjson`

Caminho do arquivo

AWS IoT SiteWise armazena metadados de ativos na camada fria usando o modelo a seguir.

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

Cada caminho de arquivo para metadados de ativos na camada fria contém os seguintes componentes:

Componente do caminho	Descrição
`keyPrefix`	O prefixo do Amazon S3 que você especificou na configuração de armazenamento AWS IoT SiteWise s. O Amazon S3 usa o prefixo como nome de pasta no bucket.
`asset_metadata`	A pasta que armazena os metadados do ativo. A pasta `asset_metadata` é salva na pasta de prefixos.
`fileName`	O nome do arquivo usa o caractere sublinhado (_) como delimitador para separar: • O prefixo `asset`. • O valor `assetId`. O arquivo é salvo no formato `.ndjson`.

Example caminho de arquivo para metadados de ativos na camada mais fria

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

Campos

O esquema dos metadados do ativo exportado para a camada fria contém os seguintes campos:

Nome do campo	Descrição
`assetId`	ID do ativo.
`assetName`	O nome do ativo.
`assetExternalId`	O ID externo do ativo.
`assetModelId`	ID do modelo de ativo usada para criá-lo.
`assetModelName`	O nome do modelo do ativo.

Nome do campo	Descrição
`assetModelExternalId`	O ID externo do modelo de ativo.
`assetPropertyId`	A ID da propriedade do ativo.
`assetPropertyName`	O nome da propriedade do ativo.
`assetPropertyExternalId`	O ID externo da propriedade do ativo.
`assetPropertyDataType`	O tipo de dados da propriedade do ativo.
`assetPropertyUnit`	A unidade da propriedade do ativo (por exemplo, `Newtons` e `RPM`).
`assetPropertyAlias`	O apelido que identifica a propriedade do ativo, como um caminho de fluxo de dados do servidor de OPC-UA (por exemplo, `/company/windfarm/3/turbine/7/temperature`).
`timeSeriesId`	A ID que identifica dados de séries temporais de equipamentos, métricas ou transformações. Você pode usar esse campo para unir dados brutos e metadados de ativos em consultas.
`timeSeriesBucket`	Um número hexadecimal entre 00 e ff. Esse número é derivado de `timeSeriesId` . Essa partição é usada para aumentar a taxa de transferência ao AWS IoT SiteWise gravar na camada fria. Ao usar o Amazon Athena para executar consultas, você pode usar a partição para particionamento refinado, a fim de melhorar o desempenho da consulta. `timeSeriesBucket` e `seriesBucket` no caminho do arquivo para os dados brutos são o mesmo número.

Nome do campo	Descrição
`assetCompositeModelId`	O ID do modelo composto.
`assetCompositeModelExternalId`	O ID externo do modelo composto.
`assetCompositeModelDescription`	A descrição do modelo composto.
`assetCompositeModelName`	O nome do modelo composto.
`assetCompositeModelType`	O tipo do modelo composto. Para modelos compostos de alarme, este tipo é `AWS/ALARM` .
`assetCreationDate`	A data na qual o ativo foi criado, no horário de época do Unix.
`assetLastUpdateDate`	A data na qual o ativo foi atualizado pela última vez, no horário de época do Unix.
`assetStatusErrorCode`	O código do erro.
`assetStatusErrorMessage`	A mensagem de erro.
`assetStatusState`	O status atual do ativo.

Example metadados de ativos na camada fria


```
  {"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
```


Metadados de hierarquia de ativos

Quando você ativa AWS IoT SiteWise para salvar dados na camada fria pela primeira vez, os metadados da hierarquia de ativos são exportados para a camada fria. Após a configuração inicial, AWS IoT SiteWise exporta os metadados da hierarquia de ativos para a camada fria somente quando você faz alterações no modelo do ativo ou nas definições do ativo. Os metadados da hierarquia de ativos são salvos na camada fria no formato JSON () delimitado por nova linha. `.ndjson`

Um identificador externo para a hierarquia, o ativo de destino ou o ativo de origem é recuperado chamando a DescribeAssetAPI.

Caminho do arquivo

AWS IoT SiteWise armazena metadados da hierarquia de ativos na camada fria usando o modelo a seguir.

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

Cada caminho de arquivo para metadados da hierarquia do ativo na camada fria contém os seguintes componentes:

Componente do caminho	Descrição
`keyPrefix`	O prefixo do Amazon S3 que você especific ou na configuração de armazenamento. AWS IoT SiteWise O Amazon S3 usa o prefixo como nome de pasta no bucket.
`asset_hierarchy_metadata`	A pasta que armazena os metadados da hierarquia do ativo. A pasta `asset_hie rarchy_metadata` é salva na pasta de prefixos.
`fileName`	O nome do arquivo usa o caractere sublinhado (_) como delimitador para separar: • O valor `parentAssetId` . • O valor `hierarchyId` . O arquivo é salvo no formato `.ndjson`.

Example caminho do arquivo para metadados da hierarquia do ativo na camada fria

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

Campos

O esquema dos metadados da hierarquia do ativo exportados para a camada fria contém os seguintes campos:

Nome do campo	Descrição
`sourceAssetId`	ID do ativo de origem nessa relação de ativos.
`targetAssetId`	ID do ativo de destino nessa relação de ativos.

Nome do campo	Descrição
`hierarchyId`	ID da hierarquia.
`associationType`	O tipo de associação dessa relação de ativos. O valor deve ser `CHILD`. O ativo de destino é um ativo filho do ativo de origem.

Example metadados da hierarquia do ativo na camada fria

```
{"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 visualizar seus dados na camada fria:

1. Navegue até o console do Amazon S3.
2. No painel de navegação, escolha Buckets e, em seguida, o bucket do Amazon S3.
3. Navegue até a pasta contendo os dados brutos, os metadados do ativo, ou os metadados da hierarquia do ativo.
4. Selecione os arquivos e em Ações, escolha Baixar.

Arquivos de índice de dados de armazenamento

AWS IoT SiteWise usa esses arquivos para otimizar o desempenho da consulta de dados. Eles aparecem no seu bucket do Amazon S3, mas você não precisa usá-los.

Caminho do arquivo

AWS IoT SiteWise armazena arquivos de índice de dados na camada fria usando o modelo a seguir.

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

Example caminho do arquivo para o arquivo de índice de armazenamento de dados

```
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
```

Segurança em AWS IoT SiteWise

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isso como a segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos AWS programas de de . Para saber mais sobre os programas de conformidade que se aplicam a AWS IoT SiteWise, consulte AWS serviços no escopo por programa de conformidade AWS .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar AWS IoT SiteWise. Os tópicos a seguir mostram como configurar para atender AWS IoT SiteWise aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus AWS IoT SiteWise recursos.

Tópicos

Proteção de dados em AWS IoT SiteWise

O modelo de responsabilidade AWS compartilhada modelo se aplica à proteção de dados em AWS IoT SiteWise. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para ter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para ter mais informações sobre a proteção de dados na Europa, consulte a AWS postagem do blog Shared Responsibility Model and GDPR no AWS Blog de segurança da.

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de email dos seus clientes, em marcações ou campos de formato livre, como um campo Name (Nome). Isso inclui quando você trabalha com AWS IoT SiteWise ou Serviços da AWS usa o console, a API ou AWS os SDKs. AWS CLI Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de

diagnóstico. Se você fornecer um URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Tópicos

Privacidade do tráfego entre redes

As conexões entre aplicativos locais AWS IoT SiteWise e aplicativos, como gateways SiteWise Edge, são protegidas por conexões TLS (Transport Layer Security). Para ter mais informações, consulte Criptografia em trânsito.

AWS IoT SiteWise não suporta conexões entre zonas de disponibilidade em uma AWS região ou conexões entre AWS contas.

Você pode configurar o Centro de identidade do IAM em apenas uma região de cada vez. SiteWise O Monitor se conecta à região que você configurou para o IAM Identity Center. Isso significa que você usa uma região para acessar o Centro de identidade do IAM, mas pode criar portais em qualquer região.

Criptografia de dados

A criptografia de dados se refere à proteção de dados em trânsito (à medida que viajam de AWS IoT SiteWise e para e entre os gateways e servidores do SiteWise Edge) e em repouso (enquanto são armazenados em dispositivos locais ou em AWS serviços). É possível proteger dados em trânsito usando TLS (Transport Layer Security) ou em repouso usando criptografia do lado do cliente.

> **Note**
>
> AWS IoT SiteWise o processamento de borda expõe APIs hospedadas nos gateways do SiteWise Edge e acessíveis pela rede local. Essas APIs são expostas por meio de uma conexão TLS apoiada por um certificado de servidor de propriedade do conector Edge. AWS IoT SiteWise Para autenticação do cliente, essas APIs utilizam uma senha de controle de acesso. A chave privada do certificado do servidor e a senha de controle de acesso são armazenadas em disco. AWS IoT SiteWise o processamento de borda depende da criptografia do sistema de arquivos para a segurança dessas credenciais em repouso.

Para obter mais informações sobre criptografia do lado do servidor e criptografia do lado do cliente, consulte os tópicos listados abaixo.

Tópicos

Criptografia inativa

AWS IoT SiteWise armazena seus dados na AWS nuvem e nos gateways AWS IoT SiteWise Edge.

Dados em repouso na AWS nuvem

AWS IoT SiteWise armazena dados em outros AWS serviços que criptografam dados em repouso por padrão. A criptografia em repouso se integra com AWS Key Management Service (AWS KMS) para gerenciar a chave de criptografia usada para criptografar os valores das propriedades do seu ativo e agregar valores em. AWS IoT SiteWise Você pode optar por usar uma chave gerenciada pelo cliente para criptografar valores de propriedades do ativo e agregar valores em AWS IoT SiteWise. Você pode criar, gerenciar e visualizar sua chave de criptografia por meio do AWS KMS.

Você pode escolher uma Chave pertencente à AWS para criptografar seus dados ou escolher uma chave gerenciada pelo cliente para criptografar os valores das propriedades do seu ativo e valores agregados:

Como funciona

A criptografia em repouso se AWS KMS integra ao gerenciamento da chave de criptografia usada para criptografar seus dados.

- Chave pertencente à AWS — Chave de criptografia padrão. AWS IoT SiteWise possui essa chave. Você não pode ver essa chave na sua AWS conta. Você também não pode ver operações na chave nos logs de AWS CloudTrail . Você pode usar esta chave sem custo adicional.
- Chave gerenciada pelo cliente – A chave é armazenada na sua conta e é você que a cria, detém e gerencia. Você tem controle total sobre a chave KMS. AWS KMS Taxas adicionais se aplicam.

Chaves pertencentes à AWS

Chaves pertencentes à AWS não estão armazenados em sua conta. Elas fazem parte de uma coleção de chaves KMS que AWS possui e gerencia para uso em várias AWS contas. AWS serviços que você pode Chaves pertencentes à AWS usar para proteger seus dados.

Você não pode visualizar, gerenciar Chaves pertencentes à AWS, usar ou auditar seu uso. No entanto, você não precisa fazer nenhum trabalho nem alterar nenhum programa para proteger as chaves que criptografam seus dados.

Não é cobrada uma taxa mensal ou uma taxa de uso se você usar Chaves pertencentes à AWS, e elas não contam nas AWS KMS cotas da sua conta.

Chaves gerenciadas pelo cliente

Chaves gerenciadas pelo cliente são chaves do KMS disponíveis na sua conta do que você cria, detém e gerencia. Você tem controle total sobre as chaves KMS, como as seguintes:

- Estabelecer e manter políticas de chaves, políticas do IAM e concessões
- Ativação e desativação das chaves
- Alternar os materiais de criptografia das chaves
- Adicionar etiquetas
- Criar aliases que se referem as chaves
- Agendá-las para exclusão

Você também pode usar CloudTrail o Amazon CloudWatch Logs para rastrear as solicitações AWS IoT SiteWise enviadas para AWS KMS você.

Se você estiver usando chaves gerenciadas pelo cliente, precisará conceder AWS IoT SiteWise acesso à chave KMS armazenada em sua conta. AWS IoT SiteWise usa criptografia de envelope e hierarquia de chaves para criptografar dados. Sua chave de AWS KMS criptografia é usada para criptografar a chave raiz dessa hierarquia de chaves. Para obter mais informações, consulte Criptografia envelopada no Guia do desenvolvedor do AWS Key Management Service .

O exemplo de política a seguir concede AWS IoT SiteWise permissões para criar uma chave gerenciada pelo cliente em seu nome. Ao criar sua chave, você precisa permitir as ações de `kms:CreateGrant` e `kms:DescribeKey`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1603902045292",
      "Action": [
        "kms:CreateGrant",
        "kms:DescribeKey"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

O contexto de criptografia para a concessão criada usa sua `aws:iotsitewise:subscriberId` e ID da conta.

Dados em repouso nos gateways SiteWise Edge

AWS IoT SiteWise os gateways armazenam os seguintes dados no sistema de arquivos local:

- Informações de configuração de fonte OPC-UA
- O conjunto de caminhos de stream de dados OPC-UA de origens OPC-UA conectadas
- Dados industriais armazenados em cache quando o gateway SiteWise Edge perde a conexão com a Internet

SiteWise Os gateways Edge são executados. AWS IoT Greengrass AWS IoT Greengrass depende das permissões de arquivo Unix e da criptografia de disco inteiro (se ativada) para proteger os dados em repouso no núcleo. É sua responsabilidade proteger o sistema de arquivos e o dispositivo.

No entanto, AWS IoT Greengrass criptografa cópias locais dos segredos do servidor OPC-UA recuperados do Secrets Manager. Para obter mais informações, consulte Criptografia de segredos no Guia do Desenvolvedor do AWS IoT Greengrass Version 1 .

Para obter mais informações sobre criptografia em repouso em AWS IoT Greengrass núcleos, consulte Criptografia em repouso no Guia do AWS IoT Greengrass Version 1 desenvolvedor.

Criptografia em trânsito

AWS IoT SiteWise tem três modos de comunicação em que os dados estão em trânsito:

- Pela Internet — Comunicação entre dispositivos locais (incluindo gateways SiteWise Edge) e AWS IoT SiteWise é criptografada.
- OpsHub Pela rede local — A comunicação entre o SiteWise aplicativo e os gateways SiteWise Edge é sempre criptografada. A comunicação entre o aplicativo de SiteWise monitoramento em execução no seu navegador e os gateways do SiteWise Edge é sempre criptografada. A comunicação entre os gateways SiteWise Edge e as fontes OPC-UA pode ser criptografada.
- Entre componentes nos gateways SiteWise Edge — A comunicação entre AWS IoT Greengrass componentes nos gateways SiteWise Edge não é criptografada.

Tópicos

Dados em trânsito pela Internet

AWS IoT SiteWise usa Transport Layer Security (TLS) para criptografar toda a comunicação pela Internet. Todos os dados enviados para a AWS nuvem são enviados por uma conexão TLS usando os protocolos MQTT ou HTTPS, portanto, são seguros por padrão. SiteWise Os gateways de borda, que são executados em AWS IoT Greengrass, e as notificações de valor de propriedade usam o modelo de segurança de AWS IoT transporte. Para obter mais informações, consulte Segurança de transporte no Guia do desenvolvedor do AWS IoT .

Dados em trânsito por meio da rede local

SiteWise Os gateways Edge seguem as especificações OPC-UA para comunicação com fontes OPC-UA locais. É sua responsabilidade configurar suas origens para usarem um modo de segurança de mensagens que criptografa dados em trânsito.

Se você escolher um modo de segurança de mensagem de assinatura, os dados em trânsito entre os gateways e as fontes do SiteWise Edge serão assinados, mas não criptografados. Se você escolher um modo de segurança de mensagem de assinatura e criptografia, os dados em trânsito

entre os gateways e as fontes do SiteWise Edge serão assinados e criptografados. Para obter mais informações sobre como configurar origens, consulte Configurar fontes de dados.

A comunicação entre o aplicativo do console de borda e os gateways do SiteWise Edge é sempre criptografada pelo TLS. O conector SiteWise SiteWise Edge no gateway Edge gera e armazena um certificado autoassinado para poder estabelecer uma conexão TLS com o console de borda para AWS IoT SiteWise aplicação. Você precisará copiar esse certificado do seu gateway SiteWise Edge para o console de borda do AWS IoT SiteWise aplicativo antes de conectar o aplicativo ao gateway SiteWise Edge. Isso garante que o console de borda do AWS IoT SiteWise aplicativo seja capaz de verificar se ele está conectado ao seu gateway SiteWise Edge confiável.

Além do TLS para sigilo e autenticidade do servidor, o SiteWise Edge usa o protocolo SigV4 para estabelecer a autenticidade do aplicativo do console de borda. O conector SiteWise Edge no gateway SiteWise Edge aceita e armazena uma senha para poder verificar as conexões de entrada do aplicativo do console de borda, SiteWise monitorar o aplicativo em execução nos navegadores e outros clientes com base no AWS IoT SiteWise SDK.

Para obter mais informações sobre como gerar a senha e o certificado do servidor, consulte the section called “Gerenciando gateways SiteWise Edge”

Dados em trânsito entre componentes locais nos gateways SiteWise Edge

SiteWise Os gateways Edge são executados AWS IoT Greengrass, o que não criptografa os dados trocados localmente no AWS IoT Greengrass núcleo porque os dados não saem do dispositivo. Isso inclui a comunicação entre AWS IoT Greengrass componentes, como o AWS IoT SiteWise conector. Para obter mais informações, consulte Dados no dispositivo de núcleo no Guia do desenvolvedor do AWS IoT Greengrass Version 1 .

Gerenciamento de chaves

AWS IoT SiteWise gerenciamento de chaves na nuvem

Por padrão, AWS IoT SiteWise usa Chaves gerenciadas pela AWS para proteger seus dados na AWS nuvem. É possível atualizar suas configurações para usar uma chave gerenciada pelo cliente para criptografar alguns dados em AWS IoT SiteWise. Você pode criar, gerenciar e visualizar sua chave de criptografia por meio do AWS Key Management Service (AWS KMS).

AWS IoT SiteWise oferece suporte à criptografia do lado do servidor com chaves gerenciadas pelo cliente armazenadas AWS KMS para criptografar os seguintes dados:

- Valores de propriedade de ativos
- Valores agregados

> **Note**
>
> Outros dados e recursos são criptografados usando a criptografia padrão com chaves gerenciadas por AWS IoT SiteWise. Essa chave é armazenada na conta de AWS IoT SiteWise .

Para obter mais informações, consulte O que é AWS Key Management Service? no Guia do AWS Key Management Service desenvolvedor.

Habilite a criptografia usando chaves gerenciadas pelo cliente

Para usar chaves gerenciadas pelo cliente com AWS IoT SiteWise, você precisa atualizar suas AWS IoT SiteWise configurações.

Para habilitar a criptografia usando chaves KMS

1. Navegue até o console do AWS IoT SiteWise.
2. Escolha Configurações da conta e escolha Editar para abrir a página Editar configurações da conta.
3. Em Tipo de chave de criptografia, escolha Escolher uma chave de AWS KMS diferente. Isso habilita a criptografia com chaves gerenciadas pelo cliente armazenadas em AWS KMS.

   > **Note**
   >
   > Atualmente, você só pode usar a criptografia de chave gerenciada pelo cliente para valores de propriedade do ativo e valores agregados.

4. Escolha a Chave KMS através de uma das opções a seguir:
   - Para usar uma chave KMS existente — Escolha o alias da chave KMS na lista.
   - Para criar uma nova chave KMS — Escolha Criar uma AWS KMS chave.

> **Note**
>
> Isso abre o AWS KMS Painel. Para obter mais informações sobre como criar chaves KMS, consulte Criar chaves no Guia do desenvolvedor do AWS Key Management Service .

5. Selecione Salvar para atualizar as configurações.

SiteWise Gerenciamento de chaves do Edge Gateway

SiteWise Os gateways Edge são executados AWS IoT Greengrass e os dispositivos AWS IoT Greengrass principais usam chaves públicas e privadas para se autenticar na AWS nuvem e criptografar segredos locais, como segredos de autenticação OPC-UA. Para obter mais informações, consulte Gerenciamento de chaves no Guia do desenvolvedor do AWS IoT Greengrass Version 1 .

Gerenciamento de identidade e acesso para AWS IoT SiteWise

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar AWS IoT SiteWise os recursos. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz AWS IoT SiteWise.

Usuário do serviço — Se você usar o AWS IoT SiteWise serviço para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais AWS IoT SiteWise recursos para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudá-lo a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um recurso no AWS IoT SiteWise, consulte Solução de problemas AWS IoT SiteWise de identidade e acesso.

Administrador de serviços — Se você é responsável pelos AWS IoT SiteWise recursos da sua empresa, provavelmente tem acesso total AWS IoT SiteWise a. É seu trabalho determinar quais AWS IoT SiteWise recursos e recursos seus usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como sua empresa pode usar o IAM com AWS IoT SiteWise, consulteComo AWS IoT SiteWise funciona com o IAM.

Administrador do IAM: Se você for um administrador do IAM, talvez queira saber detalhes sobre como pode gravar políticas para gerenciar acesso ao AWS IoT SiteWise. Para ver exemplos de políticas AWS IoT SiteWise baseadas em identidade que você pode usar no IAM, consulte. AWS IoT SiteWise exemplos de políticas baseadas em identidade

Autenticando com identidades

A autenticação é como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login em AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinatura de solicitações de AWS API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação Multifator no AWS IAM Identity Center Guia do Usuário. Usar a autenticação multifator (MFA) na AWS no Guia do Usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele pode executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do usuário do IAM.

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos depender de credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne Chaves de Acesso Regularmente para Casos de Uso que exijam Credenciais de Longo Prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários

usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um nome de grupo IAMAdmins e atribuir a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a um aplicativo, mas uma função pode ser assumida por qualquer pessoa que precisar dela. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando Criar um Usuário do IAM (Ao Invés de uma Função) no Guia do Usuário do IAM.

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma função do IAM no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para usar perfis, consulte Usando Funções do IAM no Guia do Usuário do IAM.

Funções do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte Criando um Perfil para um Provedor de Identidades Terceirizado no Guia do Usuário do IAM. Se você usa o IAM Identity Center, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no AWS IAM Identity Center Manual do Usuário.
- Permissões de usuários temporárias do IAM: um usuário ou perfil do IAM pode assumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: você pode usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) acesse recursos na sua conta de uma conta diferente. As funções são a forma primária de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para aprender a diferença entre funções e políticas baseadas em recurso para acesso entre contas,

consulte Como as Funções do IAM Diferem das Políticas Baseadas em Recurso no Guia do Usuário do IAM.

- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões de chamada da entidade principal, uma função de serviço ou uma função vinculada ao serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.
  - Função de Serviço: uma função de serviço é uma função do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criando um Perfil para Delegar Permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.
  - Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para funções vinculadas a serviço.
- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Usar uma função do IAM para conceder permissões a aplicativos em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para aprender se deseja usar perfis do IAM, consulte Quando Criar uma Função do IAM (em Vez de um Usuário) no Guia do Usuário do IAM.

Como AWS IoT SiteWise funciona com o IAM

Antes de usar o AWS Identity and Access Management (IAM) para gerenciar o acesso AWS IoT SiteWise, você deve entender quais recursos do IAM estão disponíveis para uso AWS IoT SiteWise.

Atributo do IAM	Apoiado por AWS IoT SiteWis
Políticas baseadas em identidade com permissões em nível de recurso	Sim
Ações das políticas	Sim
atributos de políticas	Sim
Chaves de condição de políticas	Sim
Políticas baseadas em recursos	Não
Listas de controle de acesso (ACLs)	Não
Autorização baseada em tags (ABAC)	Sim
Credenciais temporárias	Sim
Sessões de acesso direto (FAS)	Sim
Funções vinculadas a serviço	Sim
Perfis de serviço	Sim

Para ter uma visão de alto nível de como AWS IoT SiteWise e outros AWS serviços funcionam com o IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

Sumário

AWS IoT SiteWise Funções do IAM

Um perfil do IAM é uma entidade dentro da sua Conta da AWS que tem permissões específicas.

Usando credenciais temporárias com AWS IoT SiteWise

É possível usar credenciais temporárias para fazer login com federação, assumir um perfil do IAM ou assumir um perfil entre contas. Você obtém credenciais de segurança temporárias chamando operações de AWS STS API, como AssumeRoleou GetFederationToken.

AWS IoT SiteWise suporta o uso de credenciais temporárias.

SiteWise O Monitor oferece suporte a usuários federados para acessar portais. Os usuários do portal são autenticados com suas credenciais do IAM Identity Center ou do IAM.

> **Important**
>
> Usuários ou perfis devem ter a permissão de `iotsitewise:DescribePortal` para entrar no portal.

Quando um usuário entra em um portal, o SiteWise Monitor gera uma política de sessão que fornece as seguintes permissões:

- Acesso somente para leitura aos ativos e dados do ativo AWS IoT SiteWise em sua conta à qual a função desse portal fornece acesso.
- Acesso a projetos nesse portal aos quais o usuário tem acesso de administrador (proprietário do projeto) ou somente leitura (visualizador do projeto).

Para obter mais informações sobre permissões de usuário federado do portal, consulte Usando funções de serviço para AWS IoT SiteWise Monitor.

Sessões de acesso direto (FAS) para AWS IoT SiteWise

Suporte para o recurso Encaminhamento de sessões de acesso (FAS)	Sim

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado um principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos

serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.

Funções vinculadas a serviço

As funções vinculadas ao serviço permitem que AWS os serviços acessem recursos em outros serviços para concluir uma ação em seu nome. Funções vinculadas ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados a serviço.

AWS IoT SiteWise oferece suporte a funções vinculadas a serviços. Para obter detalhes sobre como criar ou gerenciar perfis vinculados a serviço do AWS IoT SiteWise , consulte Usar perfis vinculados ao serviço do AWS IoT SiteWise.

Perfis de serviço

Esse atributo permite que um serviço assuma um perfil de serviço em seu nome. O perfil permite que o serviço acesse recursos em outros serviços para concluir uma ação em seu nome. Os perfis de serviço aparecem em Conta da AWS e são de propriedade da conta. Isso indica que um administrador do IAM pode alterar as permissões para essa função. Porém, fazer isso pode alterar a funcionalidade do serviço.

AWS IoT SiteWise usa uma função de serviço para permitir que os usuários do portal SiteWise Monitor acessem alguns de seus AWS IoT SiteWise recursos em seu nome. Para ter mais informações, consulte Usando funções de serviço para AWS IoT SiteWise Monitor.

Você deve ter as permissões necessárias antes de poder criar modelos de AWS IoT Events alarme no AWS IoT SiteWise. Para ter mais informações, consulte Configurando permissões para AWS IoT Events alarmes.

Selecionar um perfil do IAM no AWS IoT SiteWise

Ao criar um `portal` recurso no AWS IoT SiteWise, você deve escolher uma função para permitir que os usuários federados do seu portal SiteWise Monitor AWS IoT SiteWise acessem em seu nome. Se você já criou uma função de serviço, AWS IoT SiteWise fornece uma lista de funções para escolher. Caso contrário, crie uma função com as permissões necessárias ao criar um portal. É importante escolher uma função que permita acesso aos seus ativos e aos dados dos ativos. Para ter mais informações, consulte Usando funções de serviço para AWS IoT SiteWise Monitor.

Autorização baseada em tags do AWS IoT SiteWise

Você pode anexar tags a AWS IoT SiteWise recursos ou passar tags em uma solicitação para AWS IoT SiteWise. Para controlar o acesso baseado em tags, forneça informações sobre a tag no elemento de condição de uma política usando as chaves de condição `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`. Para obter mais informações sobre recursos de marcação do AWS IoT SiteWise , consulte Marcando seus recursos AWS IoT SiteWise.

Para visualizar um exemplo de política baseada em identidade para limitar o acesso a um recurso baseado em tags desse recurso, consulte Visualizar ativos do AWS IoT SiteWise com base em tags.

AWS IoT SiteWise políticas baseadas em identidade

As políticas do IAM permitem que você controle quem pode fazer o quê AWS IoT SiteWise. Você pode decidir quais ações são permitidas ou não e definir condições específicas para essas ações. Por exemplo, você pode criar regras sobre quem pode ver ou alterar as informações AWS IoT SiteWise. AWS IoT SiteWise oferece suporte a ações, recursos e chaves de condição específicos. Para saber mais sobre todos os elementos usados em uma política JSON, consulte Referência de elementos de política JSON do IAM no Guia do usuário do IAM.

Ações das políticas

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Há também algumas operações que exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

As ações políticas AWS IoT SiteWise usam o seguinte prefixo antes da ação:`iotsitewise:`. Por exemplo, para conceder permissão a alguém para fazer upload de dados de propriedades de ativos AWS IoT SiteWise com a operação da `BatchPutAssetPropertyValue` API, você inclui a `iotsitewise:BatchPutAssetPropertyValue` ação na política dessa pessoa. As declarações de política devem incluir um `NotAction` elemento `Action` ou. AWS IoT SiteWise define seu próprio conjunto de ações que descrevem as tarefas que você pode executar com esse serviço.

Para especificar várias ações em uma única declaração, separe-as com vírgulas, conforme a seguir.

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

Você também pode especificar várias ações utilizando caracteres curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `Describe`, inclua a ação a seguir:

```
"Action": "iotsitewise:Describe*"
```

Para ver uma lista de AWS IoT SiteWise ações, consulte Ações definidas por AWS IoT SiteWise no Guia do usuário do IAM.

BatchPutAssetPropertyValue autorização

AWS IoT SiteWise autoriza o acesso à ação BatchPutAssetPropertyValue de uma forma incomum. Para a maioria das ações, quando você permite ou nega acesso, essa ação retorna um erro se as permissões não forem concedidas. Com`BatchPutAssetPropertyValue`, você pode enviar várias entradas de dados para diferentes ativos e propriedades de ativos em uma única solicitação de API. AWS IoT SiteWise autoriza cada entrada de dados de forma independente. Para qualquer entrada individual que falhe na autorização na solicitação, AWS IoT SiteWise inclua um `AccessDeniedException` na lista de erros retornada. AWS IoT SiteWise recebe os dados de qualquer entrada autorizada e bem-sucedida, mesmo que outra entrada na mesma solicitação falhe.

> **Important**
>
> Antes de ingerir dados em um stream de dados, faça o seguinte:
>
> - Autorize o `time-series` recurso se você usar um alias de propriedade para identificar o fluxo de dados.
> - Autorize o `asset` recurso se você usar uma ID de ativo para identificar o ativo que contém a propriedade do ativo associada.

atributos de políticas

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Resource` de política JSON especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou um elemento `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem suporte a um tipo de atributo específico, conhecido como permissões em nível de atributo.

Para ações não compatíveis com permissões no nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Cada declaração de política do IAM se aplica aos recursos que você especifica usando os ARNs. Um ARN tem a seguinte sintaxe geral.

```
arn:${Partition}:${Service}:${Region}:${Account}:${ResourceType}/${ResourcePath}
```

Para obter mais informações sobre o formato dos ARNs, consulte Amazon Resource Names (ARNs) e namespaces AWS de serviços.

Por exemplo, para especificar ativo com o ID `a1b2c3d4-5678-90ab-cdef-22222EXAMPLE` em sua instrução, use o seguinte ARN.

```
"Resource": "arn:aws:iotsitewise:region:123456789012:asset/a1b2c3d4-5678-90ab-
cdef-22222EXAMPLE"
```

Para especificar todos os fluxos de dados que pertencem a uma conta específica, use o caractere curinga (*):

```
"Resource": "arn:aws:iotsitewise:region:123456789012:time-series/*"
```

Para especificar todos os ativos que pertencem a uma conta específica, use o caractere curinga (*):

```
"Resource": "arn:aws:iotsitewise:region:123456789012:asset/*"
```

Algumas AWS IoT SiteWise ações, como as de criação de recursos, não podem ser executadas em um recurso específico. Nesses casos, você deve utilizar o caractere curinga (*).

```
"Resource": "*"
```

Para especificar vários recursos em uma única instrução, separe os ARNs com vírgulas.

```
"Resource": [
  "resource1",
  "resource2"
]
```

Para ver uma lista dos tipos de AWS IoT SiteWise recursos e seus ARNs, consulte Resources Defined by AWS IoT SiteWise no Guia do usuário do IAM. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas pelo AWS IoT SiteWise.

Chaves de condição de políticas

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual principal pode executar ações em quais recursos, e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite especificar condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. Você pode criar expressões condicionais que usem operadores de condição, como “igual a” ou “menor que”, para corresponder a condição da política aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um atributo somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos de Política do IAM: Variáveis e Tags no Guia do Usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

> **Important**
>
> Muitas chaves de condição são específicas a um recurso, e algumas ações da API usam vários recursos. Se você gravar uma declaração de política com uma chave de condição, use o elemento `Resource` da declaração para especificar o recurso ao qual a chave de condição

se aplica. Caso contrário, a política pode impedir que os usuários executem a ação, porque a verificação da condição falhará para os recursos aos quais a chave de condição não se aplica. Se você não quiser especificar um recurso, ou se escreveu o elemento `Action` da política para incluir várias ações da API, use o tipo de condição `...IfExists` para garantir que a chave de condição seja ignorada pelos recursos que não a usam. Para obter mais informações, consulte... IfExists condições no Guia do usuário do IAM.

AWS IoT SiteWise define seu próprio conjunto de chaves de condição e também oferece suporte ao uso de algumas chaves de condição globais. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

AWS IoT SiteWise chaves de condição

Chave de condição	Descrição	Tipos
`iotsitewise:isAssociatedWithAssetProperty`	Se os fluxos de dados estão associados a uma proprieda de do ativo. Use essa chave de condição para definir permissões com base na existência de uma propriedade do ativo associada ao fluxo de dados. Valor de exemplo: `true`	String
`iotsitewise:assetHierarchyPath`	O caminho da hierarquia do ativo, que é uma string de IDs de ativos separados por uma barra. Use essa chave de condição para definir permissões com base em um subconjunto da hierarquia de todos os ativos em sua conta. Valor de exemplo: `/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE/`	String

Chave de condição	Descrição	Tipos
	`a1b2c3d4-5678-90ab-cdef-66666EXAMPLE`	
`iotsitewise:propertyId`	O ID de uma propriedade de ativo. Use essa chave de condição para definir permissões com base em uma propriedade especificada de um modelo de ativo. Esta chave de condição aplica-se a todos os ativos desse modelo. Valor de exemplo: `a1b2c3d4-5678-90ab-cdef-33333EXAMPLE`	String
`iotsitewise:childAssetId`	ID de um ativo que está sendo associado como filho a outro ativo. Use essa chave de condição para definir permissões com base em ativos filhos. Para definir permissões com base em ativos pai, use a seção de recurso de uma declaração de política. Valor de exemplo: `a1b2c3d4-5678-90ab-cdef-66666EXAMPLE`	String

Chave de condição	Descrição	Tipos
`iotsitewise:iam`	O ARN de uma identidade do IAM ao listar políticas de acesso. Utilize essa chave de condição para definir permissões de política de acesso para uma identidade do IAM. Valor de exemplo: `arn:aws:iam::123456789012:user/JohnDoe`	Sequência, nula
`iotsitewise:propertyAlias`	O alias que identifica uma propriedade do ativo ou fluxo de dados. Use essa chave de condição para definir permissões com base no alias.	String
`iotsitewise:user`	O ID de um usuário do IAM Identity Center ao listar políticas de acesso. Utilize essa chave de condição para definir permissões de política de acesso para um usuário do IAM Identity Center. Valor de exemplo: `a1b2c3d4e5-a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE`	Sequência, nula

Chave de condição	Descrição	Tipos
`iotsitewise:group`	O ID de um grupo do IAM Identity Center ao listar políticas de acesso. Utilize essa chave de condição para definir permissões de política de acesso para um grupo do IAM Identity Center. Valor de exemplo: `a1b2c3d4e5-a1b2c3d4-5678-90ab-cdef-bbbbbEXAMPLE`	Sequência, nula
`iotsitewise:portal`	O ID de um portal em uma política de acesso. Use essa chave de condição para definir permissões de política de acesso com base em um portal. Valor de exemplo: `a1b2c3d4-5678-90ab-cdef-77777EXAMPLE`	Sequência, nula
`iotsitewise:project`	O ID de um projeto em uma política de acesso ou o ID de um projeto de um painel. Use essa chave de condição para definir permissões de painel ou política de acesso com base em um projeto. Valor de exemplo: `a1b2c3d4-5678-90ab-cdef-88888EXAMPLE`	Sequência, nula

Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas por AWS IoT SiteWise.

Exemplos

Para ver exemplos de políticas AWS IoT SiteWise baseadas em identidade, consulte. AWS IoT SiteWise exemplos de políticas baseadas em identidade

AWS IoT SiteWise exemplos de políticas baseadas em identidade

Por padrão, entidades (usuários e funções) não têm permissão para criar ou modificar AWS IoT SiteWise recursos. Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para ajustar as permissões, um administrador AWS Identity and Access Management (IAM) deve fazer o seguinte:

1. Crie políticas do IAM que concedam aos usuários e funções permissão para realizar operações de API específicas nos recursos de que precisam.
2. Anexe essas políticas aos usuários ou grupos que exigem essas permissões.

Para saber como criar uma política baseada em identidade do IAM utilizando esses exemplos de documentos de política JSON, consulte Criar políticas na guia JSON no Guia do usuário do IAM.

Tópicos

- Melhores práticas de política
- Usar o console do AWS IoT SiteWise
- Permitir que os usuários visualizem suas próprias permissões
- Permitir que os usuários consumam dados em ativos em uma hierarquia
- Visualizar ativos do AWS IoT SiteWise com base em tags

Melhores práticas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir AWS IoT SiteWise recursos em sua conta. Essas ações podem incorrer em custos para seus Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas

AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte Políticas Gerenciadas pela AWS ou AWS Políticas Gerenciadas para Funções de Trabalho no Guia do Usuário do IAM.

- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e Permissões no IAM no Guia do Usuário do IAM.
- Utilize condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode gravar uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte Condição de Elementos de Política JSON do IAM no Guia do Usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM para garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam o idioma de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e ações recomendadas para ajudar você a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de Política do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configurando Acesso à API Protegido por MFA no Guia do Usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas Recomendadas de Segurança no IAM no Guia do Usuário do IAM.

Usar o console do AWS IoT SiteWise

Para acessar o AWS IoT SiteWise console, você precisa de um conjunto básico de permissões. Essas permissões permitem que você veja e gerencie detalhes sobre os AWS IoT SiteWise recursos em seu Conta da AWS.

Se você criar uma política muito restritiva, o console poderá não funcionar conforme o esperado para usuários ou funções (entidades) com essa política. Para garantir que essas entidades ainda possam usar o AWS IoT SiteWise console, anexe a política AWSIoTSiteWiseConsoleFullAccessgerenciada a elas ou defina permissões equivalentes para essas entidades. Para obter mais informações, consulte Adicionando Permissões a um Usuário no Guia do Usuário do IAM.

Se as entidades estiverem usando apenas a AWS Command Line Interface (CLI) ou a AWS IoT SiteWise API, e não o console, elas não precisarão dessas permissões mínimas. Nesse caso, basta dar a eles acesso às ações específicas de que precisam para suas tarefas de API.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou 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 que os usuários consumam dados em ativos em uma hierarquia

Neste exemplo, você deseja conceder a um usuário em seu Conta da AWS acesso para gravar dados em todas as propriedades do ativo em uma hierarquia específica de ativos, começando pelo ativo `a1b2c3d4-5678-90ab-cdef-22222EXAMPLE` raiz. A política concede a permissão `iotsitewise:BatchPutAssetPropertyValue` ao usuário. Essa política usa a chave de condição `iotsitewise:assetHierarchyPath` para restringir o acesso a ativos cujo caminho de hierarquia corresponde ao ativo ou a seus descendentes.

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

Visualizar ativos do AWS IoT SiteWise com base em tags

Use condições em sua política baseada em identidade para controlar o acesso a AWS IoT SiteWise recursos com base em tags. Este exemplo mostra como criar uma política que permita a visualização de ativos. No entanto, a permissão será concedida somente se a tag do ativo do `Owner` tiver o valor do nome de usuário desse usuário. Essa política também concede permissão para concluir essa ação no console.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAllAssets",
      "Effect": "Allow",
      "Action": [
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DescribeAssetIfOwner",
      "Effect": "Allow",
      "Action": "iotsitewise:DescribeAsset",
      "Resource": "arn:aws:iotsitewise:*:*:asset/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Owner": "${aws:username}"
        }
      }
    }
  ]
}
```

Anexe essa política aos usuários da sua conta. Se um usuário chamado `richard-roe` tentar visualizar um AWS IoT SiteWise ativo, o ativo deverá ser marcado com `Owner=richard-roe` ou`owner=richard-roe`. Caso contrário, o acesso de Richard é negado. Os nomes das chaves da etiqueta de condição não diferenciam maiúsculas de minúsculas. Então, `Owner` combina com `Owner` `owner` e. Para obter mais informações, consulte IAM JSON Policy Elements: Condition (Elementos da política JSON do IAM: Condição) no Guia do usuário do IAM.

Gerenciando acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão Geral das Políticas JSON no Guia do Usuário do IAM.

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissão para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM às funções e os usuários podem assumir as funções.

As políticas do IAM definem permissões para uma ação, independente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em quais condições. Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

As políticas baseadas em identidade também podem ser categorizadas como políticas em linha ou políticas gerenciadas. As políticas em linha são incorporadas diretamente a um único usuário, grupo ou função. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como selecionar entre uma política gerenciada ou uma política em linha, consulte Selecionar entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de função do IAM e as políticas do bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificada pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em atributos são políticas em linha que estão localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou funções da conta) têm permissão para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS WAF Saiba mais sobre ACLs em Configurações da lista de controle de acesso (ACL) no Guia do Desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um recurso avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade e dos seus limites de permissões. As políticas baseadas em atributo que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de Permissões para Entidades do IAM no Guia do Usuário do IAM.
- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em. AWS

Organizations AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizações e SCPs, consulte Como os SCPs Funcionam no AWS Organizations Manual do Usuário do.

- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para uma função ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

AWS políticas gerenciadas para AWS IoT SiteWise

Simplifique a adição de permissões a usuários, grupos e funções usando políticas AWS gerenciadas em vez de escrever políticas você mesmo. É preciso tempo e experiência para criar políticas gerenciadas pelo cliente do IAM que forneçam permissões precisas à sua equipe. Para uma configuração mais rápida, considere usar nossas políticas AWS gerenciadas para casos de uso comuns. Encontre políticas AWS gerenciadas em seu Conta da AWS. Para obter mais informações sobre as políticas gerenciadas da AWS , consulte Políticas gerenciadas da AWS no IAM User Guide.

AWS os serviços cuidam da atualização e manutenção das políticas AWS gerenciadas, o que significa que você não pode modificar as permissões dessas políticas. Ocasionalmente, AWS IoT SiteWise pode adicionar permissões para acomodar novos recursos, afetando todas as identidades com a política anexada. Essas atualizações são comuns com a introdução de novos serviços ou recursos. No entanto, as permissões nunca são removidas, garantindo que suas configurações permaneçam intactas.

Além disso, AWS oferece suporte a políticas gerenciadas para funções de trabalho que abrangem vários serviços. Por exemplo, a política de ReadOnlyacesso AWS gerenciado fornece acesso somente de leitura a todos os AWS serviços e recursos. Quando um serviço lança um novo recurso, AWS adiciona permissões somente de leitura para novas operações e recursos. Para obter uma lista com descrições das políticas de funções de trabalho, consulte Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.

AWS política gerenciada: AWSIoTSiteWiseReadOnlyAccess

Use a política `AWSIoTSiteWiseReadOnlyAccess` AWS gerenciada para permitir acesso somente para leitura a. AWS IoT SiteWise

É possível anexar a política `AWSIoTSiteWiseReadOnlyAccess` a suas identidades do IAM.

Permissões no nível do serviço

Essa política fornece acesso somente para leitura a. AWS IoT SiteWise Nenhuma outra permissão de serviço está incluída nesta política.

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

AWS política gerenciada: AWSServiceRoleForIoTSiteWise

O perfil de `AWSServiceRoleForIoTSiteWise` utiliza a política de `AWSServiceRoleForIoTSiteWise` com as seguintes permissões. Esta política:

- Permite AWS IoT SiteWise implantar gateways SiteWise Edge (que funcionam em`AWS IoT Greengrass`).

- Permite AWS IoT SiteWise realizar o registro.
- Permite AWS IoT SiteWise executar uma consulta de pesquisa de metadados no AWS IoT TwinMaker banco de dados.

Se você estiver usando AWS IoT SiteWise com uma única conta de usuário, a `AWSServiceRoleForIoTSiteWise` função cria a `AWSServiceRoleForIoTSiteWise` política na sua conta do IAM e a anexa ao formulário de funções `AWSServiceRoleForIoTSiteWise` vinculadas ao serviço. 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 atualizações nas políticas AWS gerenciadas

Você pode ver detalhes sobre as atualizações das políticas AWS gerenciadas AWS IoT SiteWise, a partir de quando esse serviço começou a rastrear as alterações. Para receber alertas automáticos sobre alterações nessa página, assine o feed RSS na página Histórico do AWS IoT SiteWise documento.

Alteração	Descrição	Data
AWSServiceRoleForIoTSiteWise: atualizar para uma política existente	AWS IoT SiteWise agora pode executar uma consulta de pesquisa de metadados no AWS IoT TwinMaker banco de dados.	6 de novembro de 2023
AWSIoTSiteWiseReadOnlyAccess: atualização para uma política existente	AWS IoT SiteWise adicionou um novo prefixo de política, `BatchGet*` , que permite	16 de setembro de 2022

Alteração	Descrição	Data
	realizar operações de leitura em lote.	
AWSIoTSiteWiseReadOnlyAccess – Nova política	AWS IoT SiteWise adicionou uma nova política para conceder acesso somente para leitura a. AWS IoT SiteWise	24 de novembro de 2021
AWS IoT SiteWise começou a rastrear alterações	AWS IoT SiteWise começou a rastrear as mudanças em suas políticas AWS gerenciadas.	24 de novembro de 2021

Usar perfis vinculados ao serviço do AWS IoT SiteWise

AWS IoT SiteWise usa funções vinculadas ao serviço AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente a. AWS IoT SiteWise As funções vinculadas ao serviço são predefinidas AWS IoT SiteWise e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

As funções vinculadas ao serviço simplificam a configuração do AWS IoT SiteWise , incluindo automaticamente todas as permissões necessárias. AWS IoT SiteWise define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, só AWS IoT SiteWise pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões. E essa política de permissões não pode ser anexada a nenhuma outra entidade do IAM.

Um perfil vinculado ao serviço poderá ser excluído somente após excluir seus atributos relacionados. Isso protege seus AWS IoT SiteWise recursos porque você não pode remover inadvertidamente a permissão para acessar os recursos.

Para obter informações sobre outros serviços compatíveis com funções vinculadas a serviços, consulte Serviços da AWS compatíveis com o IAM e procure serviços que tenham Sim na coluna função vinculada ao serviço. Escolha Sim com um link para visualizar a documentação da função vinculada a esse serviço.

Tópicos

- Permissões de função vinculada ao serviço AWS IoT SiteWise
- Crie uma função vinculada ao serviço para o AWS IoT SiteWise
- Editar uma função vinculada ao serviço para o AWS IoT SiteWise
- Excluir uma função vinculada ao serviço para o AWS IoT SiteWise
- Regiões suportadas para funções vinculadas a AWS IoT SiteWise serviços
- Usando funções de serviço para AWS IoT SiteWise Monitor

Permissões de função vinculada ao serviço AWS IoT SiteWise

AWS IoT SiteWise usa a função vinculada ao serviço chamada. AWSServiceRoleForIoTSiteWise AWS IoT SiteWise usa essa função vinculada ao serviço para implantar gateways SiteWise Edge (que são executados em AWS IoT Greengrass) e realizar o registro.

A função `AWSServiceRoleForIoTSiteWise` vinculada ao serviço usa a `AWSServiceRoleForIoTSiteWise` política com as seguintes permissões. Esta política:

- Permite AWS IoT SiteWise implantar gateways SiteWise Edge (que funcionam em`AWS IoT Greengrass`).
- Permite AWS IoT SiteWise realizar o registro.
- Permite AWS IoT SiteWise executar uma consulta de pesquisa de metadados no AWS IoT TwinMaker banco de dados.

Para obter mais informações sobre as ações permitidas em`AWSServiceRoleForIoTSiteWise`, consulte políticas AWS gerenciadas 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"
      ]
     }
    }
   }
  ]
}
```

Você pode usar os registros para monitorar e solucionar problemas em seus gateways do SiteWise Edge. Para ter mais informações, consulte Monitorando registros SiteWise do gateway Edge.

Primeiro configure as permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada ao serviço. Para ter mais informações, consulte Permissões de função vinculada a serviços no Guia do usuário do IAM.

Crie uma função vinculada ao serviço para o AWS IoT SiteWise

Não é necessário criar manualmente uma função vinculada a serviço. Quando você executa as seguintes operações no AWS IoT SiteWise console, AWS IoT SiteWise cria a função vinculada ao serviço para você.

- Crie um gateway Greengrass V1.
- Configure a opção de registro.
- Escolher o botão de aceitação no banner de execução da consulta.

Se excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, você poderá usar esse mesmo processo para recriar o perfil em sua conta. Quando você executa qualquer operação no AWS IoT SiteWise console, AWS IoT SiteWise cria a função vinculada ao serviço para você novamente.

Você também pode usar o console ou a API do IAM para criar uma função vinculada ao serviço para o AWS IoT SiteWise.

- Para fazer isso no console do IAM, crie uma função com a AWSServiceRoleForIoTSiteWisepolítica e uma relação de confiança com`iotsitewise.amazonaws.com`.
- Para fazer isso usando a API AWS CLI ou IAM, crie uma função com a `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise` política e uma relação de confiança com`iotsitewise.amazonaws.com`.

Para obter mais informações, consulte Criar um perfil vinculado a serviço no Guia do usuário do IAM.

Se você excluir essa função vinculada ao serviço, será possível usar esse mesmo processo para criar a função novamente.

Editar uma função vinculada ao serviço para o AWS IoT SiteWise

AWS IoT SiteWise não permite que você edite a função AWSServiceRoleForIoTSiteWise vinculada ao serviço. Depois que você criar um perfil vinculado ao serviço, não poderá alterar o nome do perfil, pois várias entidades podem fazer referência ao perfil. No entanto, você pode editar a descrição da

função usando o IAM. Para obter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço para o AWS IoT SiteWise

Se um recurso ou serviço que exige uma função vinculada ao serviço não estiver mais em uso, é recomendável excluir a função associada. Isso evita ter uma entidade inativa que não esteja sendo monitorada ou mantida. No entanto, você deve limpar os recursos de sua função vinculada ao serviço antes de excluí-la manualmente.

> **Note**
>
> Se o AWS IoT SiteWise serviço estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, aguarde alguns minutos e tente novamente.

Para excluir AWS IoT SiteWise recursos usados pelo AWSServiceRoleForIoTSiteWise

1. Desative o registro para AWS IoT SiteWise. Para mais informações, consulte Alterando seu nível de registro.
2. Exclua todos os gateways ativos SiteWise do Edge.

Como excluir manualmente a função vinculada a serviço usando o IAM

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função AWSServiceRoleForIoTSiteWise vinculada ao serviço. Para mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Regiões suportadas para funções vinculadas a AWS IoT SiteWise serviços

AWS IoT SiteWise suporta o uso de funções vinculadas ao serviço em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte Endpoints e cotas do AWS IoT SiteWise.

Usando funções de serviço para AWS IoT SiteWise Monitor

A função de serviço é uma função do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para

obter mais informações, consulte Criando um Perfil para Delegar Permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

Para permitir que usuários federados do portal SiteWise Monitor acessem seus AWS IAM Identity Center recursos AWS IoT SiteWisee seus, você deve anexar uma função de serviço a cada portal que você criar. A função de serviço deve especificar o SiteWise Monitor como uma entidade confiável e incluir a política AWSIoTSiteWiseMonitorPortalAccessgerenciada ou definir permissões equivalentes. Essa política é mantida AWS e define o conjunto de permissões que o SiteWise Monitor usa para acessar seus recursos AWS IoT SiteWise e os do IAM Identity Center.

Ao criar um portal do SiteWise Monitor, você deve escolher uma função que permita que os usuários desse portal acessem seus recursos AWS IoT SiteWisee os do IAM Identity Center. O AWS IoT SiteWise console pode criar e configurar a função para você. Você pode editar o perfil no IAM posteriormente. Os usuários do seu portal terão problemas ao usar seus portais SiteWise Monitor se você remover as permissões necessárias da função ou excluir a função.

> **Note**
>
> Os portais criados antes de 29 de abril de 2020 não exigiram funções de serviço. Se você criou portais antes dessa data, deverá anexar funções de serviço para continuar usando-as. Para fazer isso, navegue até a página Portais no AWS IoT SiteWise console e escolha Migrar todos os portais para usar os perfis do IAM.

As seções a seguir descrevem como criar e gerenciar a função de serviço SiteWise Monitor no AWS Management Console ou no AWS Command Line Interface.

Sumário

- SiteWise Monitore as atualizações do AWSIoTSiteWiseMonitorServiceRole

Permissões de função de serviço para SiteWise Monitor

Quando você cria um portal, AWS IoT SiteWise permite criar uma função cujo nome comece com AWSIoTSiteWiseMonitorServiceRole. Essa função permite que usuários federados do SiteWise Monitor acessem sua configuração do portal, ativos, dados de ativos e dados de configuração do IAM Identity Center.

A função confia que o seguinte serviço assuma a função:

- `monitor.iotsitewise.amazonaws.com`

A função usa a seguinte política de permissões, cujo nome começa com AWSIoTSiteWiseMonitorServicePortalPolicy, para permitir que os usuários do SiteWise Monitor concluam ações nos recursos da sua conta. A política AWSIoTSiteWiseMonitorPortalAccessgerenciada define permissões 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 mais informações sobre as permissões necessárias para alarmes, consulte Configurando permissões para AWS IoT Events alarmes.

Quando um usuário do portal entra, o SiteWise Monitor cria uma política de sessão com base na interseção da função de serviço e das políticas de acesso desse usuário. As políticas de acesso definem o nível de acesso das identidades aos seus portais e projetos. Para obter mais informações

sobre permissões do portal e políticas de acesso, consulte Administrando seus portais do SiteWise Monitor CreateAccessPolítica.

Gerenciando a função de serviço SiteWise Monitor (console)

Isso Console do AWS IoT SiteWise facilita o gerenciamento da função de serviço SiteWise Monitor para portais. Ao criar um portal, o console verifica as funções existentes adequadas para anexação. Se nenhuma estiver disponível, o console poderá criar e configurar uma função de serviço para você. Para ter mais informações, consulte Criar um portal.

Tópicos

- Encontrar uma função de serviço de portal (console)
- Criando uma função de serviço do SiteWise Monitor (AWS IoT SiteWise console)
- Criação de uma função de serviço do SiteWise Monitor (console do IAM)
- Alterar a função de serviço de um portal (console)

Encontrar uma função de serviço de portal (console)

Use as etapas a seguir para encontrar a função de serviço anexada a um portal do SiteWise Monitor.

Como encontrar a função de serviço de um portal

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação à esquerda, escolha Portais.
3. Escolha o portal para o qual deseja encontrar a função de serviço.

   A função anexada ao portal aparece em Permissions (Permissões), Service Role (Função de serviço).

Criando uma função de serviço do SiteWise Monitor (AWS IoT SiteWise console)

Ao criar um portal SiteWise Monitor, você pode criar uma função de serviço para seu portal. Para ter mais informações, consulte Criar um portal.

Você também pode criar uma função de serviço para um portal existente no AWS IoT SiteWise console. Isso substitui o perfil de serviço existente do portal.

Como criar uma função de serviço para um portal existente

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Portais.
3. Escolha o portal para o qual você deseja criar uma função de serviço.
4. Em Portal details (Detalhes do portal), escolha Edit (Editar).
5. Em Permissions (Permissões), escolha Create and use a new service role (Criar e usar uma nova função de serviço) na lista.
6. Insira um nome para a nova função.
7. Selecione Save (Salvar).

Criação de uma função de serviço do SiteWise Monitor (console do IAM)

É possível criar um perfil de serviço a partir do modelo de perfil de serviço no console do IAM. Esse modelo de função inclui a política AWSIoTSiteWiseMonitorPortalAccessgerenciada e especifica o SiteWise Monitor como uma entidade confiável.

Para criar um perfil de serviço a partir do modelo de perfil de serviço do portal

1. Navegue até o console do IAM.
2. No painel de navegação, escolha Roles.
3. Escolha Criar Perfil.
4. Em Escolha um caso de uso, escolha IoT SiteWise.
5. Em Selecione seu caso de uso, escolha IoT SiteWise Monitor - Portal.
6. Escolha Next: Permissions (Próximo: Permissões).
7. Escolha Next: Tags (Próximo: tags).
8. Selecione Next: Review (Próximo: revisar).
9. Insira um Nome do perfil para o novo perfil de serviço.
10. Selecione Criar função.

Alterar a função de serviço de um portal (console)

Use o procedimento a seguir para escolher uma função de serviço SiteWise Monitor diferente para um portal.

Como alterar a função de serviço de um portal

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, selecione Portais.
3. Escolha o portal para o qual você deseja alterar a função de serviço.
4. Em Portal details (Detalhes do portal), escolha Edit (Editar).
5. Em Permissions (Permissões), escolha Use an existing role (Usar uma função existente).
6. Escolha uma função existente para anexar a este portal.
7. Selecione Save (Salvar).

Gerenciando a função de serviço do SiteWise Monitor (CLI)

Você pode usar o AWS CLI para as seguintes tarefas de gerenciamento de função de serviço do portal:

Tópicos

- Encontrar a função de serviço de um portal (CLI)
- Criando a função de serviço do SiteWise Monitor (CLI)

Encontrar a função de serviço de um portal (CLI)

Para encontrar a função de serviço anexada a um portal do SiteWise Monitor, execute o comando a seguir para listar todos os seus portais na região atual.

```
aws iotsitewise list-portals
```

A operação retorna uma resposta que contém os resumos de seu portal no formato a seguir.

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

Você também pode utilizar a DescribePortaloperação para localizar a função do seu portal se você souber a ID do seu portal.

Criando a função de serviço do SiteWise Monitor (CLI)

Use as etapas a seguir para criar uma nova função de serviço do SiteWise Monitor.

Para criar uma função de serviço do SiteWise Monitor

1. Crie uma função com uma política de confiança que permita que o SiteWise Monitor assuma a função. Este exemplo cria uma função chamada **`MySiteWiseMonitorPortalRole`** de uma política de confiança armazenada em uma string 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 o ARN da função dos metadados da função na saída. Ao criar um portal, você usa esse ARN para associar a função ao portal. Para obter mais informações sobre a criação de um portal, consulte CreatePortalna Referência AWS IoT SiteWise da API.
3. Anexe a política `AWSIoTSiteWiseMonitorPortalAccess` à função ou anexe uma política que defina permissões equivalentes.

```
aws iam attach-role-policy --role-name MySiteWiseMonitorPortalRole --policy-arn
 arn:aws:iam::aws:policy/service-role/AWSIoTSiteWiseMonitorPortalAccess
```

Como anexar uma função de serviço a um portal existente

1. Para recuperar os detalhes existentes do portal, execute o comando a seguir. Substitua *`portal-id`* pelo ID do portal.

```
aws iotsitewise describe-portal --portal-id portal-id
```

A operação retorna uma resposta que contém os detalhes do portal no seguinte 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 anexar uma função de serviço a um portal, execute o comando a seguir. Substitua *role-arn* pelo ARN da função de serviço e substitua os parâmetros restantes pelos valores existentes do 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 Monitore as atualizações do AWSIoTSiteWiseMonitorServiceRole

Você pode ver detalhes sobre as atualizações do SiteWise Monitor, a AWSIoTSiteWiseMonitorServiceRolepartir de quando esse serviço começou a rastrear as alterações. Para receber alertas automáticos sobre alterações nessa página, assine o feed RSS na página Histórico do AWS IoT SiteWise documento.

Alteração	Descrição	Data
AWSIoTSiteWiseMonitorPortalAccess: política atualizada	AWS IoT SiteWise atualizou a política AWSIoTSiteWiseMonitorPortalAccessgerenciada para o recurso de alarmes.	27 de maio de 2021
AWS IoT SiteWise começou a rastrear alterações	AWS IoT SiteWise começou a rastrear as alterações em sua função de serviço.	15 de dezembro de 2020

Configurando permissões para AWS IoT Events alarmes

Ao usar um modelo de AWS IoT Events alarme para monitorar uma propriedade AWS IoT SiteWise de ativo, você deve ter as seguintes permissões do IAM:

- Uma função AWS IoT Events de serviço que AWS IoT Events permite enviar dados para AWS IoT SiteWise o. Para mais informações, consulte Gerenciamento de identidade e acesso para o AWS IoT Events no Guia do desenvolvedor do AWS IoT Events .

- Você deve ter as seguintes permissões de AWS IoT SiteWise ação: `iotsitewise:DescribeAssetModel` `iotsitewise:UpdateAssetModelPropertyRouting` e. Essas permissões permitem AWS IoT SiteWise enviar valores de propriedades de ativos para modelos AWS IoT Events de alarme.

Para obter mais informações, consulte Políticas baseadas em recursos no Manual do usuário do IAM.

Permissões obrigatórias para ações

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições. O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política.

Antes de definir um modelo de AWS IoT Events alarme, você deve conceder as seguintes permissões que permitem AWS IoT SiteWise enviar valores de propriedades do ativo para o modelo de alarme.

- `iotsitewise:DescribeAssetModel`— Permite AWS IoT Events verificar se existe uma propriedade do ativo.
- `iotsitewise:UpdateAssetModelPropertyRouting`— Permite AWS IoT SiteWise criar automaticamente assinaturas que permitem enviar dados AWS IoT SiteWise para. AWS IoT Events

Para obter mais informações sobre as ações AWS IoT SiteWise suportadas, consulte Ações definidas por AWS IoT SiteWise na Referência de Autorização de Serviço.

Example Exemplo 1 de política de permissões

A política a seguir permite AWS IoT SiteWise enviar valores de propriedades de ativos para qualquer modelo de AWS IoT Events alarme.

```
{
    "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 Exemplo 2 de política de permissões

A política a seguir permite AWS IoT SiteWise enviar valores de uma propriedade de ativo especificada para um modelo de AWS IoT Events alarme especificado.

```
{
    "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 Permissão (opcional)

Quando você atualiza ou exclui um modelo de ativo, AWS IoT SiteWise pode verificar se um modelo de alarme AWS IoT Events está monitorando uma propriedade de ativo associada a esse modelo de ativo. Isso impede que você exclua uma propriedade do ativo que um AWS IoT Events alarme está usando atualmente. Para ativar esse recurso AWS IoT SiteWise, você deve ter a `iotevents:ListInputRoutings` permissão. Essa permissão permite AWS IoT SiteWise fazer chamadas para a operação da API ListInputRoutings suportada pelo AWS IoT Events.

> **Note**
>
> É altamente recomendável adicionar a permissão `ListInputRoutings`.

Example Exemplo de política de permissões

A política a seguir permite que você atualize e exclua modelos de ativos e use a `ListInputRoutings` API em 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/*"
        }
    ]
}
```

Permissões necessárias para o SiteWise Monitor

Se quiser usar o recurso de alarmes nos portais do SiteWise Monitor, você deve atualizar a função de serviço SiteWise Monitor com a seguinte 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"
                    ]
                }
            }
        }
    ]
}
```

Prevenção contra o ataque do “substituto confuso” em todos os serviços

O problema “confused deputy” é um problema de segurança no qual uma entidade que não tem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executá-la. Em AWS, a falsificação de identidade entre serviços pode resultar no problema confuso do deputado. A imitação entre serviços pode ocorrer quando um serviço (o serviço de chamada) chama outro serviço (o serviço chamado). O serviço de chamada pode ser manipulado de modo a usar suas permissões para atuar nos recursos de outro cliente de uma forma na qual ele não deveria ter permissão para acessar. Para evitar isso, o AWS fornece ferramentas que ajudam você a proteger seus dados para todos os serviços com entidades principais de serviço que receberam acesso aos recursos em sua conta.

Recomendamos usar as chaves de contexto de condição global `aws:SourceAccount` e `aws:SourceArn` nas políticas de recursos para limitar as permissões que AWS IoT SiteWise concedem outro serviço ao recurso. Se o valor `aws:SourceArn` não contiver o ID da conta, como um nome do recurso da Amazon (ARN) do bucket do Amazon S3, você deverá usar ambas as chaves de contexto de condição global para limitar as permissões. Se você utilizar ambas as chaves de contexto de condição global e o valor de `aws:SourceArn` contiver o ID da conta, o valor de `aws:SourceAccount` e a conta no valor de `aws:SourceArn` deverão utilizar o mesmo ID de conta quando utilizados na mesma declaração da política.

- Use `aws:SourceArn` se quiser apenas um recurso associado a acessibilidade de serviço.
- Use `aws:SourceAccount` se quiser permitir que qualquer recurso nessa conta seja associado ao uso entre serviços.

O valor de `aws:SourceArn` deve ser o recurso AWS IoT SiteWise do cliente associado à `sts:AssumeRole` solicitação.

A maneira mais eficaz de se proteger contra o problema do substituto confuso é usar a chave de contexto de condição global `aws:SourceArn` com o ARN completo do recurso. Se você não souber o ARN completo do recurso ou se estiver especificando vários recursos, use a chave da condição de contexto global `aws:SourceArn` com curingas (*) para as partes desconhecidas do ARN. Por exemplo, `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`.

Example — Prevenção confusa de delegado

O exemplo a seguir mostra como você pode usar as chaves de contexto de condição `aws:SourceAccount` global `aws:SourceArn` e as chaves de contexto AWS IoT SiteWise para evitar o confuso problema substituto.

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

Solução de problemas AWS IoT SiteWise de identidade e acesso

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com AWS IoT SiteWise e AWS Identity and Access Management (IAM).

Tópicos

- Não estou autorizado a realizar uma ação em AWS IoT SiteWise
- Não tenho autorização para executar uma iam:PassRole
- Quero permitir que pessoas fora da minha Conta da AWS acessem meus AWS IoT SiteWise recursos

Não estou autorizado a realizar uma ação em AWS IoT SiteWise

Se isso AWS Management Console indicar que você não está autorizado a realizar uma ação, entre em contato com o administrador para obter ajuda. O administrador é a pessoa que forneceu o seu nome de usuário e senha.

O erro do exemplo a seguir ocorre quando o usuário do IAM de `mateojackson` tenta usar o console para visualizar detalhes sobre um ativo, mas não tem permissões `iotsitewise:DescribeAsset`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 iotsitewise:DescribeAsset on resource: a1b2c3d4-5678-90ab-cdef-22222EXAMPLE
```

Nesse caso, Mateo pede ao administrador para atualizar suas políticas a fim de obter acesso ao recurso do ativo com o ID `a1b2c3d4-5678-90ab-cdef-22222EXAMPLE` usando a ação `iotsitewise:DescribeAsset`.

Não tenho autorização para executar uma `iam:PassRole`

Se você receber uma mensagem de erro informando que não está autorizado a executar a ação `iam:PassRole`, as suas políticas devem ser atualizadas para permitir que você passe uma função para o AWS IoT SiteWise.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazê-lo, você deve ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta utilizar o console para executar uma ação no AWS IoT SiteWise. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

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

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha Conta da AWS acessem meus AWS IoT SiteWise recursos

Você pode criar uma função que os usuários de outras contas ou pessoas fora da sua organização possam usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se é AWS IoT SiteWise compatível com esses recursos, consulteComo AWS IoT SiteWise funciona com o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.

- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Saiba como conceder acesso por meio da federação de identidades consultando Concedendo Acesso a Usuários Autenticados Externamente (Federação de Identidades) no Guia do Usuário do IAM.
- Para saber a diferença entre usar perfis e políticas baseadas em recursos para acesso entre contas, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

Validação de conformidade para AWS IoT SiteWise

AWS IoT SiteWise não está no escopo de nenhum programa de AWS conformidade.

Para obter uma lista de AWS serviços no escopo de programas de conformidade específicos, consulte AWS Serviços no escopo do programa de conformidade AWS . Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar AWS IoT SiteWise é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos com foco em segurança e conformidade em. AWS
- Documento técnico sobre arquitetura para segurança e conformidade com a HIPAA — Este whitepaper descreve como as empresas podem usar para criar aplicativos compatíveis com a HIPAA. AWS
- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- Avaliação de recursos com as regras do Guia do AWS Config Desenvolvedor — O AWS Config serviço avalia se suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.

- AWS Security Hub— Esse AWS serviço fornece uma visão abrangente do seu estado de segurança interno, AWS que ajuda você a verificar sua conformidade com os padrões e as melhores práticas do setor de segurança.
- Dez regras de ouro de segurança para soluções de IoT Industrial – Esta postagem do blog apresenta dez regras de ouro que ajudam a proteger seus sistemas de controle industrial (ICS), Internet das Coisas Industrial (IIoT) e ambientes em nuvem.
- Melhores práticas de segurança para OT de manufatura — Este whitepaper descreve as melhores práticas de segurança para projetar, implantar e arquitetar essas cargas de trabalho de manufatura híbrida local para a nuvem. AWS

Resiliência em AWS IoT SiteWise

A infraestrutura AWS global é construída em torno de AWS regiões e zonas de disponibilidade. AWS As regiões fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

AWS IoT SiteWise é totalmente gerenciado e usa AWS serviços duráveis e de alta disponibilidade, como Amazon S3 e Amazon EC2. Para garantir a disponibilidade no caso de uma interrupção na zona de disponibilidade, AWS IoT SiteWise opera em várias zonas de disponibilidade.

Para obter mais informações sobre AWS regiões e zonas de disponibilidade, consulte Infraestrutura AWS global.

Além da infraestrutura AWS global, AWS IoT SiteWise oferece vários recursos para ajudar a suportar suas necessidades de resiliência e backup de dados:

- Você pode publicar atualizações de valores de propriedades AWS IoT Core por meio de mensagens MQTT e, em seguida, configurar regras para agir com base nesses dados. Com esse recurso, você pode fazer backup de dados em outros AWS serviços, como Amazon S3 e Amazon DynamoDB. Para obter mais informações, consulte Interagindo com outros serviços AWS e Exporte dados para o Amazon S3 com notificações de propriedades de ativos.

- Você pode usar as AWS IoT SiteWise `Get*` APIs para recuperar e fazer backup de dados históricos de propriedades de ativos. Para ter mais informações, consulte Consultar valores históricos de propriedade de ativos.
- Você pode usar as AWS IoT SiteWise `Describe*` APIs para recuperar as definições de seus recursos, como ativos e modelos. Você pode fazer backup dessas definições e depois usá-las para recriar seus recursos. Para obter mais informações, consulte a Referência da API do AWS IoT SiteWise .

Segurança da infraestrutura em AWS IoT SiteWise

Como serviço gerenciado, AWS IoT SiteWise é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar AWS IoT SiteWise pela rede. Os clientes devem ser compatíveis com:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com Perfect Forward Secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, suporta esses modos.

Além disso, as solicitações devem ser assinadas utilizando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou é possível usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

SiteWise Os gateways Edge, que são executados em AWS IoT Greengrass, usam certificados X.509 e chaves criptográficas para se conectar e se autenticar na nuvem. AWS Para obter mais informações, consulte Autenticação e autorização de dispositivos de AWS IoT Greengrass no Guia do desenvolvedor do AWS IoT Greengrass Version 1 .

Análise de configuração e vulnerabilidade

Frotas de IoT consistem em grandes quantidades de dispositivos com diversos recursos, duradouros e geograficamente distribuídos. Essas características tornam a configuração da frota complexa e propensa a erros. Como os dispositivos geralmente têm capacidade de processamento, memória e armazenamento limitados, eles nem sempre oferecem suporte à criptografia e a outras medidas de segurança. Além disso, muitas vezes, os dispositivos usam software com vulnerabilidades conhecidas. Esses fatores tornam frotas de IoT um alvo atrativo para hackers e tornam difícil proteger a frota de dispositivos de forma contínua.

AWS IoT Device Defender aborda esses desafios fornecendo ferramentas para identificar problemas de segurança e desvios das melhores práticas. Use AWS IoT Device Defender para analisar, auditar e monitorar dispositivos conectados para detectar comportamentos anormais e mitigar riscos de segurança. AWS IoT Device Defender pode auditar frotas de dispositivos para garantir que elas sigam as melhores práticas de segurança e detectem comportamentos anormais nos dispositivos. Isso possibilita aplicar políticas de segurança consistentes em toda a sua frota de AWS IoT dispositivos e responder rapidamente quando os dispositivos são comprometidos. Para obter mais informações, consulte AWS IoT Device Defender no AWS IoT Guia do desenvolvedor.

Se você usa gateways SiteWise Edge para ingerir dados para o serviço, é sua responsabilidade configurar e manter o ambiente do gateway SiteWise Edge. Essa responsabilidade inclui a atualização para as versões mais recentes do software do sistema, AWS IoT Greengrass do software e do AWS IoT SiteWise conector do gateway SiteWise Edge. Para obter mais informações, consulte Configurar o AWS IoT Greengrass núcleo no Guia do AWS IoT Greengrass Version 1 desenvolvedor Atualizando um conector e.

Endpoints da VPC

Uma interface VPC endpoint estabelece uma conexão privada entre sua nuvem privada virtual (VPC) e. AWS IoT SiteWiseAWS PrivateLinkalimenta os endpoints da interface, permitindo acesso privado às operações AWS IoT SiteWise da API. Você pode ignorar a necessidade de um gateway de internet, dispositivo NAT, conexão VPN ou. AWS Direct Connect As instâncias na sua VPC não precisam de endereços IP públicos para se comunicarem com operações da API do AWS IoT SiteWise . Tráfego entre sua VPC e o tráfego AWS IoT SiteWise que não sai da AWS rede.

Cada endpoint de interface é representado por uma ou mais interfaces de rede elástica nas sub-redes.

Antes de configurar uma interface para o VPC endpoint AWS IoT SiteWise, revise as propriedades e limitações do endpoint de interface no Guia do usuário do Amazon VPC.

Para obter mais informações, consulte Endpoints da VPC da interface (AWS PrivateLink) no Manual do Usuário do Amazon VPC.

Operações de API compatíveis para endpoints de VPC

AWS IoT SiteWise suporta fazer chamadas para as seguintes operações de AWS IoT SiteWise API a partir da sua VPC:

- Para todas as operações da API do plano de dados, use o seguinte endpoint: *region*Substitua por seu Região da AWS

  ```
  data.iotsitewise.region.amazonaws.com
  ```

  As operações da API do plano de dados incluem o seguinte:

  - BatchGetAssetPropertyValor
  - BatchGetAssetPropertyValueHistory
  - BatchPutAssetPropertyValor
  - GetAssetPropertyAggregates
  - GetAssetPropertyValue
  - GetAssetPropertyValueHistória
  - GetInterpolatedAssetPropertyValores
- Para as operações de API do plano de controle que você usa para gerenciar modelos de ativos, ativos, gateways SiteWise Edge, tags e configurações de conta, use o seguinte endpoint. Substitua *region* por seu Região da AWS.

  ```
  api.iotsitewise.region.amazonaws.com
  ```

  As operações de API do ambiente de gerenciamento suportadas incluem o seguinte:

  - AssociateAssets
  - CreateAsset
  - CreateAssetmodelo
  - DeleteAsset

- DeleteAssetmodelo
- DeleteDashboard
- DescribeAsset
- DescribeAssetmodelo
- DescribeAssetPropriedade
- DescribeDashboard
- DescribeLoggingOpções
- DisassociateAssets
- ListAssetModelos
- ListAssetRelacionamentos
- ListAssets
- ListAssociatedAtivos
- PutLoggingOpções
- UpdateAsset
- UpdateAssetmodelo
- UpdateAssetPropriedade
- CreateGateway
- DeleteGateway
- DescribeDefaultEncryptionConfiguration
- DescribeGateway
- DescribeGatewayCapabilityConfiguration
- DescribeStorageConfiguração
- ListGateways
- ListTagsForResource
- UpdateGateway
- UpdateGatewayCapabilityConfiguration
- PutDefaultEncryptionConfiguration
- PutStorageConfiguração
- TagResource
- UntagResource

Note

Atualmente, a interface VPC endpoint para as operações da API do plano de controle não oferece suporte à realização de chamadas para as seguintes operações da API SiteWise Monitor:

- BatchAssociateProjectAssets
- BatchDisassociateProjectAssets
- CreateAccessPolítica
- CreateDashboard
- CreatePortal
- CreateProject
- DeleteAccessPolítica
- DeletePortal
- DeleteProject
- DescribeAccessPolítica
- DescribePortal
- DescribeProject
- ListAccessPolíticas
- ListDashboards
- ListPortals
- ListProjects
- ListProjectAtivos
- UpdateAccessPolítica
- UpdateDashboard
- UpdatePortal
- UpdateProject

Criar um endpoint da VPC de interface para o AWS IoT SiteWise

Para criar um VPC endpoint para o AWS IoT SiteWise serviço, use o console Amazon VPC ou o (). AWS Command Line Interface AWS CLI Para mais informações, consulte Criar um endpoint de interface no Guia do usuário da Amazon VPC.

Crie um VPC endpoint para AWS IoT SiteWise usando um dos seguintes nomes de serviço:

- Para as operações da API do plano de dados, use o seguinte nome de serviço:

```
com.amazonaws.region.iotsitewise.data
```

- Para as operações da API do plano de controle, use o seguinte nome de serviço:

```
com.amazonaws.region.iotsitewise.api
```

Acessando AWS IoT SiteWise por meio de uma interface VPC endpoint

Quando você cria um endpoint de interface, geramos nomes de host DNS específicos do endpoint que você pode usar para se comunicar. AWS IoT SiteWise A opção de DNS privado é habilitada opcionalmente. Para obter mais informações, consulte Uso de zonas hospedadas privadas no Guia do usuário do Amazon VPC.

Se você habilitar o DNS privado para o endpoint, poderá fazer solicitações de API AWS IoT SiteWise por meio de um dos seguintes endpoints de VPC.

- Para as operações da API do plano de dados, use o seguinte endpoint: Substitua a *região* por sua Região da AWS.

```
data.iotsitewise.region.amazonaws.com
```

- Para as operações da API do plano de controle, use o seguinte endpoint: Substitua a *região* por sua Região da AWS.

```
api.iotsitewise.region.amazonaws.com
```

Se você desabilitar o DNS privado para o endpoint, deverá fazer o seguinte para acessar AWS IoT SiteWise por meio do endpoint:

1. Especifique o URL do endpoint da VPC nas solicitações de API.
   - Para as operações da API do plano de dados, use o seguinte URL do endpoint. Substitua o *vpc-endpoint-id* e a *região* com seu endpoint da VPC e região.

     ```
     vpc-endpoint-id.data.iotsitewise.region.vpce.amazonaws.com
     ```

   - Para as operações da API do plano de controle, use o seguinte URL do endpoint. Substitua o *vpc-endpoint-id* e a *região* com seu endpoint da VPC e região.

     ```
     vpc-endpoint-id.api.iotsitewise.region.vpce.amazonaws.com
     ```

2. Desative a injeção do prefixo do host. Os AWS SDKs AWS CLI e prefixam o endpoint de serviço com vários prefixos de host quando você chama cada operação de API. Esse recurso faz com que os AWS SDKs AWS CLI e produzam URLs que não são válidos para AWS IoT SiteWise quando você especifica um VPC endpoint.

   > **Important**
   >
   > Você não pode desativar a injeção do prefixo do host no AWS CLI ou no AWS Tools for PowerShell. Isso significa que, se você desativar o DNS privado, não poderá usar essas ferramentas para acessar AWS IoT SiteWise por meio do VPC endpoint. Habilite o DNS privado para usar o AWS CLI ou o AWS Tools for PowerShell para acessar AWS IoT SiteWise por meio do endpoint.

   Para obter mais informações sobre como desabilitar a injeção de prefixo de host nos AWS SDKs, consulte as seções de documentação a seguir para 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 mais informações, consulte Acessar um serviço por um endpoint de interface no Guia do usuário da Amazon VPC.

Criação de uma política de VPC endpoint para AWS IoT SiteWise

É possível anexar uma política de endpoint ao endpoint da VPC que controla o acesso ao AWS IoT SiteWise. Essa política especifica as seguintes informações:

- A entidade principal que pode executar operações.
- As operações que podem ser executadas.
- Os recursos sobre os quais as operações podem ser executadas.

Para mais informações, consulte Controlar o acesso a serviços com VPC endpoints no Guia do usuário da Amazon VPC.

Exemplo: política de VPC endpoint para ações AWS IoT SiteWise

Veja a seguir um exemplo de uma política de endpoint para AWS IoT SiteWise. Quando anexada a um endpoint, essa política concede acesso às AWS IoT SiteWise ações listadas para o usuário *iotsitewiseadmin* em Conta da AWS *123456789012* no ativo 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"
                ]
            }
```

```
        }
    ]
}
```

Melhores práticas de segurança para AWS IoT SiteWise

Este tópico contém as melhores práticas de segurança para AWS IoT SiteWise.

Usar credenciais de autenticação em servidores OPC-UA

Exija credenciais de autenticação para se conectar aos servidores OPC-UA. Consulte a documentação de seus servidores para fazer isso. Em seguida, para permitir que seu gateway SiteWise Edge se conecte aos seus servidores OPC-UA, adicione segredos de autenticação do servidor ao seu gateway SiteWise Edge. Para ter mais informações, consulte Configurar a autenticação de origem.

Use modos de comunicação criptografados para seus servidores OPC-UA

Escolha um modo de segurança de mensagens criptografadas não obsoleto ao configurar suas fontes OPC-UA para seu gateway Edge. SiteWise Isso ajuda a proteger seus dados industriais à medida que eles se movem dos servidores OPC-UA para o gateway SiteWise Edge. Para obter mais informações, consulte Dados em trânsito por meio da rede local e Configurar fontes de dados.

Mantém os componentes atualizados

Se você usa gateways SiteWise Edge para ingerir dados para o serviço, é sua responsabilidade configurar e manter o ambiente do gateway Edge. SiteWise Essa responsabilidade inclui a atualização para as versões mais recentes do software do sistema do gateway, software do AWS IoT Greengrass e conectores.

> **Note**
>
> O conector AWS IoT SiteWise Edge armazena segredos em seu sistema de arquivos. Esses segredos controlam quem pode visualizar os dados armazenados em cache no seu gateway SiteWise Edge. É altamente recomendável que você ative a criptografia de disco ou sistema de arquivos para o sistema que executa seu gateway SiteWise Edge.

Criptografe o sistema de arquivos do seu gateway SiteWise Edge

Criptografe e proteja seu gateway SiteWise Edge, para que seus dados industriais estejam seguros enquanto se movem pelo gateway SiteWise Edge. Se seu gateway SiteWise Edge tiver um módulo de segurança de hardware, você poderá configurar AWS IoT Greengrass para proteger seu gateway SiteWise Edge. Para obter mais informações, consulte Integrações de segurança do hardware no Guia do desenvolvedor do AWS IoT Greengrass Version 1 . Caso contrário, consulte a documentação do seu sistema operacional para saber como criptografar e proteger seu sistema de arquivos.

Acesso seguro à sua configuração de borda

Não compartilhe a senha do aplicativo Edge Console nem a senha do aplicativo SiteWise Monitor. Não coloque essa senha em lugares onde qualquer pessoa possa vê-la. Implemente uma política saudável de alternância de senhas configurando uma expiração apropriada para sua senha.

Conceda aos usuários do SiteWise Monitor as permissões mínimas possíveis

Siga o princípio de privilégio mínimo usando o conjunto mínimo de permissões de políticas de acesso para os usuários do portal.

- Ao criar um portal, defina uma função que permita o conjunto mínimo de ativos necessários para esse portal. Para ter mais informações, consulte Usando funções de serviço para AWS IoT SiteWise Monitor.
- Quando você e os administradores do portal criam e compartilham projetos, use o conjunto mínimo de ativos necessários para esse projeto.
- Quando uma identidade não precisar mais acessar um portal ou projeto, remova-a desse recurso. Se essa identidade não for mais aplicável à sua organização, exclua essa identidade do seu repositório de identidades.

O princípio mínimo das melhores práticas também se aplica aos perfis do IAM. Para ter mais informações, consulte Melhores práticas de política.

Não exponha informações confidenciais

Impeça o registro em log de credenciais e outras informações confidenciais, como informações de identificação pessoal (PII). Recomendamos que você implemente as seguintes proteções, mesmo

que o acesso aos registros locais em um gateway do SiteWise Edge exija privilégios de root e o acesso aos CloudWatch registros exija permissões do IAM.

- Não use informações confidenciais em nomes, descrições ou propriedades de seus ativos ou modelos.
- Não use informações confidenciais no gateway do SiteWise Edge ou nos nomes das fontes.
- Não use informações confidenciais em nomes ou descrições de portais, projetos ou painéis.

Siga as melhores práticas de AWS IoT Greengrass segurança

Siga as melhores práticas de AWS IoT Greengrass segurança para seu gateway SiteWise Edge. Para obter mais informações, consulte Melhores práticas de segurança no Guia do usuário do AWS IoT Greengrass Version 1 .

Consulte também

- Melhores práticas de segurança no Guia do desenvolvedor do AWS IoT
- Dez regras de ouro de segurança para soluções de IoT industrial

Registro e monitoramento em AWS IoT SiteWise

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho de AWS IoT SiteWise suas outras AWS soluções. AWS IoT SiteWise oferece suporte às seguintes ferramentas de monitoramento para monitorar o serviço, relatar quando algo está errado e realizar ações automáticas quando apropriado:

- A Amazon CloudWatch monitora seus AWS recursos e os aplicativos nos quais você executa AWS em tempo real. Colete e monitore métricas, crie painéis personalizados e defina alarmes que notificam você ou realizam ações quando uma métrica específica atinge um determinado limite. Por exemplo, você pode CloudWatch rastrear o uso da CPU ou outras métricas de suas instâncias do Amazon EC2 e iniciar automaticamente novas instâncias quando necessário. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.
- O Amazon CloudWatch Logs monitora, armazena e acessa seus arquivos de log a partir de gateways SiteWise Edge e outras fontes. CloudTrail CloudWatch Os registros podem monitorar as informações nos arquivos de log e notificá-lo quando determinados limites forem atingidos. É possível também arquivar seus dados de log em armazenamento resiliente. Para obter mais informações, consulte o Guia do usuário do Amazon CloudWatch Logs.
- AWS CloudTrailcaptura chamadas de API e eventos relacionados feitos por ou em nome de sua AWS conta. Em seguida, CloudTrail entrega os arquivos de log para um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem a partir do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte o Guia do usuário da AWS CloudTrail.

Tópicos

Monitoramento com Amazon CloudWatch Logs

Configure AWS IoT SiteWise para registrar informações no CloudWatch Logs para monitorar e solucionar problemas do serviço.

Quando você usa o AWS IoT SiteWise console, AWS IoT SiteWise cria uma função vinculada ao serviço que permite que o serviço registre informações em seu nome. Se você não usa o AWS IoT SiteWise console, deve criar manualmente uma função vinculada ao serviço para receber registros. Para ter mais informações, consulte Crie uma função vinculada ao serviço para o AWS IoT SiteWise.

Você deve ter uma política de recursos que permita AWS IoT SiteWise colocar eventos de log em CloudWatch fluxos. Para criar e atualizar uma política de recursos para o CloudWatch Logs, execute o comando a seguir. *logging-policy-name*Substitua pelo nome da política a ser criada.

```
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 O Logs também oferece suporte às chaves de contexto de SourceAccount condição aws: SourceArn e aws:. Essas chaves de contexto de condição são opcionais.

Para criar ou atualizar uma política de recursos que AWS IoT SiteWise permita colocar somente registros associados ao AWS IoT SiteWise recurso especificado em CloudWatch fluxos, execute o comando e faça o seguinte:

- *logging-policy-name*Substitua pelo nome da política a ser criada.
- Substitua o *Source-ARN* pelo ARN do seu AWS IoT SiteWise recurso, como um modelo de ativo ou ativo. Para encontrar o ARN para cada tipo de AWS IoT SiteWise recurso, consulte Tipos de recursos definidos por AWS IoT SiteWise na Referência de Autorização de Serviço.
- Substitua *a ID* da AWS conta pela ID da conta associada ao 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\"]}}}]}"
```

Por padrão, AWS IoT SiteWise não registra informações no CloudWatch Logs. Para ativar o registro, escolha um nível de registro diferente de Desativado (`OFF`). AWS IoT SiteWise suporta os seguintes níveis de registro:

- `OFF`: o registro em log está desativado.
- `ERROR`: os erros são registrados em log.
- `INFO`: os erros e mensagens informativas são registrados em log.

Você pode configurar os gateways do SiteWise Edge para registrar informações no CloudWatch Logs por meio AWS IoT Greengrass de. Para ter mais informações, consulte Monitorando registros SiteWise do gateway Edge.

Você também pode configurar AWS IoT Core para registrar informações no CloudWatch Logs se estiver solucionando uma ação de AWS IoT SiteWise regra. Para ter mais informações, consulte Solução de problemas de uma ação de AWS IoT SiteWise regra.

Sumário

Gerenciando o login AWS IoT SiteWise

Use o AWS IoT SiteWise console ou AWS CLI para as seguintes tarefas de configuração de registro.

Encontrando seu nível de registro

Console

Use o procedimento a seguir para encontrar o nível de registro em log atual no console do AWS IoT SiteWise .

Para encontrar seu nível de AWS IoT SiteWise registro atual

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação à esquerda, escolha Opções de registro em log.

O status do registro em log atual aparece em Status do registro em log. Se o registro em log estiver habilitado, o nível de registro em log atual será exibido em Nível de verbosidade.

AWS CLI

Execute o comando a seguir para encontrar seu nível de AWS IoT SiteWise registro atual com AWS CLI o.

```
aws iotsitewise describe-logging-options
```

A operação retorna uma resposta que contém o nível do registro em log no seguinte formato.

```
{
  "loggingOptions": {
    "level": "String"
  }
}
```

Alterando seu nível de registro

Use o procedimento a seguir para alterar seu nível de registro no AWS IoT SiteWise console ou usando AWS CLI.

Console

Para alterar seu nível de AWS IoT SiteWise registro

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação à esquerda, escolha Opções de registro em log.
3. Selecione a opção Editar.
4. Escolha o Nível de verbosidade a ser habilitado.
5. Escolha Salvar.

AWS CLI

Execute o AWS CLI comando a seguir para alterar seu nível de AWS IoT SiteWise registro. Substitua *nível de* registro pelo nível de registro em log desejado.

```
aws iotsitewise put-logging-options --logging-options level=logging-level
```

Exemplo: entradas do arquivo de AWS IoT SiteWise log

Cada entrada de AWS IoT SiteWise registro inclui informações do evento e recursos relevantes para esse evento, para que você possa entender e analisar os dados do registro.

O exemplo a seguir mostra uma entrada de CloudWatch AWS IoT SiteWise registros que registra quando você cria com sucesso um modelo de ativo.

```
{
  "eventTime": "2020-05-05T00:10:22.902Z",
  "logLevel": "INFO",
  "eventType": "AssetModelCreationSuccess",
  "message": "Successfully created asset model.",
  "resources": {
    "assetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE"
  }
}
```

Monitorando registros SiteWise do gateway Edge

Você pode configurar seu gateway AWS IoT SiteWise Edge para registrar informações no Amazon CloudWatch Logs ou no sistema de arquivos local.

Tópicos

- Usando o Amazon CloudWatch Logs
- Usando registros de serviço
- Usando registros de eventos

Usando o Amazon CloudWatch Logs

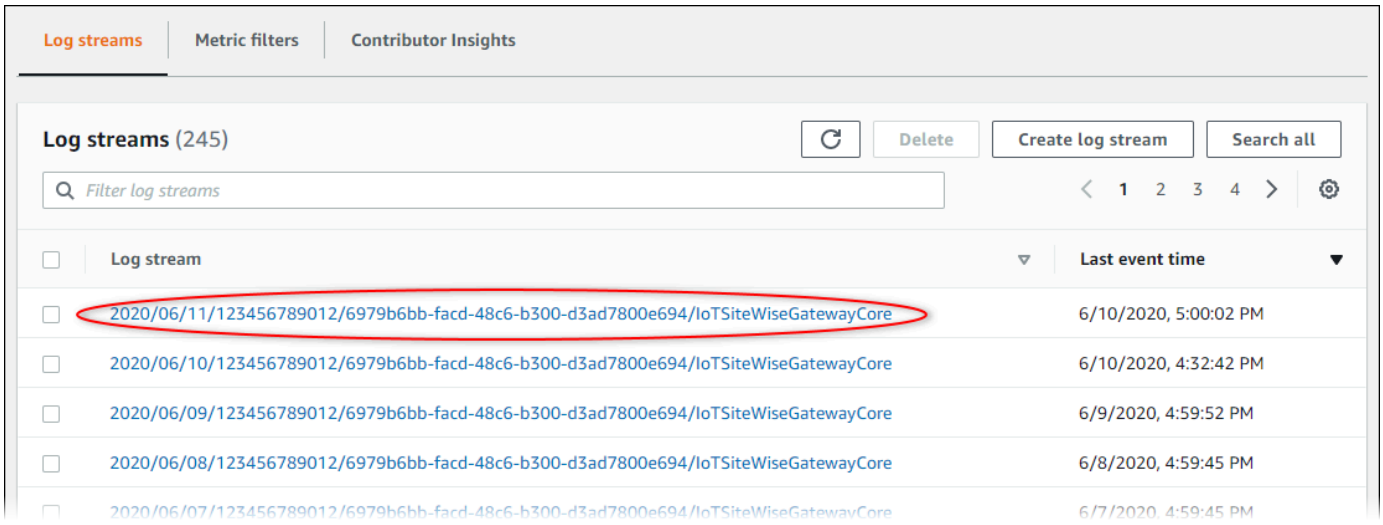
Você pode configurar seu gateway SiteWise Edge para enviar registros para o CloudWatch Logs. Para obter mais informações, consulte Habilitar o registro para CloudWatch registros no Guia do AWS IoT Greengrass Version 2 desenvolvedor.

Para configurar e acessar CloudWatch registros (console)

1. Navegue até o console do CloudWatch.
2. No painel de navegação, escolha Grupos de logs.
3. Você pode encontrar os registros de AWS IoT SiteWise componentes nos seguintes grupos de registros:

   - `/aws/greengrass/UserComponent/region/aws.iot.SiteWiseEdgeCollectorOpcua`— Os registros do componente do gateway SiteWise Edge que coleta dados das fontes OPC-UA do gateway SiteWise Edge.
   - `/aws/greengrass/UserComponent/region/aws.iot.SiteWiseEdgePublisher`— Os registros do componente do gateway SiteWise Edge que publica fluxos de dados OPC-UA no. AWS IoT SiteWise

   Escolha o grupo de logs para a função a ser depurada.
4. Escolha um fluxo de log que tenha um nome que termine com o nome do seu AWS IoT Greengrass grupo. Por padrão, CloudWatch exibe primeiro o fluxo de registros mais recente.



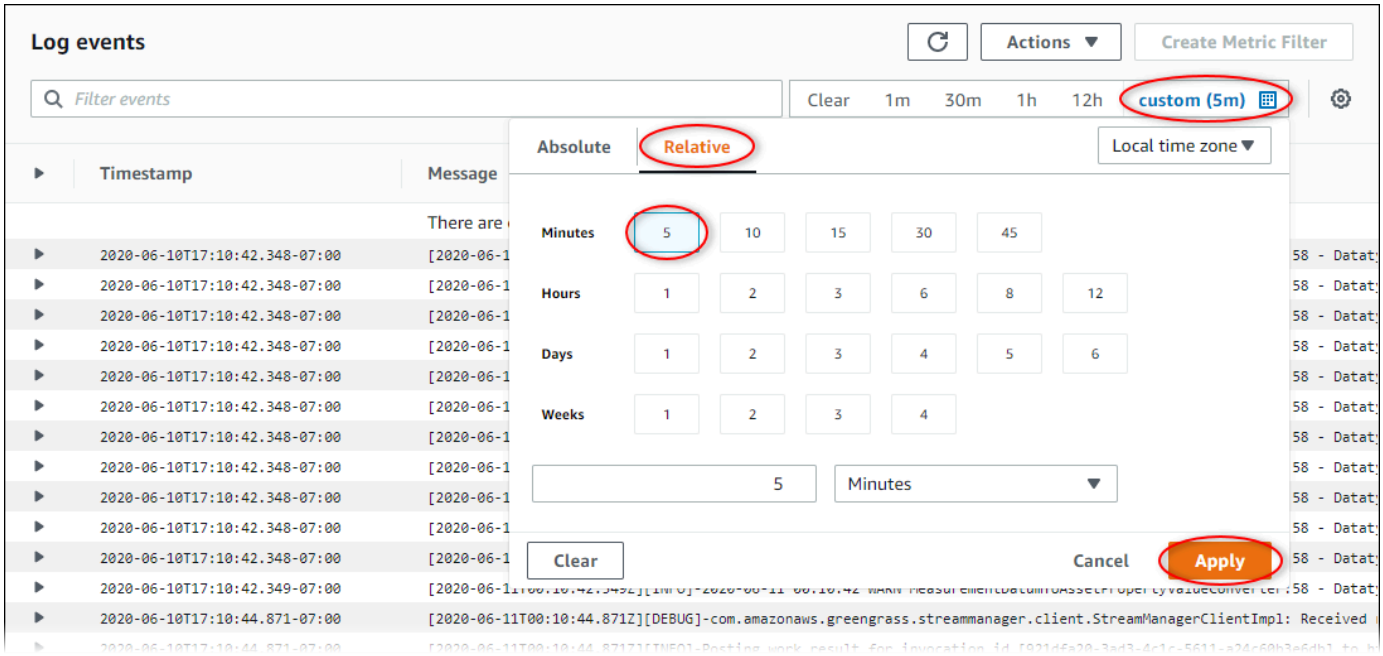
5. Para mostrar logs dos últimos 5 minutos, faça o seguinte:

   a. Escolha personalizado no canto superior direito.

   b. Escolha Relativo.

   c. Escolha 5 minutos.

   d. Escolha Aplicar.



6. (Opcional) Para ver menos logs, é possível escolher 1m no canto superior direito.
7. Role até a parte inferior das entradas de log para exibir os logs mais recentes.

Usando registros de serviço

SiteWise Os dispositivos Edge Gateway incluem arquivos de registro de serviço para ajudar a depurar problemas. As seções a seguir ajudarão você a encontrar e utilizar os arquivos de log de serviço dos componentes AWS IoT SiteWise OPC-UA Collector e AWS IoT SiteWise Publisher.

AWS IoT SiteWise Arquivo de registro do serviço OPC-UA Collector

O componente AWS IoT SiteWise OPC-UA Collector usa o seguinte arquivo de log.

Linux

```
/greengrass/v2/logs/aws.iot.SiteWiseEdgeCollectorOpcua.log
```

Windows

```
C:\greengrass\v2\logs\aws.iot.SiteWiseEdgeCollectorOpcua.log
```

Para ver os registros desse componente

- Execute o comando a seguir no dispositivo principal para visualizar o arquivo de log desse componente em tempo real. Substitua */greengrass/v2*ou *C:\greengrass\v2* pelo caminho para a pasta AWS IoT Greengrass raiz.

  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 Arquivo de log do serviço do editor

O componente AWS IoT SiteWise Publisher usa o seguinte arquivo de log.

Linux

```
/greengrass/v2/logs/aws.iot.SiteWiseEdgePublisher.log
```

Windows

```
C:\greengrass\v2\logs\aws.iot.SiteWiseEdgePublisher.log
```

Para ver os registros desse componente

- Execute o comando a seguir no dispositivo principal para visualizar o arquivo de log desse componente em tempo real. Substitua */greengrass/v2*ou *C:\greengrass\v2* pelo caminho para a pasta AWS IoT Greengrass raiz.

  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
```

Usando registros de eventos

SiteWise Os dispositivos Edge Gateway incluem arquivos de registro de eventos para ajudar a depurar problemas. As seções a seguir ajudarão você a encontrar e utilizar os arquivos de registro de eventos dos componentes AWS IoT SiteWise OPC-UA Collector e AWS IoT SiteWise Publisher.

AWS IoT SiteWise Registros de eventos do OPC-UA Collector

O componente AWS IoT SiteWise OPC-UA Collector inclui um registro de eventos para ajudar os clientes a identificar e corrigir problemas. O arquivo de log é separado do arquivo de log local e é encontrado no seguinte local. Substitua */greengrass/v2*ou *C:\greengrass\v2* pelo caminho para a pasta AWS IoT Greengrass raiz.

Linux

```
/greengrass/v2/work/aws.iot.SiteWiseEdgeCollectorOpcua/logs/
IotSiteWiseOpcUaCollectorEvents.log
```

Windows

```
C:\greengrass\v2\work\aws.iot.SiteWiseEdgeCollectorOpcua\logs
\IotSiteWiseOpcUaCollectorEvents.log
```

Esse registro inclui informações detalhadas e instruções de solução de problemas. As informações de solução de problemas são fornecidas junto com o diagnóstico, com uma descrição de como solucionar o problema e, às vezes, com links para mais informações. As informações de diagnóstico incluem o seguinte:

- Nível de gravidade
- Timestamp
- Informações adicionais específicas do evento

Example Log de exemplo

```
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 do editor

O componente AWS IoT SiteWise Publisher inclui um registro de eventos para ajudar os clientes a identificar e corrigir problemas. O arquivo de log é separado do arquivo de log local e é encontrado no seguinte local. Substitua */greengrass/v2*ou *C:\greengrass\v2* pelo caminho para a pasta AWS IoT Greengrass raiz.

Linux

```
/greengrass/v2/work/aws.iot.SiteWiseEdgePublisher/logs/
IotSiteWisePublisherEvents.log
```

Windows

```
C:\greengrass\v2\work\aws.iot.SiteWiseEdgePublisher\logs
\IotSiteWisePublisherEvents.log
```

Esse registro inclui informações detalhadas e instruções de solução de problemas. As informações de solução de problemas são fornecidas junto com o diagnóstico, com uma descrição de como solucionar o problema e, às vezes, com links para mais informações. As informações de diagnóstico incluem o seguinte:

- Nível de gravidade
- Timestamp
- Informações adicionais específicas do evento

Example Log de exemplo

```
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
```

Monitoramento AWS IoT SiteWise com CloudWatch métricas da Amazon

Você pode monitorar AWS IoT SiteWise o uso CloudWatch, que coleta dados brutos e os processa em métricas legíveis e quase em tempo real. Essas estatísticas são mantidas por 15 meses, de maneira que você possa acessar informações históricas e ter uma perspectiva melhor de como o aplicativo web ou o serviço está se saindo. Você também pode definir alarmes que observam determinados limites e enviam notificações ou realizam ações quando esses limites são atingidos. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.

AWS IoT SiteWise publica as métricas e dimensões listadas nas seções abaixo no `AWS/IoTSiteWise` namespace.

> **Tip**
>
> AWS IoT SiteWise publica métricas em um intervalo de um minuto. Ao visualizar essas métricas em gráficos no CloudWatch console, recomendamos que você escolha um Período de 1 minuto. Isso permite que você veja a resolução mais alta disponível de seus dados de métricas.

Tópicos

- AWS IoT Greengrass Version 2 métricas de gateway
- AWS IoT Greengrass Version 1 métricas de gateway

AWS IoT Greengrass Version 2 métricas de gateway

AWS IoT SiteWise publica as seguintes métricas do SiteWise Edge Gateway. Todas as métricas do SiteWise Edge Gateway são publicadas em um intervalo de um minuto.

SiteWise Métricas do gateway Edge

Métrica	Descrição
`Gateway.CpuUsage`	O uso da CPU de um gateway SiteWise Edge.

Métrica	Descrição
	Unidade: porcentagem Dimensões: nenhuma
`Gateway.TotalDiskSpace`	O espaço total em disco de um gateway SiteWise Edge. Unidade: bytes Dimensões: nenhuma
`Gateway.UsedDiskSpace`	O espaço em disco usado de um gateway SiteWise Edge. Unidade: bytes Dimensões: nenhuma
`Gateway.AvailableDiskSpace`	O espaço em disco disponível de um gateway SiteWise Edge. Unidade: bytes Dimensões: nenhuma
`Gateway.UsedPercentageDiskSpace`	A porcentagem usada do espaço em disco de um gateway SiteWise Edge. Unidade: bytes Dimensões: nenhuma
`Gateway.TotalMemory`	A memória total de um gateway SiteWise Edge. Unidade: bytes Dimensões: nenhuma

Métrica	Descrição
`Gateway.UsedMemory`	A memória usada de um gateway SiteWise Edge. Unidade: bytes Dimensões: nenhuma
`Gateway.AvailableMemory`	A memória disponível de um gateway SiteWise Edge. Unidade: bytes Dimensões: nenhuma
`Gateway.UsedPercentageMemory`	A porcentagem de memória usada de um gateway SiteWise Edge. Unidade: bytes Dimensões: nenhuma
`Gateway.CloudConnectivity`	O status da conectividade na nuvem de um gateway SiteWise Edge. Unidade: nenhuma Dimensão: GatewayId
`Gateway.SWE.Component.RunningStatus`	O status de execução dos componentes em um gateway SiteWise Edge. Unidade: nenhuma Dimensão: GatewayId

Métricas do coletor OPC-UA

Métrica	Descrição
`OpcUaCollector.Heartbeat`	Gerado a cada minuto para cada fonte OPC-UA (`sourceName`) conectada a um gateway SiteWise Edge (`gatewayId`). Unidade: Contagem (1 representando a fonte conectada e 0 representando a fonte desconectada). Dimensões: GatewayId, SourceName
`OpcUaCollector.ActiveDataStreamCount`	O número de fluxos de dados que um gateway SiteWise Edge (`gatewayId`) assinou para uma fonte OPC-UA (). `sourceName` Unidade: Contagem Dimensões: GatewayId, SourceName, PropertyGroup
`OpcUaCollector.IncomingValuesCount`	O número de pontos de dados que um gateway SiteWise Edge (`gatewayId`) recebeu para uma fonte OPC-UA (`sourceName`), gerados a cada minuto. Unidade: Contagem Dimensões: GatewayId, SourceName, PropertyGroup
`OpcUaCollector.IncomingValuesError`	O número de pontos de dados que um gateway SiteWise Edge (`gatewayId`) recebe de uma fonte OPC-UA (`sourceName`) que não são valores válidos. Esses pontos de dados não são ingeridos pelo OpcUa Collector, gerados a cada minuto.

Métrica	Descrição
	Unidade: Contagem Dimensões: GatewayId, SourceName, PropertyGroup
`OpcUaCollector.ConversionErrors`	O número de pontos de dados que um gateway SiteWise Edge (`gatewayId`) recebeu para uma fonte OPC-UA (`sourceName`) que resultou em erros de conversão ao enviar os dados para. AWS IoT SiteWise Esses pontos de dados não serão ingeridos pelo OpcUa Collector. Unidade: Contagem Dimensões: GatewayId, SourceName

AWS IoT SiteWise métricas do processador

Métrica	Descrição
`Gateway.DataProcessor.IngestionSuccess`	O número de pontos de dados que foram ingeridos com sucesso, gerados a cada minuto. Unidade: Contagem Dimensões: nenhuma
`Gateway.DataProcessor.IngestionThrottled`	O número de pontos de dados que foram limitados, gerados a cada minuto. Unidade: Contagem Dimensões: ThrottledAt
`Gateway.DataProcessor.MeasurementRejected`	O número de medições que foram rejeitadas, geradas a cada minuto.

Métrica	Descrição
	Unidade: Contagem Dimensões: Motivo
`Gateway.DataProcessor.MeasurementUnmodeled`	O número de medições que não foram modeladas, geradas a cada minuto. Unidade: Contagem Dimensões: Motivo
`Gateway.DataProcessor.MessagesRemaining`	O número de mensagens restantes em um fluxo, gerado a cada minuto. Unidade: Contagem Dimensões: StreamName
`Gateway.DataProcessor.ProcessingError`	O número de erros de processamento, gerados a cada minuto. Unidade: Contagem Dimensões: Motivo
`IoTSiteWiseProcessor.IsConnectedToMqttBroker`	Gerado a cada minuto pelo processador no gateway SiteWise Edge. Unidade: 1 (1 representando o processador conectado a um broker MQTT.) Dimensões: GatewayId

Métrica	Descrição
`IoTSiteWiseProcessor.NumberOfSubscriptionsToMqttBroker`	O número de tópicos inscritos no broker MQTT pelo processador, gerado a cada minuto. Um tópico curinga de vários níveis é contado como 1. Unidade: Contagem Dimensões: GatewayId
`IoTSiteWiseProcessor.NumberOfUniqueMqttTopicsReceived`	O número de tópicos exclusivos recebidos pelo processador do corretor MQTT, gerados a cada minuto. Unidade: Contagem Dimensões: GatewayId
`IoTSiteWiseProcessor.MqttMessageReceivedSuccessCount`	O número de mensagens recebidas com sucesso pelo processador do broker MQTT, gerado a cada minuto. Unidade: Contagem Dimensões: GatewayId
`IoTSiteWiseProcessor.MqttReceivedSuccessBytes`	O número de bytes de dados da mensagem recebidos com sucesso pelo processador do broker MQTT, gerados a cada minuto. Unidade: Contagem Dimensões: GatewayId

AWS IoT SiteWise métricas do editor

Métrica	Descrição
`IoTSiteWisePublisher.Heartbeat`	Gerado a cada minuto pelo editor no gateway SiteWise Edge. Unidade: 1 (1 representando que o Editor está em execução e falta o ponto de dados que representa que o Editor não está em execução.) Dimensões: GatewayId
`IoTSiteWisePublisher.PublishSuccessCount`	O número de pontos de dados que um gateway SiteWise Edge (`GatewayId`) publicou com sucesso na nuvem, gerados a cada minuto. Unidade: Contagem Dimensões: GatewayId
`IoTSiteWisePublisher.PublishFailureCount`	O número de pontos de dados que um gateway SiteWise Edge (`GatewayId`) falhou em publicar, gerados a cada minuto. Unidade: Contagem Dimensões: GatewayId
`IoTSiteWisePublisher.PublishRejectedCount`	O número de pontos de dados que um gateway SiteWise Edge (`GatewayId`) rejeitou do lado da nuvem, gerados a cada minuto. Unidade: Contagem Dimensões: GatewayId
`IoTSiteWisePublisher.DroppedCount`	O número de pontos de dados que são descartados por um gateway SiteWise Edge

Métrica	Descrição
	(`GatewayId `) e não publicados na nuvem, gerados a cada minuto. Unidade: Contagem Dimensões: GatewayId
`IoTSiteWisePublisher.IsConnectedToMqttBroker`	Gerado a cada minuto pelo editor no gateway SiteWise Edge. Unidade: 1 (1 representando o editor está conectado a um corretor MQTT.) Dimensões: GatewayId
`IoTSiteWisePublisher.NumberOfSubscriptionsToMqttBroker`	O número de tópicos inscritos no corretor MQTT pelo editor, gerado a cada minuto. Um tópico curinga de vários níveis é contado como 1. Unidade: Contagem Dimensões: GatewayId
`IoTSiteWisePublisher.NumberOfUniqueMqttTopicsReceived`	O número de tópicos exclusivos recebidos pelo editor do corretor MQTT, gerados a cada minuto. Unidade: Contagem Dimensões: GatewayId
`IoTSiteWisePublisher.MqttMessageReceivedSuccessCount`	O número de mensagens recebidas com sucesso pelo editor do corretor MQTT, geradas a cada minuto. Unidade: Contagem Dimensões: GatewayId

Métrica	Descrição
`IoTSiteWisePublisher.MqttReceivedSuccessBytes`	O número de bytes de dados da mensagem recebidos com sucesso pelo editor do corretor MQTT, gerados a cada minuto. Unidade: Contagem Dimensões: GatewayId

AWS IoT Greengrass Version 1 métricas de gateway

AWS IoT SiteWise publica as seguintes métricas do SiteWise Edge Gateway. Todas as métricas do SiteWise Edge Gateway são publicadas em um intervalo de um minuto.

> **Important**
>
> Para receber as métricas do SiteWise Edge Gateway, você deve usar pelo menos a versão 6 do AWS IoT SiteWise conector no seu SiteWise Edge Gateway. Para obter mais informações, consulte AWS IoT SiteWise Coletor OPC-UA no Guia do desenvolvedor do AWS IoT Greengrass Version 1 .

SiteWise Métricas do gateway Edge

Métrica	Descrição
`Gateway.Heartbeat`	Gerado a cada minuto para cada gateway SiteWise Edge (`gatewayId`) conectado. Unidade: 1 (1 representando o gateway SiteWise Edge está ativo e ausente, o ponto de dados que representa o gateway SiteWise Edge está desconectado da nuvem.) Dimensão: GatewayId

Métrica	Descrição
`Gateway.PublishSuccessCount`	O número de pontos de dados que um gateway SiteWise Edge (`gatewayId `) publicou com sucesso. Unidade: Contagem Dimensão: GatewayId
`Gateway.PublishFailureCount`	O número de pontos de dados que um gateway SiteWise Edge (`gatewayId `) não conseguiu publicar. Essa métrica conta os erros que resultam das chamadas do gateway SiteWise Edge para a BatchPutAssetPropertyValueoperação. Para obter mais informações sobre a solução de problemas de gateways do SiteWise Edge, consulteSolução de problemas de um gateway SiteWise Edge. Unidade: Contagem Dimensão: GatewayId

Métrica	Descrição
`Gateway.ProcessFailureCount`	O número de pontos de dados que um gateway SiteWise Edge (`gatewayId`) falhou em processar. Essa métrica conta os erros que ocorrem entre o gateway SiteWise Edge e as fontes do gateway SiteWise Edge, incluindo erros relatados pelas fontes. Para obter mais informações sobre a solução de problemas de gateways do SiteWise Edge, consulte Solução de problemas de um gateway SiteWise Edge. Unidade: Contagem Dimensão: GatewayId
`Gateway.PublishRejectedCount`	O número de pontos de dados de um gateway SiteWise Edge (`gatewayId`) que são rejeitados. Unidade: Contagem Dimensão: GatewayId

Métricas relacionadas a OPC-UA

Métrica	Descrição
`OPCUACollector.Heartbeat`	Gerado a cada minuto para cada fonte OPC-UA (`sourceName`) conectada a um gateway SiteWise Edge (`gatewayId`). Unidade: Contagem (1 representando a fonte conectada e 0 representando a fonte desconectada). Dimensões: GatewayId, SourceName

Métrica	Descrição
`OPCUACollector.ActiveDataStreamCount`	O número de fluxos de dados que um gateway SiteWise Edge (`gatewayId`) assinou para uma fonte OPC-UA (). `sourceName` Unidade: Contagem Dimensões: GatewayId, SourceName, PropertyGroup
`OpcUaCollector.IncomingValuesCount`	O número de pontos de dados que um gateway SiteWise Edge (`gatewayId`) recebeu para uma fonte OPC-UA (`sourceName`), gerados a cada minuto. Unidade: Contagem Dimensões: GatewayId, SourceName, PropertyGroup
`OpcUaCollector.IncomingValuesError`	O número de pontos de dados que um gateway SiteWise Edge (`gatewayId`) recebeu de uma fonte OPC-UA (`sourceName`) que não são valores válidos. Esses pontos de dados não serão ingeridos pelo OpcUa Collector, gerados a cada minuto. Unidade: Contagem Dimensões: GatewayId, SourceName, PropertyGroup

Métrica	Descrição
`OpcUaCollector.ConversionErrors`	O número de pontos de dados que um gateway SiteWise Edge (`gatewayId`) recebeu para uma fonte OPC-UA (`sourceName`) que resultou em erros de conversão ao enviar os dados para. AWS IoT SiteWise Esses pontos de dados não serão ingeridos pelo OpcUa Collector. Unidade: Contagem Dimensões: GatewayId, SourceName

Métricas relacionadas ao EIP

Métrica	Descrição
`EIPCollector.Heartbeat`	Gerado a cada minuto para cada fonte EIP (`sourceName`) conectada a um gateway SiteWise Edge (`gatewayId`). Unidade: 1 (1 representando que a fonte está conectada e ausente o ponto de dados representando que a fonte está desconectada). Dimensões: GatewayId, SourceName
`EIPCollector.IncomingValuesCount`	O número de fluxos de dados nos quais um gateway SiteWise Edge (`gatewayId`) está inscrito para uma fonte EIP (). `sourceName` Unidade: Contagem Dimensões: GatewayId, SourceName
`EIPCollector.ActiveDataStreamCount`	O número de pontos de dados que um gateway SiteWise Edge (`gatewayId`) recebeu para uma fonte EIP (`sourceName`).

Métrica	Descrição
	Unidade: Contagem Dimensões: GatewayId, SourceName

Métricas relacionadas ao Modbus

Métrica	Descrição
`ModbusTCPCollector.Heartbeat`	Gerado a cada minuto para cada Modbus Source (`sourceName`) conectado a um gateway SiteWise Edge (`gatewayId`). Unidade: 1 (1 representando que a fonte Modbus está conectada e ausente o ponto de dados representando que a fonte está desconectada). Dimensões: GatewayId, SourceName
`ModbusTCPCollector.IncomingValuesCount`	O número de fluxos de dados nos quais um gateway SiteWise Edge (`gatewayId`) está inscrito para uma fonte Modbus (). `sourceName` Unidade: Contagem Dimensões: GatewayId, SourceName
`ModbusTCPCollector.ActiveDataStreamCount`	O número de pontos de dados que um gateway SiteWise Edge (`gatewayId`) recebeu para uma fonte Modbus (`sourceName`). Unidade: Contagem Dimensões: GatewayId, SourceName

Registrando chamadas de AWS IoT SiteWise API com AWS CloudTrail

AWS IoT SiteWise é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço em AWS IoT SiteWise. CloudTrail captura chamadas de API AWS IoT SiteWise como eventos. As chamadas capturadas incluem chamadas do AWS IoT SiteWise console e chamadas de código para as operações AWS IoT SiteWise da API. Se você criar uma trilha, poderá ativar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para. AWS IoT SiteWise Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita AWS IoT SiteWise, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para obter mais informações sobre CloudTrail, consulte o Guia AWS CloudTrail do usuário.

AWS IoT SiteWise informações em CloudTrail

CloudTrail é ativado em sua AWS conta quando você cria a conta. Quando uma atividade de evento suportada ocorre em AWS IoT SiteWise, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua AWS conta. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em sua AWS conta, incluindo eventos para AWS IoT SiteWise, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, a trilha se aplica a todas as AWS regiões. A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para mais informações, consulte:

- Visão geral da criação de uma trilha
- CloudTrail serviços e integrações suportados
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário root ou AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail .

AWS IoT SiteWise eventos de dados em CloudTrail

Os eventos de dados fornecem informações sobre as operações de recursos realizadas em um recurso (por exemplo, leitura ou gravação em um objeto do Amazon S3). Elas também são conhecidas como operações de plano de dados. Eventos de dados geralmente são atividades de alto volume. Por padrão, CloudTrail não registra eventos de dados. O histórico de CloudTrail eventos não registra eventos de dados.

Há cobranças adicionais para eventos de dados. Para obter mais informações sobre CloudTrail preços, consulte AWS CloudTrail Preços.

Você pode registrar eventos de dados para os tipos de AWS IoT SiteWise recursos usando o CloudTrail console ou AWS CLI as operações CloudTrail da API. A tabela nesta seção mostra os tipos de recursos disponíveis para AWS IoT SiteWise.

- Para registrar eventos de dados usando o CloudTrail console, crie um armazenamento de dados de trilhas ou eventos para registrar eventos de dados ou atualize um armazenamento de dados de trilhas ou eventos existente para registrar eventos de dados.

  1. Escolha Eventos de dados para registrar eventos de dados.
  2. Na lista Tipo de evento de dados, escolha o tipo de recurso para o qual você deseja registrar eventos de dados.
  3. Escolha o modelo do seletor de registros que você deseja usar. Você pode registrar todos os eventos de dados do tipo de recurso, registrar todos os `readOnly` eventos, registrar todos os `writeOnly` eventos ou criar um modelo de seletor de registros personalizado para filtrar os `resources.ARN` campos `readOnly` `eventName`, e.

- Para registrar eventos de dados usando o AWS CLI, configure o `--advanced-event-selectors` parâmetro para definir o `eventCategory` campo igual `Data` e o `resources.type` campo igual ao valor do tipo de recurso (consulte a tabela). Você pode adicionar condições para filtrar os valores dos `resources.ARN` campos `readOnly` e `eventName`.
  - Para configurar uma trilha para registrar eventos de dados, execute o AWS CloudTrail put-event-selectorscomando. Para obter mais informações, consulte Registro de eventos de dados para trilhas com AWS CLI o.
  - Para configurar um armazenamento de dados de eventos para registrar eventos de dados, execute o AWS CloudTrail create-event-data-storecomando para criar um novo armazenamento de dados de eventos para registrar eventos de dados ou execute o AWS CloudTrail update-event-data-storecomando para atualizar um armazenamento de dados de eventos existente. Para obter mais informações, consulte Registro de eventos de dados para armazenamentos de dados de eventos com AWS CLI o.

A tabela a seguir lista os tipos de AWS IoT SiteWise recursos. A coluna Tipo de evento de dados (console) mostra o valor a ser escolhido na lista Tipo de evento de dados no CloudTrail console. A coluna de valor resources.type mostra o **`resources.type`** valor, que você especificaria ao configurar seletores de eventos avançados usando as APIs ou. AWS CLI CloudTrail A CloudTrail coluna Data APIs logged to mostra as chamadas de API registradas CloudTrail para o tipo de recurso.

Tipo de evento de dados (console)	valor resources.type	APIs de dados registradas em * CloudTrail
AWS IoT SiteWise asset	`AWS::IoTSiteWise::Asset`	• BatchPutAssetPropertyValue • GetAssetPropertyValue • GetAssetPropertyValueHistory • GetAssetPropertyAggregates • GetInterpolatedAssetPropertyValues • BatchGetAssetPropertyValue

Tipo de evento de dados (console)	valor resources.type	APIs de dados registradas em * CloudTrail
		• BatchGetAssetPropertyValueHistory • BatchGetAssetPropertyAggregates
AWS IoT SiteWise séries temporais	`AWS::IoTSiteWise::TimeSeries`	• BatchPutAssetPropertyValue • GetAssetPropertyValue • GetAssetPropertyValueHistory • GetAssetPropertyAggregates • GetInterpolatedAssetPropertyValues • BatchGetAssetPropertyValue • BatchGetAssetPropertyValueHistory • BatchGetAssetPropertyAggregates

> **Note**
>
> O resources.type registrado no evento do Cloudtrail depende do identificador usado na solicitação da API. Se um ID de ativo for especificado na solicitação, o Asset resources.type será registrado, caso contrário, o TimeSeries resources.type será registrado.

*Você pode configurar seletores de eventos avançados para filtrar os `resources.ARN` campos `eventNamereadOnly`, e e para registrar somente os eventos que são importantes para você. Consulte mais informações sobre esses campos em AdvancedFieldSelector.

AWS IoT SiteWise eventos de gerenciamento em CloudTrail

Os eventos de gerenciamento fornecem informações sobre as operações de gerenciamento que são realizadas nos recursos AWS da sua conta. Elas também são conhecidas como operações de plano de controle. Por padrão, CloudTrail registra eventos de gerenciamento.

AWS IoT SiteWise registra todas as operações do plano de AWS IoT SiteWise controle como eventos de gerenciamento. Para ver uma lista das operações do plano de AWS IoT SiteWise controle AWS IoT SiteWise registradas CloudTrail, consulte a Referência da AWS IoT SiteWise API.

Exemplo: entradas do arquivo de AWS IoT SiteWise log

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a operação solicitada, a data e a hora da operação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `CreateAsset` operação.

```
{
  "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"
}
```

Marcando seus recursos AWS IoT SiteWise

Marcar seus AWS IoT SiteWise recursos fornece uma maneira poderosa de categorizar, gerenciar e recuperar ativos organizacionais com eficiência. Ao atribuir tags, que consistem em pares de valores-chave, você pode anexar metadados descritivos aos seus recursos. Os metadados das tags podem ser usados para agilizar as operações. Por exemplo, em um cenário de parque eólico, as etiquetas permitem rotular turbinas com atributos específicos, como localização, capacidade e status operacional, permitindo rápida identificação e gerenciamento interno AWS IoT SiteWise.

A integração de tags com políticas AWS Identity and Access Management (IAM) aprimora a segurança e o controle operacional ao definir regras de acesso condicional. Isso significa que você pode especificar que somente usuários com determinadas tags. Por exemplo, somente aqueles marcados com uma determinada função ou departamento podem acessar ou modificar recursos específicos.

Usando tags em AWS IoT SiteWise

Use tags para categorizar seus AWS IoT SiteWise recursos por finalidade, proprietário, ambiente ou qualquer outra classificação para seu caso de uso. Quando você tem muitos recursos do mesmo tipo, é possível identificar rapidamente um recurso específico com base em suas tags.

Cada tag é composta por uma chave e um valor opcional que você especifica. Por exemplo, você pode estabelecer uma série de tags para seus modelos de ativos para rastreá-los de acordo com os processos industriais que eles suportam. É recomendável desenvolver um conjunto personalizado de chaves de tag para cada tipo de recurso que você gerencia. Usar um conjunto consistente de chaves de tag pode facilitar o gerenciamento de recursos.

Marcando com o AWS Management Console

O Editor de tags no AWS Management Console fornece uma maneira central e unificada de criar e gerenciar suas tags para recursos de todos os AWS serviços. Para obter mais informações, consulte Tag Editor (Editor de tags) no Guia do usuário do AWS Resource Groups .

Marcação com a API AWS IoT SiteWise

A AWS IoT SiteWise API também usa tags. Antes de criar tags, esteja ciente dessas restrições de marcação. Para obter mais informações, consulte Convenções de nomenclatura e uso de tags na Referência geral da AWS.

- Para adicionar tags ao criar um recurso, defina-as na propriedade `tags` do recurso.
- Para adicionar tags a um recurso existente ou atualizar os valores das tags, use a TagResourceoperação.
- Para remover tags de um recurso, use a UntagResourceoperação.
- Para recuperar as tags associadas a um recurso, use a ListTagsForResourceoperação ou descreva o recurso e inspecione sua `tags` propriedade.

A tabela a seguir lista os recursos que você pode marcar usando a AWS IoT SiteWise API e suas `Describe` operações correspondentes`Create`.

Recursos etiquetáveis AWS IoT SiteWise

Recurso	Criar operação	Descrever operação
Modelo de ativo ou modelo de componente	CreateAssetModel	DescribeAssetModel
Ativo	CreateAsset	DescribeAsset
SiteWise Gateway Edge	CreateGateway	DescribeGateway
Portal	CreatePortal	DescribePortal
Projeto	CreateProject	DescribeProject
Painel	CreateDashboard	DescribeDashboard
Política de acesso	CreateAccessPolicy	DescribeAccessPolicy
Séries temporais	BatchPutAssetPropertyValue	DescribeTimeSeries

Pois`BatchPutAssetPropertyValue`, você pode configurar suas fontes de dados para enviar dados industriais AWS IoT SiteWise antes de criar modelos e ativos de ativos. AWS IoT SiteWise cria automaticamente fluxos de dados para receber fluxos de dados brutos do seu equipamento. Para obter mais informações, consulte Managing data ingestion.

Use as operações a seguir para visualizar e gerenciar as tags de recursos que são compatíveis com a marcação:

- TagResource— Adiciona tags a um recurso ou atualiza o valor de uma tag existente.
- ListTagsForResource— Lista as tags de um recurso.
- UntagResource— Remove as tags de um recurso.

Adicione ou remova tags de um recurso a qualquer momento. Para atualizar o valor de uma chave de tag existente, adicione uma nova tag com a mesma chave e o novo valor desejado ao recurso. Essa ação substitui o valor antigo pelo novo. Embora seja possível atribuir uma string vazia como valor de tag, você não pode atribuir um valor nulo.

A exclusão de um recurso também remove todas as tags vinculadas a ele.

Utilização de tags com políticas do IAM

Use tags de recursos em suas políticas do IAM para controlar o acesso e as permissões dos usuários. Por exemplo, as políticas podem permitir que os usuários criem somente recursos que tenham uma tag específica anexada. As políticas também podem restringir os usuários de criar ou modificar recursos que tenham determinadas tags.

> **Note**
>
> Se você usar tags para permitir ou negar o acesso de usuários a recursos, negue aos usuários a capacidade de adicionar ou remover essas tags para os mesmos recursos. Caso contrário, um usuário poderia contornar suas restrições e obter acesso a um recurso modificando suas tags.

Você pode usar as chaves de contexto de condição e os valores a seguir no elemento `Condition` (também chamado de bloco `Condition`) de uma declaração de política.

`aws:ResourceTag/`*`tag-key`*`: `*`tag-value`*

Permitir ou negar ações em recursos com tags específicas.

`aws:RequestTag/`*`tag-key`*`: `*`tag-value`*

Exigir que uma tag específica seja usada (ou não) ao criar ou modificar um recurso marcável.

`aws:TagKeys: [tag-key, ...]`

Exigir que um conjunto específico de chaves de tag seja usado (ou não usado) ao criar ou modificar um recurso marcável.

> **Note**
>
> As chaves e valores de contexto de condição em uma política do IAM se aplicam somente a ações que têm um recurso marcável como um parâmetro obrigatório. Por exemplo, você pode definir o acesso condicional baseado em tags para. ListAssets Você não pode ativar o acesso condicional baseado em tags PutLoggingOptionsporque nenhum recurso marcável é referenciado na solicitação.

Para obter mais informações, consulte Controle do acesso aos AWS recursos usando tags de recursos e a referência da política JSON do IAM no Guia do usuário do IAM.

Exemplo de políticas do IAM usando tags

- Visualizar ativos do AWS IoT SiteWise com base em tags

Solução de problemas AWS IoT SiteWise

Use as informações nessas seções para solucionar problemas com AWS IoT SiteWise.

Tópicos

Solução de problemas de operações de importação e exportação em massa

Para lidar e diagnosticar erros produzidos durante um trabalho de transferência, consulte a AWS IoT TwinMaker GetMetadataTransferJobAPI:

1. Depois de criar e executar um trabalho de transferência, chame a GetMetadataTransferJobAPI:

```
aws iottwinmaker get-metadata-transfer-job \
--metadata-transfer-job-id your_metadata_transfer_job_id \
--region us-east-1
```

2. O estado do trabalho muda para um dos estados abaixo:
   - CONCLUÍDO
   - CANCELADO
   - ERRO
3. A GetMetadataTransferJobAPI retorna um MetadataTransferJobProgressobjeto.
4. O MetadataTransferJobProgressobjeto contém os seguintes parâmetros:
   - FailedCount: indica a contagem de ativos que falharam durante o processo de transferência.
   - skippedCount: indica a contagem de ativos que foram ignorados durante o processo de transferência.

- SucceededCount: indica a contagem de ativos que foram bem-sucedidos durante o processo de transferência.
- TotalCount: indica a contagem total de ativos envolvidos no processo de transferência.

5. Além disso, um elemento reportURL é retornado pela chamada da API, que contém uma URL pré-assinada. Se sua tarefa de transferência tiver erros que precisem ser investigados, você pode baixar um relatório de erros completo neste URL.

Solução de problemas em um AWS IoT SiteWise portal

Solucione problemas comuns com seus AWS IoT SiteWise portais.

Usuários e administradores não podem acessar o portal AWS IoT SiteWise

Se os usuários ou administradores não puderem acessar seu AWS IoT SiteWise portal, você pode ter permissões restritas nas políticas anexadas AWS Identity and Access Management (IAM) que impedem logins bem-sucedidos.

Veja os seguintes exemplos de políticas do IAM que resultarão em falha de login:

> **Note**
>
> Qualquer política do IAM anexada que inclua um elemento `"Condition"` causará uma falha no login.

Exemplo 1: A condição aqui é um IP limitado, e isso causará uma falha no login.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iotsitewise:DescribePortal"
            ],
            "Resource": "*",
            "Condition": {
                "IpAddress": {
```

```
                    "aws:SourceIp": [
                        "REPLACESAMPLEIP"
                    ]
                }
            }
        }
    ]
}
```

Exemplo 2: A condição aqui é uma tag incluída, e isso causará uma falha no login.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iotsitewise:DescribePortal"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/project": "*"
                }
            }
        }
    ]
}
```

Ao adicionar usuários ou administradores ao portal, evite criar políticas do IAM que restrinjam as permissões do usuário, como IP limitado. Quaisquer políticas anexadas com permissões restritas não poderão se conectar ao AWS IoT SiteWise portal.

Solução de problemas de um gateway SiteWise Edge

AWS IoT SiteWise Os gateways Edge executam um conjunto de AWS IoT Greengrass componentes. Você pode configurar seu gateway SiteWise Edge para registrar eventos na Amazon CloudWatch e no sistema de arquivos local do seu gateway SiteWise Edge. Em seguida, você pode visualizar os arquivos de log para solucionar problemas no gateway do SiteWise Edge.

Você também pode visualizar CloudWatch as métricas relatadas pelos seus gateways do SiteWise Edge para solucionar problemas de conectividade ou fluxos de dados. Para ter mais informações, consulte Monitoramento AWS IoT SiteWise com CloudWatch métricas da Amazon.

Tópicos

Configurando e acessando os registros do SiteWise Edge Gateway

Antes de poder visualizar os registros do SiteWise Edge Gateway, você deve configurar seu SiteWise Edge Gateway para enviar registros para o Amazon CloudWatch Logs ou armazenar os registros no sistema de arquivos local.

- Use CloudWatch Registros se quiser usar o AWS Management Console para visualizar os arquivos de log do seu gateway SiteWise Edge. Para ter mais informações, consulte Usando o Amazon CloudWatch Logs.
- Use registros do sistema de arquivos local se quiser usar a linha de comando ou o software local para visualizar os arquivos de log do gateway SiteWise Edge. Para ter mais informações, consulte Usando registros de serviço.

Solução de problemas SiteWise do Edge Gateway

Use as informações a seguir para solucionar problemas do gateway SiteWise Edge.

Problemas

Não é possível implantar pacotes nos gateways SiteWise Edge

Se o componente AWS IoT Greengrass nucleus (`aws.greengrass.Nucleus`) estiver desatualizado, talvez você não consiga implantar pacotes no seu gateway SiteWise Edge. Você pode usar o AWS IoT Greengrass V2 console para atualizar o componente do AWS IoT Greengrass núcleo.

Atualize o componente do AWS IoT Greengrass núcleo (console)

1. Navegue até o console do AWS IoT Greengrass.
2. No painel de navegação, em AWS IoT Greengrass, escolha Implantações.
3. Na lista Deployments, selecione a implantação que você deseja revisar.
4. Escolha Revisar.
5. Na página Especificar destino, escolha Próximo.
6. Na página Selecionar componentes, em Componentes públicos, na caixa de pesquisa, digite **`aws.greengrass.Nucleus`** e em seguida escolha aws.greengrass.Nucleus.
7. Escolha Próximo.
8. Na página Configurar componentes, escolha Próximo.
9. Na página Definir configurações de segurança, escolha Próximo.
10. Na página Review, escolha Deploy.

AWS IoT SiteWise não recebe dados dos servidores OPC-UA

Se seus AWS IoT SiteWise ativos não estiverem recebendo dados enviados por seus servidores OPC-UA, você pode pesquisar os registros do gateway SiteWise Edge para solucionar problemas. Procure registros `swPublisher` de nível de informações que contenham a mensagem a seguir.

```
Emitting diagnostic name=PublishError.SomeException
```

Com base no tipo de *`SomeException`*registro, use os seguintes tipos de exceção e os problemas correspondentes para solucionar problemas com seu gateway SiteWise Edge:

- ResourceNotFoundException— Seus servidores OPC-UA estão enviando dados que não correspondem ao alias de propriedade de nenhum ativo. Essa exceção pode ocorrer em dois casos:

  - Os aliases de propriedade não correspondem exatamente às variáveis OPC-UA, incluindo qualquer prefixo de origem definido. Verifique se os aliases de propriedade e os prefixos de origem estão corretos.
  - Você não mapeou as variáveis OPC-UA para propriedades de ativos. Para ter mais informações, consulte Mapeamento de fluxos de dados industriais para propriedades de ativos.

    Se você já mapeou todas as variáveis OPC-UA que deseja inserir AWS IoT SiteWise, você pode filtrar quais variáveis OPC-UA o gateway Edge envia. SiteWise Para ter mais informações, consulte Usando filtros de nó OPC-UA.
- InvalidRequestException— Seus tipos de dados de variáveis OPC-UA não correspondem aos tipos de dados de propriedades do seu ativo. Por exemplo, se uma variável de OPC-UA tiver um tipo de dados inteiro, sua propriedade de ativo correspondente deverá ser do tipo de dados inteiro. Uma propriedade de ativo de tipo duplo não pode receber valores inteiros OPC-UA. Para corrigir esse problema, defina novas propriedades com os tipos de dados corretos.
- TimestampOutOfRangeException— Seu gateway SiteWise Edge está enviando dados que estão fora do alcance AWS IoT SiteWise aceito. AWS IoT SiteWise rejeita quaisquer pontos de dados com carimbos de data/hora anteriores a 7 dias no passado ou mais recentes que 5 minutos no futuro. Se seu gateway SiteWise Edge perdeu energia ou conexão com a AWS nuvem, talvez seja necessário limpar o cache do gateway SiteWise Edge.
- ThrottlingExceptionou LimitExceededException— Sua solicitação excedeu uma cota de AWS IoT SiteWise serviço, como taxa de pontos de dados ingeridos ou taxa de solicitação para operações de API de dados de propriedades de ativos. Verifique se a configuração não excede a AWS IoT SiteWise cotas.

Nenhum dado foi mostrado no painel

Se não houver dados mostrados em seu painel, a configuração do Publisher e a fonte de dados do gateway SiteWise Edge podem estar fora de sincronia. Se estiverem fora de sincronia, a atualização do nome da fonte de dados pode acelerar a sincronização da nuvem para a borda, corrigindo o erro Fora de sincronização.

Para atualizar o nome de uma fonte de dados

1. Navegue até o console do AWS IoT SiteWise.
2. No painel de navegação, escolha Edge gateways.
3. Selecione o gateway SiteWise Edge conectado ao painel.

4. Em Fontes de dados, selecione Editar.
5. Selecione um novo nome de fonte e selecione Salvar para confirmar sua alteração.
6. Verifique suas alterações confirmando que o nome da fonte de dados foi atualizado na tabela Fontes de dados.

“Não foi possível encontrar ou carregar a classe principal” que aparece no aws.iot. SiteWiseEdgePublisher registra em /greengrass/v2/logs error

Se você ver esse erro, talvez seja necessário atualizar a versão java do seu gateway SiteWise Edge.

- Em um terminal, execute o comando a seguir:

```
java -version
```

  A versão do java com a qual seu gateway SiteWise Edge está sendo executado aparecerá abaixo`OpenJDK Runtime Environment`. Você verá uma resposta como a seguinte:

```
openjdk version "11.0.20" 2023-07-18 LTS
OpenJDK Runtime Environment Corretto011.0.20.8.1 (build 11.0.20+8-LTS
OpenJDK 64-Bit Server VM Corretto-11.0.20.8.1 (build 11.0.20+8-LTS, mixed node)
```

Se você estiver executando a versão 11.0.20.8.1 do Java, deverá atualizar o pacote do IoT SiteWise Publisher para a versão 2.4.1 ou mais recente. Somente a versão 11.0.20.8.1 do java é afetada. Ambientes com outras versões java podem continuar usando versões mais antigas do componente IoT Publisher. SiteWise Para obter mais informações sobre a atualização de um pacote de componente, consulte Alterando a versão dos pacotes de componentes do SiteWise Edge Gateway.

Solução de AWS IoT Greengrass problemas

Para encontrar soluções para muitos problemas ao configurar ou implantar seu gateway SiteWise Edge AWS IoT Greengrass, consulte Solução de problemas AWS IoT Greengrass no Guia do AWS IoT Greengrass desenvolvedor.

Solução de problemas de uma ação de AWS IoT SiteWise regra

Para solucionar problemas de sua ação de AWS IoT SiteWise regra em AWS IoT Core, você pode executar um dos seguintes procedimentos:

- Configurar Amazon CloudWatch Logs
- Configure uma ação de erro de republicação para a regra

Depois, compare as mensagens de erro com os erros deste tópico a fim de solucionar o problema.

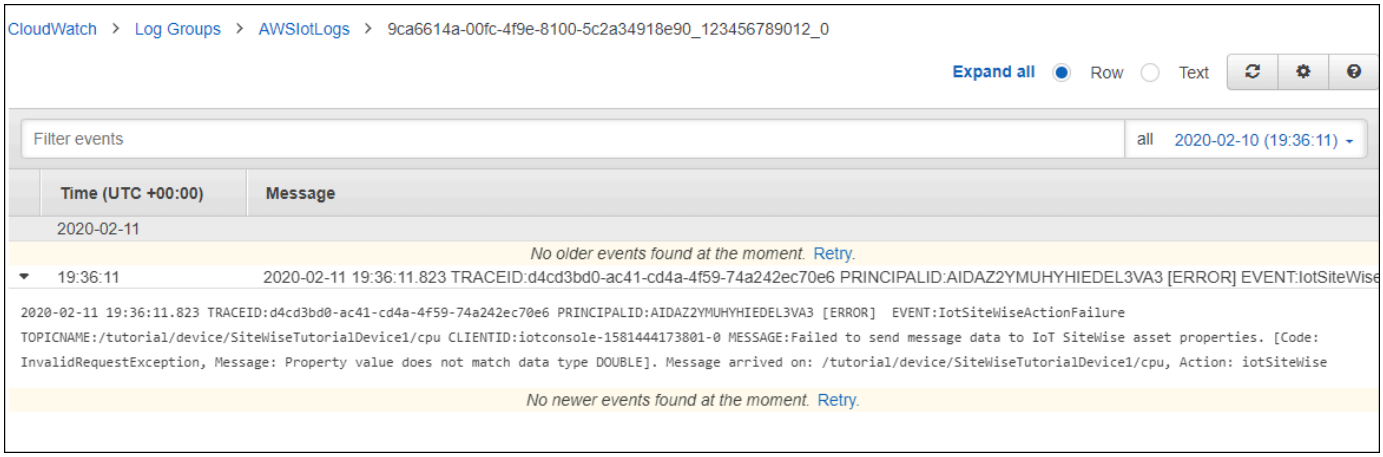
Tópicos

Configurando registros AWS IoT Core

Você pode configurar AWS IoT para registrar vários níveis de informações no CloudWatch Logs.

Para configurar e acessar CloudWatch registros

1. Para configurar o registro em log AWS IoT Core, consulte Monitoramento com CloudWatch registros no Guia do AWS IoT desenvolvedor.
2. Navegue até o console do CloudWatch .
3. No painel de navegação, escolha Grupos de logs.
4. Escolha o AWSIotLogsgrupo.
5. Escolha um fluxo de log recente. Por padrão, CloudWatch exibe primeiro o fluxo de registros mais recente.
6. Escolha uma entrada de log para expandir a mensagem de log. A entrada de log para se parecer com a captura de tela a seguir.



7. Compare as mensagens de erro com os erros deste tópico a fim de solucionar o problema.

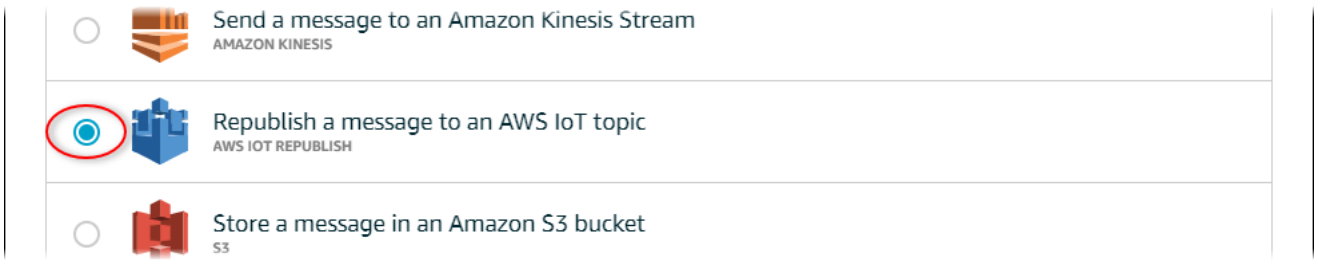
Configurar uma ação de erro de republicação

É possível configurar uma ação de erro na regra para processar mensagens de erro. Neste procedimento, configure a ação de regra de republicação como uma ação de erro para exibir mensagens de erro no cliente de teste MQTT.

> **Note**
>
> A ação de erro de republicação gera somente o equivalente de logs de nível ERROR. Se você quiser registros mais detalhados, deverá configurar CloudWatch os registros.

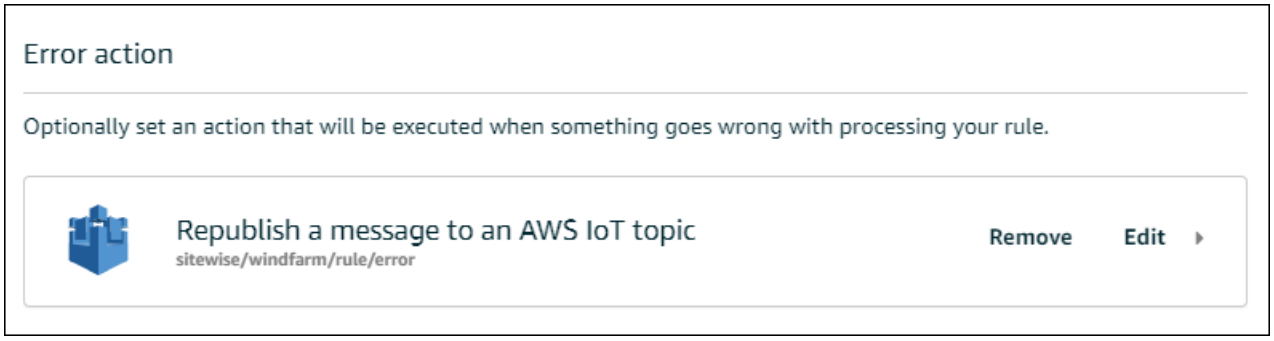
Como adicionar uma ação de erro de republicação a uma regra

1. Navegue até o console do AWS IoT.
2. No painel de navegação esquerdo, escolha Agir e Regras.
3. Selecione a regra.
4. Em Error action (Ação de erro), escolha Add action (Adicionar ação).
5. Escolha Republicar uma mensagem em um AWS IoT tópico.



6. Escolha Configurar ação na parte inferior da página.
7. Em Tópico, insira um tópico exclusivo (por exemplo,**`sitewise/windfarm/rule/error`**). AWS IoT Core republicará as mensagens de erro neste tópico.
8. Escolha Selecionar para conceder AWS IoT Core acesso para executar a ação de erro.
9. Selecione Select (Escolher) ao lado da função criada para a regra.
10. Escolha Update Role (Atualizar função) para adicionar outras permissões à função.
11. Selecione Adicionar ação.

    A ação de erro da regra deve ser semelhante à captura de tela a seguir.



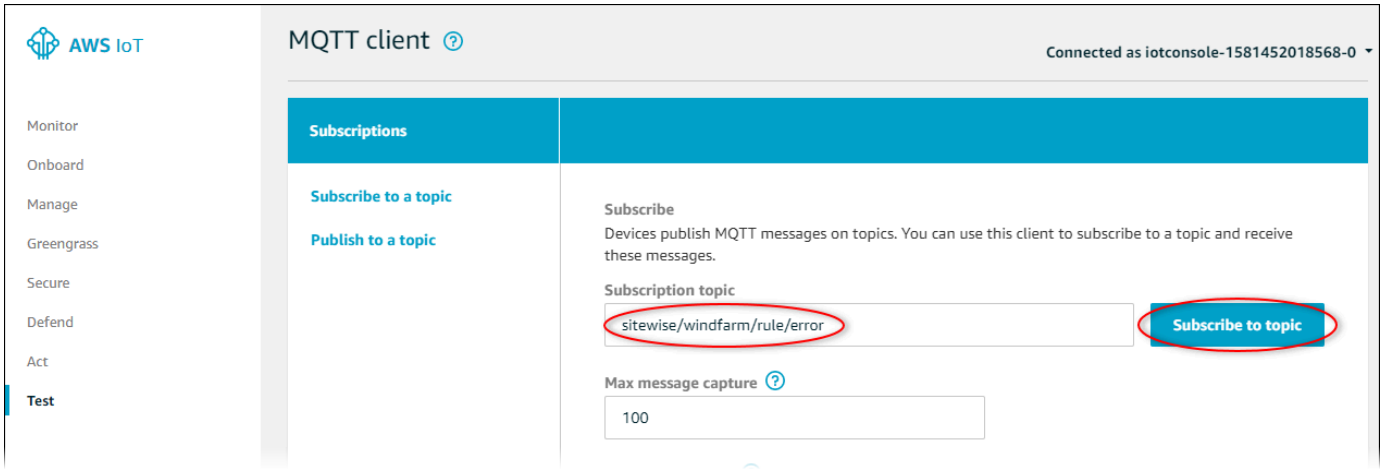
12. Escolha a seta para trás no canto superior esquerdo do console para retornar à página inicial do AWS IoT console.

Depois de configurar a ação de erro de republicação, você pode visualizar as mensagens de erro no cliente de teste MQTT no AWS IoT Core.

No procedimento a seguir, você se inscreve no tópico de erro no cliente de teste MQTT. No cliente de teste MQTT, é possível receber as mensagens de erro da regra para solucionar o problema.

Como se inscrever no tópico de ação de erro

1. Navegue até o console do AWS IoT.
2. Na página de navegação à esquerda, selecione Test (Testar) para abrir o cliente de teste MQTT.
3. No campo Subscription topic (Tópico de assinatura), insira o tópico de erro configurado anteriormente (por exemplo, **`sitewise/windfarm/rule/error`**) e selecione Subscribe to topic (Assinar o tópico).



4. Aguarde até que as mensagens de erro sejam exibidas e expanda a matriz `failures` em qualquer mensagem de erro.

   Depois, compare as mensagens de erro com os erros deste tópico a fim de solucionar o problema.

Solução de problemas

Use as informações a seguir para solucionar problemas de regra.

Problemas

- Erro: o membro deve estar entre 604.800 segundos antes e 300 segundos depois do time stamp atual.
- Erro: o valor da propriedade não corresponde ao tipo de dados <type>
- Erro: Usuário: <role-arn>não está autorizado a executar: iotsitewise: no recurso BatchPutAssetPropertyValue
- Erro: iot.amazonaws.com não consegue executar: sts: no recurso: AssumeRole <role-arn>
- Informação: nenhuma solicitação foi enviada. PutAssetPropertyValueEntries estava vazio após a execução dos modelos de substituição.

Erro: o membro deve estar entre 604.800 segundos antes e 300 segundos depois do time stamp atual.

Seu time stamp tem mais de 7 minutos ou menos de 5 minutos, comparado ao horário Unix epoch atual. Faça o seguinte:

- Verifique e o time stamp está no horário Unix epoch (UTC). Se fornecer um time stamp com um fuso horário diferente, você receberá esse erro.
- Verifique se seu carimbo de data/hora está em segundos. AWS IoT SiteWise espera que os carimbos de data/hora sejam divididos em segundos (na época do Unix) e compensados em nanossegundos.
- Verifique se você está fazendo upload de dados com time stamp de até 7 dias antes.

Erro: o valor da propriedade não corresponde ao tipo de dados <type>

Uma entrada na ação de regra tem um tipo de dados diferente da propriedade de ativo do destino. Por exemplo, a propriedade de ativo do destino é um `DOUBLE` e o tipo de dados que você selecionou é Integer (Inteiro) ou o valor foi transmitido em `integerValue`. Faça o seguinte:

- Se você configurar a regra no AWS IoT console, verifique se escolheu o tipo de dados correto para cada entrada.
- Se você configurar a regra a partir da API ou AWS Command Line Interface (AWS CLI), verifique se seu `value` objeto usa o campo de tipo correto (por exemplo, `doubleValue` para uma `DOUBLE` propriedade).

Erro: Usuário: <role-arn>não está autorizado a executar: iotsitewise: no recurso BatchPutAssetPropertyValue

A regra não está autorizada a acessar a propriedade de ativo do destino, ou a propriedade de ativo do destino não existe. Faça o seguinte:

- Verifique se o alias da propriedade está correto e se você tem uma propriedade de ativo com o alias de propriedade fornecido. Para ter mais informações, consulte Mapeamento de fluxos de dados industriais para propriedades de ativos.
- Verifique se a regra tem uma função e se a função tem a concede a permissão `iotsitewise:BatchPutAssetPropertyValue` à propriedade de ativo do destino, como por toda a hierarquia do ativo de destino. Para ter mais informações, consulte Concedendo AWS IoT o acesso necessário.

Erro: iot.amazonaws.com não consegue executar: sts: no recurso: AssumeRole <role-arn>

Seu usuário não está autorizado a assumir a função em sua regra no AWS Identity and Access Management (IAM).

Verifique se o seu usuário tem a permissão do `iam:PassRole` para a função em sua regra. Para obter mais informações, consulte Pass role permissions no Guia do desenvolvedor do AWS IoT .

Informação: nenhuma solicitação foi enviada. PutAssetPropertyValueEntries estava vazio após a execução dos modelos de substituição.

> **Note**
>
> Essa mensagem é um log de nível `INFO`.

A solicitação deve ter pelo menos uma entrada com todos os parâmetros necessários.

Verifique se os parâmetros da regra, incluindo os modelos de substituição, resultam em valores não vazios. Os modelos de substituição não podem acessar valores definidos nas cláusulas `AS` na instrução de consulta da regra. Para obter mais informações, consulte Modelos de substituição no Guia do desenvolvedor do AWS IoT .

Solucionar problemas de uma regra

Siga as etapas deste procedimento para solucionar problemas de sua regra se os dados de uso da CPU e da memória não estiverem aparecendo AWS IoT SiteWise conforme o esperado. Neste procedimento, configure a ação de regra de republicação como uma ação de erro para exibir mensagens de erro no cliente de teste MQTT. Você também pode configurar o registro no CloudWatch Logs para solucionar problemas. Para ter mais informações, consulte Solução de problemas de uma ação de AWS IoT SiteWise regra.

Como adicionar uma ação de erro de republicação a uma regra

1. Navegue até o console do AWS IoT.
2. No painel de navegação à esquerda, escolha Roteamento de mensagens e Regras.
3. Escolha a regra que criou anteriormente e escolha Edit.

4. Em Ação de erro - opcional, escolha Adicionar ação de erro.
5. Escolha Republicar uma mensagem em um AWS IoT tópico.
6. Em Tópico, insira o caminho para o erro (por exemplo,**`sitewise/rule/tutorial/error`**). AWS IoT Core republicará as mensagens de erro neste tópico.
7. Escolha a função que você criou anteriormente (por exemplo, SiteWiseTutorialDeviceRuleRole).
8. Escolha Atualizar.

Depois de configurar a ação de erro de republicação, você pode visualizar as mensagens de erro no cliente de teste MQTT no AWS IoT Core.

No procedimento a seguir, você se inscreve no tópico de erro no cliente de teste MQTT.

Como se inscrever no tópico de ação de erro

1. Navegue até o console do AWS IoT.
2. Na página de navegação à esquerda, selecione MQTT test client para abrir o cliente de teste MQTT.
3. Em Filtro de tópicos, insira **`sitewise/rule/tutorial/error`** e, em seguida, escolha Criar assinatura.

Quando forem exibidas mensagens de erro, visualize a matriz `failures` em qualquer mensagem de erro para diagnosticar problemas. Para obter mais informações sobre possíveis problemas e como resolvê-los, consulte Solução de problemas de uma ação de AWS IoT SiteWise regra.

Se os erros não aparecerem, verifique se a regra está habilitada e se você se inscreveu no mesmo tópico que configurou na ação de erro de republicação. Se os erros ainda não aparecerem depois que você fizer isso, verifique se o script do dispositivo está sendo executado e se está atualizando a sombra do dispositivo com êxito.

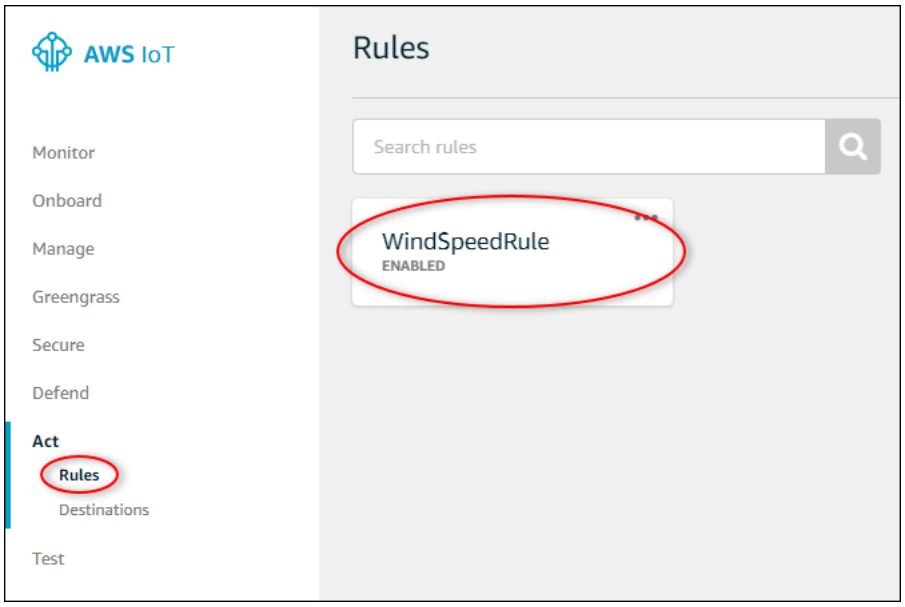
> **Note**
>
> Você também pode se inscrever no tópico de atualização paralela do seu dispositivo para ver a carga útil que sua AWS IoT SiteWise ação analisa. Para fazer isso, assine o tópico a seguir.
>
> ```
> $aws/things/+/shadow/update/accepted
> ```

Solucionar problemas de uma regra

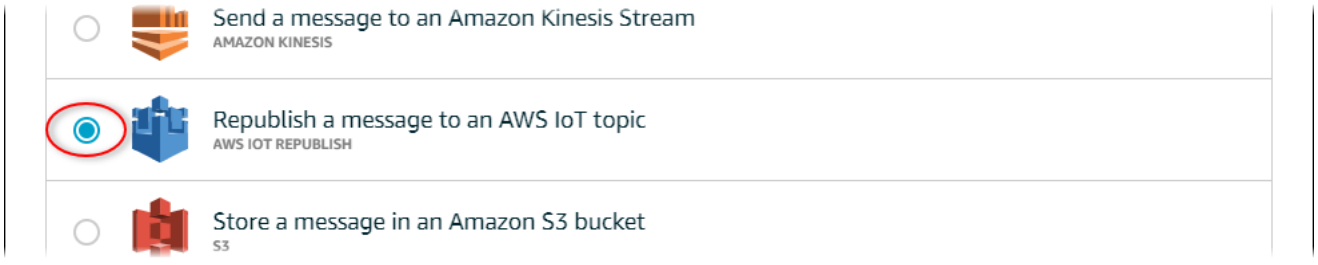
Siga as etapas neste procedimento para solucionar problemas de sua regra se os dados do ativo de demonstração não estiverem aparecendo na tabela do DynamoDB conforme o esperado. Neste procedimento, configure a ação de regra de republicação como uma ação de erro para exibir mensagens de erro no cliente de teste MQTT. Você também pode configurar o registro no CloudWatch Logs para solucionar problemas. Para obter mais informações, consulte Monitoramento com CloudWatch registros no Guia do AWS IoT desenvolvedor.

Como adicionar uma ação de erro de republicação a uma regra

1. Navegue até o console do AWS IoT.
2. No painel de navegação esquerdo, escolha Agir e Regras.
3. Escolha a regra que criou anteriormente.

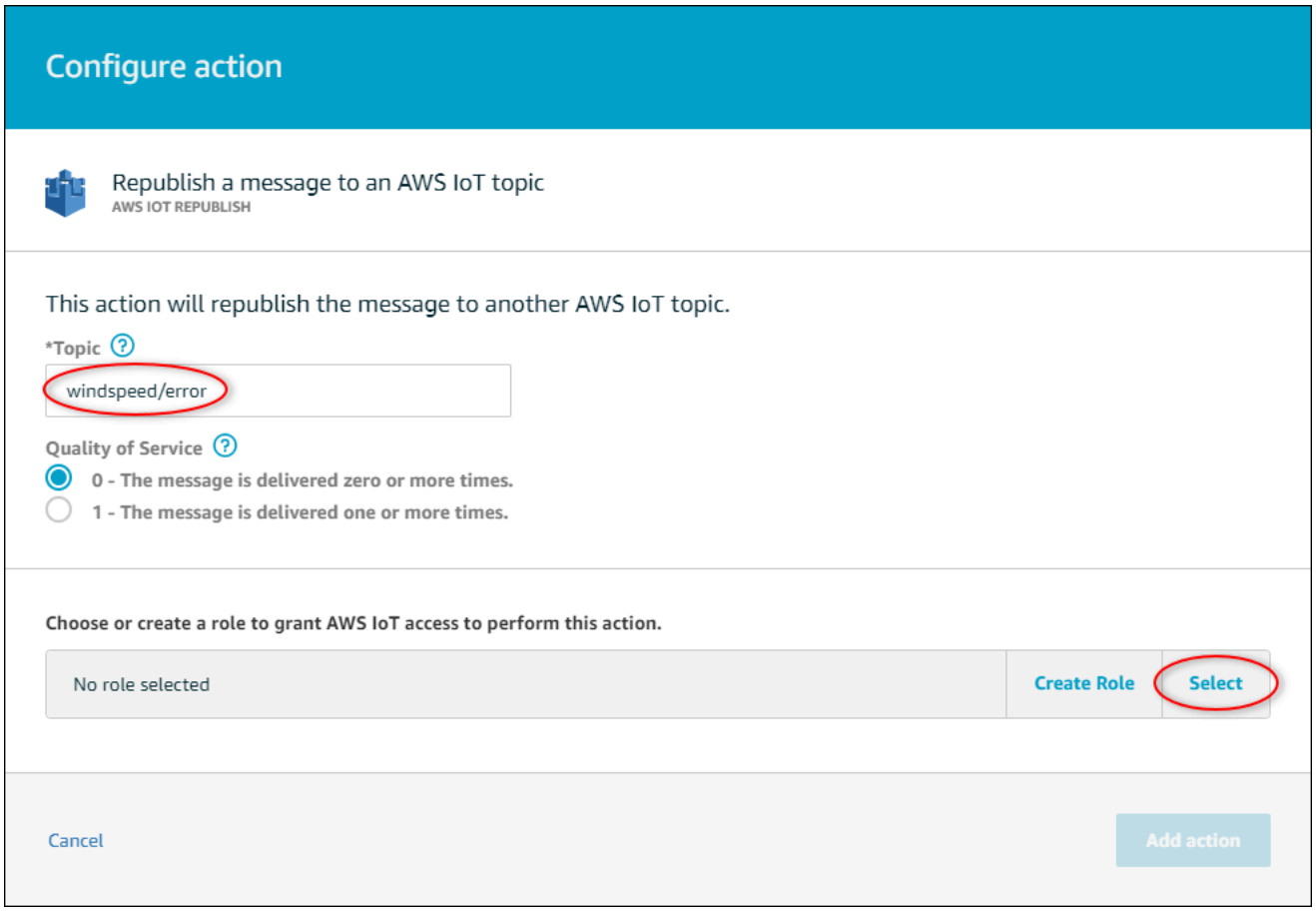


4. Em Error action (Ação de erro), escolha Add action (Adicionar ação).
5. Escolha Republicar uma mensagem em um AWS IoT tópico.

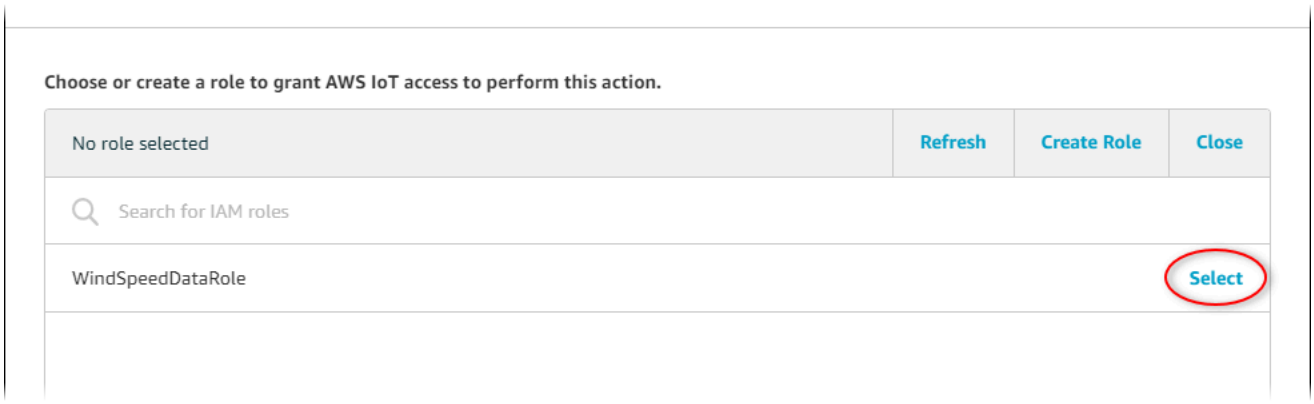


6. Escolha Configurar ação na parte inferior da página.

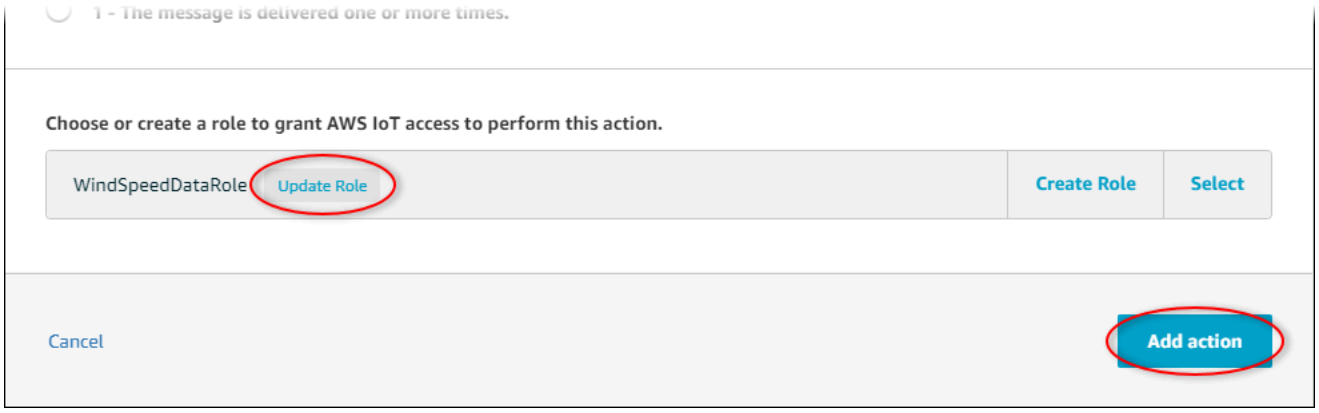
7. Em Tópico, insira **`windspeed/error`**. AWS IoT O Core republicará as mensagens de erro neste tópico.



8. Escolha Selecionar para conceder acesso ao AWS IoT Core para executar a ação de erro usando a função que você criou anteriormente.
9. Escolha Select (Selecionar) ao lado da função.



10. Escolha Update Role (Atualizar função) para adicionar outras permissões à função.



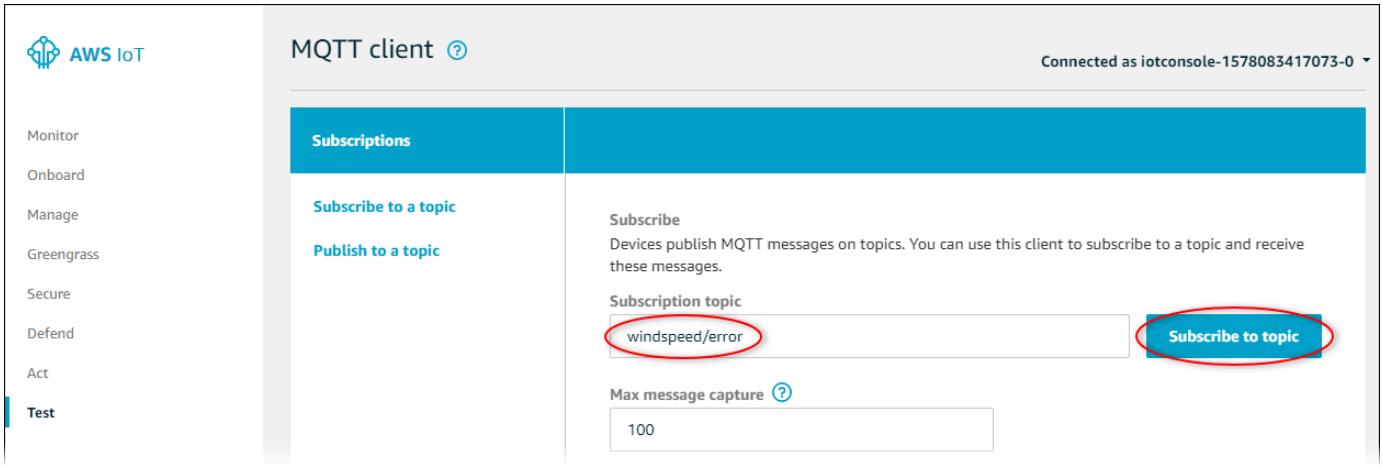
11. Escolha Add action (Adicionar ação) para concluir a adição da ação de erro.
12. Escolha a seta para trás no canto superior esquerdo do console para retornar à página inicial do console AWS IoT Core.

Depois de configurar a ação de erro de republicação, você pode visualizar as mensagens de erro no cliente de teste MQTT no AWS IoT Core.

No procedimento a seguir, você se inscreve no tópico de erro no cliente de teste MQTT.

Como se inscrever no tópico de ação de erro

1. Na página de navegação à esquerda do console AWS IoT principal, escolha Testar.
2. No campo Subscription topic (Tópico de assinatura), insira **`windspeed/error`** e selecione Subscribe to topic (Assinar o tópico).



3. Observe a exibição de mensagens de erro e explore a matriz `failures` em uma mensagem de erro para diagnosticar os seguintes problemas comuns:

   - Erros de digitação na instrução de consulta de regra

- Permissões de função insuficientes

Se os erros não aparecerem, verifique se a regra está habilitada e se você se inscreveu no mesmo tópico que configurou na ação de erro de republicação. Se os erros ainda não aparecerem, verifique se os ativos de parque eólico de demonstração ainda existem e se você ativou notificações nas propriedades da velocidade do vento. Se seus ativos de demonstração expiraram e desapareceram AWS IoT SiteWise, você pode criar uma nova demonstração e atualizar a declaração de consulta de regras para refletir o modelo de ativo e os IDs de propriedade atualizados.

AWS IoT SiteWise endpoints e cotas

As seções a seguir descrevem os endpoints e as cotas para. AWS IoT SiteWise

Conteúdo

AWS IoT SiteWise endpoints

Para se conectar programaticamente a AWS IoT SiteWise, você usa um endpoint. Os AWS SDKs e o AWS Command Line Interface (AWS CLI) usam automaticamente o endpoint padrão em uma AWS região. Para obter mais informações sobre regiões onde AWS IoT SiteWise está disponível, consulte AWS IoT SiteWise endpoints e cotas no. Referência geral da AWS

AWS IoT SiteWise suporta os seguintes endpoints.

data.iotsitewise.region.amazonaws.com

Use esse endpoint para acessar as seguintes operações de API do plano de dados: BatchPutAssetPropertyValueGetAssetPropertyAggregates, GetAssetPropertyValue, GetAssetPropertyValueHistorye. GetInterpolatedAssetPropertyValues *`region`*Substitua pela sua AWS região.

api.iotsitewise.region.amazonaws.com

AWS IoT SiteWise oferece esse endpoint consolidado para as operações de API do plano de controle que você usa para gerenciar modelos de ativos, ativos, gateways SiteWise Edge, tags e configurações de conta. Substitua *`region`* pela sua região da AWS .

> **Note**
>
> - Por padrão, AWS IoT SiteWise usa o endpoint consolidado quando você faz chamadas para as operações de API do plano de controle suportadas.
> - Recomendamos usar o endpoint consolidado para as operações de API do ambiente de gerenciamento compatível.

- Você não pode usar o endpoint consolidado para acessar as operações da API SiteWise Monitor.

As operações de API do plano de controle suportadas incluem AssociateAssetsCreateAssetCreateAssetModelDeleteAsset, DeleteAssetModel, DeleteDashboard, DescribeAsset, DescribeAssetModel, DescribeAssetProperty, DescribeDashboard, DescribeLoggingOptions, DisassociateAssets, ListAssetModels, ListAssetRelationships, ListAssets, ListAssociatedAssets, PutLoggingOptions, UpdateAsset, UpdateAssetModel, UpdateAssetProperty, CreateGateway, DeleteGateway, DescribeGateway, DescribeGatewayCapabilityConfiguration, ListGateways, UpdateGatewayUpdateGatewayCapabilityConfiguration, DescribeStorageConfiguration, PutStorageConfiguration, DescribeDefaultEncryptionConfiguration, ListTagsForResource, PutDefaultEncryptionConfiguration, TagResource,, UntagResourcee.

O endpoint da VPC da interface para as operações da API do ambiente de gerenciamento suporta somente o endpoint consolidado. Para ter mais informações, consulte Endpoints da VPC .

iotsitewise.region.amazonaws.com

Use esse endpoint para acessar as seguintes operações de API: DescribeStorageConfigurationPutStorageConfiguration, DescribeDefaultEncryptionConfiguration, ListTagsForResource, PutDefaultEncryptionConfiguration, TagResource, e. UntagResource Substitua *region* pela sua região da AWS .

model.iotsitewise.region.amazonaws.com

Use esse endpoint para acessar as seguintes operações de API: AssociateAssetsCreateAsset, CreateAssetModel,, DeleteAsset, DeleteAssetModel, DeleteDashboard, DescribeAsset, DescribeAssetModel, DescribeAssetProperty, DescribeDashboard, DescribeLoggingOptions, DisassociateAssets, ListAssetModels, ListAssetRelationships, ListAssets, ListAssociatedAssets, PutLoggingOptionsUpdateAssethttps://docs.aws.amazon.com/iot-sitewise/latest/APIReference/API_UpdateAsset.html, UpdateAssetModel, UpdateAssetPropertye. *region*Substitua pela sua AWS região.

edge.iotsitewise.region.amazonaws.com

Use esse endpoint para acessar as seguintes operações de API: CreateGatewayDeleteGateway, DescribeGateway, DescribeGatewayCapabilityConfiguration, ListGateways, UpdateGateway, e. UpdateGatewayCapabilityConfiguration *region*Substitua pela sua AWS região.

monitor.iotsitewise.region.amazonaws.com

Use esse endpoint para acessar as seguintes operações de API: BatchAssociateProjectAssetsBatchDisassociateProjectAssets, CreateAccessPolicy,, CreateDashboard, CreatePortal, CreateProject, DeleteAccessPolicy, DeletePortal, DeleteProject, DescribeAccessPolicy, DescribePortal, DescribeProject, ListAccessPolicies, ListDashboards, ListPortals, ListProjectAssets, ListProjectsUpdateAccessPolicyhttps://docs.aws.amazon.com/iot-sitewise/latest/APIReference/API_UpdateAccessPolicy.html, UpdateDashboardUpdatePortal,, UpdateProjecte. Substitua *region* pela sua região da AWS .

AWS IoT SiteWise cotas

As tabelas a seguir descrevem as cotas em AWS IoT SiteWise. Para obter mais informações sobre cotas e como solicitar um aumento de cota, consulte AWS Service Quotas no Referência geral da AWS. Para obter mais informações sobre AWS IoT SiteWise cotas, consulte cotas AWS IoT SiteWise de serviço no. Referência geral da AWS

Cotas para ativos e modelos de ativos

Recurso	Cota	Ajustável	Observações
Número de modelos de ativos por região por AWS conta	1000	Sim	
Número de ativos por modelo de ativo	10.000	Sim	
Número de ativos filho por ativo pai	2000	Sim	

Recurso	Cota	Ajustável	Observações
Profundidade da árvore hierárquica de ativos	30	Sim	
Número de definições de hierarquia de ativos por modelo de ativo	30	Yes	
Número de propriedades no nível raiz por modelo de ativo	500	Sim	Esse número máximo de `assetModelProperties` para cada modelo de ativo. Essa contagem não inclui `compositeModelProperties` . Essa cota também se aplica a qualquer ativo exclusivo criado a partir desse modelo de ativo.

Recurso	Cota	Ajustável	Observações
Número de propriedades por modelo de ativo	5000	Sim	O número máximo de propriedades de um modelo de ativo do tipo `ASSET_MODEL` ou `COMPONENT_MODEL`. Esse número é determinado pela combinação das propriedades do modelo de ativo raiz e de qualquer modelo composto incluído component-model-based ou em linha. Essa cota também se aplica a qualquer ativo exclusivo criado a partir desse modelo de ativo.
Número de propriedades por modelo composto	100	Sim	O número máximo de propriedades permitido para modelos compostos. Além disso, o número máximo de propriedades permitido para um modelo de ativo do tipo `COMPONENT_MODEL`.

Recurso	Cota	Ajustável	Observações
Profundidade da árvore de propriedades por modelo de ativo	10	Não	Por exemplo, um modelo com uma propriedade de transformação C que consome uma propriedade de transformação B que consome uma propriedade de medição A tem uma profundidade de 3.
Número de modelos de ativos por árvore hierárquica	100	Sim	

Recurso	Cota	Ajustável	Observações
Número de propriedades diretamente dependentes por modelo de ativo	20	Não	Essa cota limita quantas propriedades podem depender diretamente de uma única propriedade, conforme definido nas expressões de fórmula de propriedade. O número de propriedades dependentes de um modelo de ativo deve ser maior que o número de propriedades diretamente dependentes por modelo de ativo. Você deve solicitar um aumento de cota para ambos se o limite do Número de propriedades diretamente dependentes por modelo de ativo for maior que o limite do Número de propriedades dependentes por modelo de ativo.

Recurso	Cota	Ajustável	Observações
Número de proprieda des dependentes por modelo de ativo	30	Não	Essa cota limita quantas proprieda des podem depender direta ou indiretam ente de uma única propriedade, conforme definido nas expressões de fórmula de proprieda de.
Número de modelos compostos por modelo de ativo	50	Sim	O número máximo de modelos compostos permitidos em um único modelo de ativo.
Profundidade do modelo composto	2	Sim	A profundidade máxima da árvore do modelo composto por modelo de ativo, incluindo modelos em linha e component -model-based compostos.

Recurso	Cota	Ajustável	Observações
Número de modelos de ativos exclusivos que usam o mesmo modelo de component e	20	Sim	O número máximo de modelos de ativos exclusivo s que têm pelo menos um modelo component-model-based composto que faz referência direta a um modelo de ativo específico do tipo COMPONENT _MODEL.
Número de variáveis de propriedade por expressão de fórmula de propriedade	10	Não	Por exemplo, há duas variáveis de propriedade `power` e `temp`, na expressão `avg(power) + max(temp)` . Isso também se aplica aos resultados da computação de transformação.
Número de funções por expressão de fórmula de proprieda de	10	Não	Por exemplo, há duas funções, `avg` e `max`, na expressão `avg(power) + max(temp)` .

Cotas para dados de propriedade de ativos

Recurso	Cota	Ajustável	Observações
Taxa de solicitação para operações de API de dados de propriedade de ativos	1000 solicitações por segundo por região por AWS conta	Sim	Essa cota se aplica a operações de API, como `GetAssetPropertyValue` e `BatchPutAssetPropertyValue`.
Número de pontos de dados por segundo por qualidade de dados por propriedade do ativo	10 pontos de dados	Não	Essa cota se aplica ao número máximo de pontos de dados timestamp-quality-value (TQV) com o mesmo registro de data e hora em segundos por qualidade de dados para cada propriedade do ativo. Você pode armazenar até esse número de pontos de dados de boa qualidade, de qualidade incerta, e de baixa qualidade a qualquer segundo para cada propriedade do ativo.
Número de `BatchPutAssetPropertyValue` entradas ingeridas por segundo	10 entradas por propriedade do ativo	Não	Essa cota se aplica às `BatchPutAssetPropertyValue` entradas de todas as fontes,

Recurso	Cota	Ajustável	Observações
por propriedade do ativo por região por AWS conta.			incluindo gateways, AWS IoT Core regras e chamadas de API do SiteWise Edge.
Taxa de pontos de dados ingeridos	5000 pontos de dados por segundo por região por AWS conta	Sim	Pontos de dados Timestamp-quality-value (TQV).
Taxa de solicitações para `BatchGetAssetPropertyAggregates`	200	Sim	O número máximo de solicitações de `BatchGetAssetPropertyAggregates` por segundo permitido nessa conta na região da região atual.
Taxa de solicitações para `BatchGetAssetPropertyValue`	500	Sim	O número máximo de solicitações de `BatchGetAssetPropertyValue` por segundo permitido nessa conta na região da região atual.
Taxa de solicitações para `BatchGetAssetPropertyValueHistory`	200	Sim	O número máximo de solicitações de `BatchGetAssetPropertyValueHistory` por segundo permitido nessa conta na região da região atual.

Recurso	Cota	Ajustável	Observações
Número de `BatchPutAssetPropertyValue` entradas ingeridas por segundo por propriedade do ativo por região por AWS conta.	10 entradas por propriedade do ativo	Não	Essa cota se aplica às `BatchPutAssetPropertyValue` entradas de todas as fontes, incluindo gateways, AWS IoT Core regras e chamadas de API do SiteWise Edge.
Taxa de solicitações `GetAssetPropertyAggregates` e consultas de entrada `BatchGetAssetPropertyAggregates` por propriedade do ativo	50	Não	O número máximo de solicitações `GetAssetPropertyAggregates` e entradas `BatchGetAssetPropertyAggregates` para cada propriedade de ativos por segundo nesta conta na região da atual.
Taxa de solicitações `GetAssetPropertyValue` e consultas de entrada `BatchGetAssetPropertyValue` por propriedade do ativo	500	Não	O número máximo de solicitações `GetAssetPropertyValue` e entradas `BatchGetAssetPropertyValue` para cada propriedade de ativos por segundo nesta conta na região da atual.

Recurso	Cota	Ajustável	Observações
Taxa de solicitações `GetAssetPropertyValueHistory` e consultas de entrada `BatchGetAssetPropertyValueHistory` por propriedade do ativo	30	Não	O número máximo de solicitações `GetAssetPropertyValueHistory` e entradas `BatchGetAssetPropertyValueHistory` para cada propriedade de ativos por segundo nesta conta na região da atual.
Taxa de solicitações do `GetInterpolatedAssetPropertyValues`	500	Sim	O número máximo de solicitações de `GetInterpolatedAssetPropertyValues` por segundo permitido nessa conta na região da região atual.
Número de resultados por solicitação `GetInterpolatedAssetPropertyValues`	10	Sim	O número máximo de resultados a serem retornados por solicitação do `GetInterpolatedAssetPropertyValues` .

Recurso	Cota	Ajustável	Observações
Taxa de pontos de dados recuperados de `GetAssetPropertyValueHistory` e `BatchGetAssetPropertyValueHistory`	100 MB de resposta de leitura por segundo por região por AWS conta.	Sim	A taxa máxima de bytes (MB/segundo) dos pontos de dados recuperados por segundo por região por conta em e. AWS `GetAssetPropertyValueHistory` `BatchGetAssetPropertyValueHistory` A carga de resposta avaliada para essa cota usa campos Time stamp-Quality-Value (TQV) para cada ponto de dados e arredonda o tamanho do byte de cada solicitação de API para o próximo incremento de 4 KB. Os pontos de dados T imestamp-quality-value (TQV) recuperados por segundo variam de acordo com o tipo de dados: • Número inteiro — até 5 milhões de TQV por segundo

Recurso	Cota	Ajustável	Observações
			• Duplo — até 4 milhões de TQV por segundo • Booliano — até 6 milhões de TQV por segundo • String — varia com base no tamanho de cada valor da sequência de caracteres.

Cotas para gateways SiteWise Edge

Recurso	Cota	Ajustável
Número de gateways SiteWise Edge por região por conta AWS	100	Sim
Número de fontes OPC-UA por SiteWise gateway Edge	100	Não

Cotas para AWS IoT SiteWise Monitor

Recurso	Cota	Ajustável
Número de portais por região por conta AWS	100	Sim
Número de projetos por portal	100	Sim
Número de painéis por projeto	100	Sim

Recurso	Cota	Ajustável
Número de ativos raiz por projeto	1	Não
Número de visualizações por painel	10	Sim
Número de métricas por visualização de painel	5	Sim
Número de limites por visualização de painel	12	Não

Cotas para importação e exportação AWS IoT SiteWise em massa de metadados

Recurso	Descrição	Cota	Ajustável
Número de trabalhos de transferência de metadados na fila	O número máximo de trabalhos de transferência de `PENDING` metadados na fila.	10	Sim
Tamanho do arquivo de importação da tarefa de transferência de metadados	O tamanho máximo do arquivo importado (em MB).	100 MB	Sim
AWS IoT SiteWise cota de recursos para um trabalho de transferência de metadados	O número máximo de recursos importados ou exportados em um único trabalho. Um recurso inclui ativos e modelos de ativos.	5000	Não

Cotas para importação AWS IoT SiteWise em massa de dados

Recurso	Cota	Ajustável
Número de trabalhos de importação em massa em execução	100	Não
Tamanho do arquivo CSV	10 GB	Não
Tamanho do arquivo de parquet não compactado	256 MB	Não
Tamanho do `CSV` arquivo para ingestão em buffer	256 MB	Não
Tamanho do grupo de fileiras de parquete não compactado	64 MB	Não
Número de medidas exclusivas por grupo de fileiras de parquete	2000	Sim
Número de dias entre o registro de data e hora no passado e hoje para ingestão em buffer	30	Sim
Taxa de solicitação `CreateBulkImportJobs` para cada região em cada AWS conta	10	Sim
Taxa de solicitação `ListBulkImportJobs` para cada região em cada AWS conta	50	Sim
Taxa de solicitação `DescribeBulkImport`	50	Sim

Recurso	Cota	Ajustável
`Jobs` para cada região em cada AWS conta		

Cotas para detecção de anomalias

As cotas para detecção de anomalias são compartilhadas entre o Amazon Lookout for Equipment e o AWS IoT SiteWise Amazon Lookout for Equipment. Para obter mais informações, consulte Cotas para usar o Lookout for Equipment.

Histórico de documentos para o Guia AWS IoT SiteWise do usuário

A tabela a seguir descreve a documentação desta versão do AWS IoT SiteWise.

- Versão da API: 02-12-2019

Alteração	Descrição	Data
Suporte adicionado para executar o SiteWise Edge no Siemens Industrial Edge	AWS IoT SiteWise agora suporta a execução do SiteWise Edge em dispositivos Siemens Industrial Edge.	26 de novembro de 2023
Suporte adicional para armazenamento em camadas quentes	AWS IoT SiteWise agora oferece suporte ao armazenamento quente, um nível de armazenam ento totalmente gerenciado que facilita para os clientes armazenar e acessar dados industriais com segurança.	15 de novembro de 2023
Foi adicionado suporte para identificadores exclusivos definidos pelo usuário	AWS IoT SiteWise agora suporta o uso de identific adores exclusivos definidos pelo usuário para ativos, modelos de ativos, proprieda des e hierarquias.	15 de novembro de 2023
Suporte adicional para detecção de anomalias multivariadas de ativos industriais	AWS IoT SiteWise agora oferece suporte à detecção multivariada de anomalias de ativos industriais por meio da integração de dados históricos e em tempo real do	15 de novembro de 2023

	equipamento com o Amazon Lookout for Equipment.	
Suporte adicional para ingestão econômica e escalável de dados de séries temporais em AWS IoT SiteWise	AWS IoT SiteWise agora oferece suporte à ingestão econômica e escalável de dados de séries temporais necessários para casos de uso analíticos.	15 de novembro de 2023
Suporte adicionado para importação, exportação e atualização em massa	AWS IoT SiteWise agora suporta importação, exportação e atualização em massa de metadados de equipamentos industriais.	15 de novembro de 2023
Suporte adicionado para componentes do modelo de ativos	AWS IoT SiteWise agora oferece suporte a componentes do modelo de ativos para ajudar clientes industriais a criar componentes reutilizáveis.	15 de novembro de 2023
Suporte adicionado para o aplicativo de painel de IoT	AWS IoT SiteWise agora oferece suporte a um aplicativo de painel de controle de código aberto no qual você pode visualizar e interagir com dados operacionais.	15 de novembro de 2023
Atualizou as funções vinculadas ao serviço para AWS IoT SiteWise	AWS IoT SiteWise tem novas funções vinculadas ao serviço e pode executar uma consulta de pesquisa de metadados no banco de dados. AWS IoT TwinMaker	6 de novembro de 2023

Marcação atualizada para recursos de fluxo AWS IoT SiteWise de dados	Suporte adicionado para marcar recursos de fluxo de dados.	18 de agosto de 2022
Gateways SiteWise Edge atualizados	Agora você pode configurar o publicador para controlar quais dados são enviados da borda para a nuvem, bem como a ordem na qual são enviados.	12 de janeiro de 2022
Atualizou a AWS IoT SiteWise demonstração	Agora você pode usar a demonstração para criar um portal do SiteWise Monitor.	10 de janeiro de 2022
Gerenciamento de armazenamento atualizado	Agora você pode definir um período de retenção para controlar por quanto tempo seus dados serão mantidos na camada online atualizada.	29 de novembro de 2021
Adição do suporte para gerenciamento de fluxo de dados	Agora você pode ingerir dados AWS IoT SiteWise antes de criar modelos e ativos de ativos.	24 de novembro de 2021
Hierarquias de modelos de ativos atualizadas	Agora, um modelo de ativo secundário pode ser associado a vários modelos de ativos principais.	28 de outubro de 2021
Lançamento regional	Lançado AWS IoT SiteWise em AWS GovCloud (Oeste dos EUA).	29 de setembro de 2021

Funções atualizadas	Os seguintes atributos foram adicionados • Nas métricas, você pode usar expressões aninhadas em funções de agregação e funções temporais. • Nas transformações, você pode usar a função pretrigger() para recuperar o valor de uma variável anterior à atualização da propriedade que acionou o cálculo da transformação atual.	10 de agosto de 2021
Intervalo de tempo de métrica personalizado	Suporte adicional para intervalos de tempo personalizados e compensações nas métricas.	3 de agosto de 2021
Usando AWS IoT SiteWise na borda	O atributo de processamento de bordas agora está disponível ao público em geral.	29 de julho de 2021
Exportando dados para o Amazon S3	AWS IoT SiteWise agora pode exportar dados para o Amazon S3.	27 de julho de 2021
Endpoints da VPC (AWS PrivateLink)	O endpoint da VPC da interface para as operações da API do ambiente de gerenciamento agora está disponível ao público em geral.	15 de julho de 2021

Transformações	As transformações agora podem inserir múltiplas variáveis de propriedade do ativo.	8 de julho de 2021
Atualização da função time stamp()	Nas transformações, você agora pode fornecer uma variável como argumento para a função `timestamp()` .	16 de junho de 2021
Disponibilidade geral de alarmes	Os atributos de alarme agora estão disponíveis ao público.	27 de maio de 2021
Lançamento do Modbus-TCP Protocol Adapter versão 2	A versão 2 do conector do Modbus-TCP Protocol Adapter está disponível. Esta versão incluiu suporte para cadeias de caracteres de origem codificadas em ASCII, UTF8 e ISO8859.	24 de maio de 2021
Service Quotas atualizadas	Foram adicionadas as seguintes cotas para a GetInterpolatedAssetPropertyValuesAPI: taxa de `GetInterpolatedAssetPropertyValues` solicitações, número de resultados por `GetInterpolatedAssetPropertyValues` solicitação e número de dias entre a data de início no passado e hoje para`GetInterpolatedAssetPropertyValues` .	29 de abril de 2021

Expressões de fórmula atualizadas	Adição dos seguintes operadores e funções: • Adição dos seguintes operadores: `<`, `>`, `<=`, `>=`, `==`, `!=`, `!`, `and`, `or` e `not`. • Adição da seguinte função de comparação: `neq(x, y)`. • Adição das seguintes funções string: `join()`, `format()` e `f''`.	22 de abril de 2021
Endpoints da VPC (AWS PrivateLink)	Foram adicionadas informaçõ es sobre como estabelecer uma conexão privada entre sua nuvem privada virtual (VPC) e as APIs do plano de AWS IoT SiteWise controle criando uma interface VPC endpoint.	16 de março de 2021
Federação do IAM	Os administradores e usuários do portal SiteWise Monitor agora podem fazer login nos portais atribuídos com suas credenciais do IAM.	16 de março de 2021
Lançamento regional	Lançado AWS IoT SiteWise na China (Pequim).	3 de fevereiro de 2021

Lançado o SiteWise conector IoT versão 10	A versão 10 do SiteWise conector IoT está disponível. Essa versão configura `StreamManager` para melhorar o manuseio quando a conexão de origem for perdida e restabelecida. Essa versão também aceita valores OPC-UA com um `ServerTimestamp` quando nenhum `SourceTimestamp` estiver disponível.	22 de janeiro de 2021
Funções de data e hora	AWS IoT SiteWise agora suporta funções de data e hora.	21 de janeiro de 2021
Sintaxe de funções	Agora você pode usar a Sintaxe Uniforme de Chamada de Função (UFCS) para AWS IoT SiteWise funções.	11 de janeiro de 2021
Integração com o Grafana	Foram adicionadas informações sobre como visualizar AWS IoT SiteWise dados nos painéis do Grafana.	15 de dezembro de 2020

AWS IoT SiteWise lançamento de recursos	Agora você pode monitorar seus dados com alarmes, processar dados industriais na borda, usar fontes Modbus TCP e Ethernet/IP em seu gateway SiteWise Edge, filtrar dados recebidos com bandas mortas e muito mais. • Foi adicionada a seção Monitorando dados com alarmes para lhe permitir definir, configurar e responder aos alarmes em AWS IoT SiteWise. • Foi adicionada a seção de Processamento de borda para configurar o processamento de seus dados industriais em seus dispositivos de borda. • As seções Modbus TCP e Ethernet/IP foram adicionadas à documentação de origem do gateway Edge. SiteWise • Foi adicionada a seção de destino de origem para personalizar o local para onde você envia seus dados industriais recebidos. • Foi adicionada a seção de filtragem OPC-UA que você pode usar para controlar a frequência e o tipo de dados enviados ao gateway	15 de dezembro de 2020

	SiteWise Edge a partir do servidor local industrial.	
AWS IoT SiteWise agora oferece suporte a CMKs gerenciadas pelo cliente.	AWS IoT SiteWise agora oferece suporte à criptografia com CMKs gerenciadas pelo cliente.	24 de novembro de 2020
Lançado o SiteWise conector IoT versão 8	A versão 8 do SiteWise conector IoT está disponíve l. Esta versão melhora a estabilidade quando o conector vivencia conectivi dade de rede intermitente.	19 de novembro de 2020
Uso de strings e condicionais em expressões de fórmula	Foram adicionadas informaçõ es sobre como usar strings e funções condicionais em expressões de fórmula para transformações e métricas.	16 de novembro de 2020
Ingestão de dados usando o gerenciador de AWS IoT Greengrass streams	Foram adicionadas informaçõ es sobre como ingerir dados de IoT de alto volume de fontes de dados locais usando um dispositivo de ponta. AWS IoT Greengrass	16 de setembro de 2020
Endpoints da VPC (AWS PrivateLink)	Foram adicionadas informaçõ es sobre como estabelecer uma conexão privada entre sua nuvem privada virtual (VPC) e as APIs de AWS IoT SiteWise dados criando uma interface VPC endpoint.	4 de setembro de 2020

Lançado o SiteWise conector IoT versão 7	A versão 7 do SiteWise conector IoT está disponíve l. Esta versão corrige um problema com as métricas do SiteWise Edge Gateway.	14 de agosto de 2020
Criação de usuários do IAM Identity Center a partir do AWS IoT SiteWise console	Foram adicionadas informaçõ es sobre como você pode criar usuários do IAM Identity Center no AWS IoT SiteWise console. Agora você pode criar usuários do IAM Identity Center ao atribuir usuários a um portal novo ou existente . Atualização do tutorial Visualizando e compartilhando dados de parques eólicos para uso desse atributo. Essa alteração reduz o número de etapas no tutorial.	4 de agosto de 2020
Solução de problemas aprimorada do gateway SiteWise Edge	Foram adicionadas informaçõ es adicionais sobre como solucionar problemas em um gateway SiteWise Edge e como exportar o certificado do cliente OPC-UA para uma fonte.	18 de junho de 2020

Documentação de tarefas do console	Adicionada a documentação de tarefas do console para Modelar ativos industriais, Consultar dados de propriedades de ativos e Interagir com outros serviços. Você pode seguir estas instruções para concluir tarefas no console do AWS IoT SiteWise .	11 de junho de 2020
Analisando o tutorial de dados exportados	Foi adicionado um tutorial que você pode seguir para aprender a usar o Amazon Athena para analisar dados de ativos que você exportou para o S3 com o modelo de recurso de exportação. AWS CloudFormation	27 de maio de 2020
Aprimorado por meio de uso de expressões de fórmula	Foram adicionadas informações detalhadas sobre o comportamento das propriedades da AWS IoT SiteWise fórmula e um exemplo de como contar pontos de dados filtrados.	18 de maio de 2020

Lançado o SiteWise conector IoT versão 6	A versão 6 do SiteWise conector IoT está disponível. Esta versão adiciona suporte para CloudWatch métricas e descoberta automática de novas tags OPC-UA. Isso significa que você não precisa reiniciar seu gateway SiteWise Edge quando as tags mudam para suas fontes OPC-UA. Essa versão do conector requer o gerenciador de streams e o software AWS IoT Greengrass Core v1.10.0 ou superior.	29 de abril de 2020

AWS IoT SiteWise lançamento de recursos	AWS IoT SiteWise lançamento de recursos. Agora você pode gerenciar os gateways do SiteWise Edge com a API, adicionar seu logotipo aos portais, visualizar as métricas do gateway do SiteWise Edge e muito mais. • Foi adicionada a seção Exportação de dados para o Amazon S3 com AWS CloudFormation um modelo que você pode usar para exportar novos valores de dados para um bucket do S3. • Foi adicionada a seção Configurando fontes de dados, que aprimora a documentação da fonte do gateway SiteWise Edge e inclui as novas APIs do gateway SiteWise Edge. • Foi adicionada a seção Métricas do SiteWise Edge Gateway que descreve as CloudWatch métricas que os gateways do SiteWise Edge publicam. • Foi adicionada a seção Configurando um gateway SiteWise Edge no Amazon EC2 com AWS CloudFormation um modelo que você pode usar para SiteWise	29 de abril de 2020

	configurar rapidamente as dependências do gateway Edge em uma instância do Amazon EC2. • Foi adicionada a seção de funções de serviço do portal que descreve o novo recurso de permissões dos portais SiteWise Monitor. • Foi atualizada a documentação do portal, para perfis de serviço do portal e logotipos do portal. • Foi adicionada a seção Marcando seus AWS IoT SiteWise recursos. • Foi atualizada a seção Criando painéis (CLI) para a nova estrutura de definição de painel. • Foi adicionada a seção Segurança.	
Ingestão de dados de AWS IoT Events	Foram adicionadas informações sobre como ingerir dados de AWS IoT Events quando um evento ocorre.	20 de abril de 2020
Visualizando e compartilhando dados de parques eólicos no tutorial SiteWise Monitor	Foi adicionado um tutorial que você pode seguir para aprender a usar AWS IoT SiteWise Monitor para visualizar e compartilhar dados de ativos.	12 de março de 2020

AWS IoT SiteWise conceitos	Foi adicionado um glossário de AWS IoT SiteWise conceitos que você pode usar para aprender sobre o serviço e seus termos comuns.	5 de março de 2020
Instruções de AWS IoT Greengrass instalação removidas	As instruções de instalação do software AWS IoT Greengras s principal foram removidas do Guia AWS IoT SiteWise do usuário. O Guia do AWS IoT Greengrass desenvolvedor oferece um script de configura ção do dispositivo e instruçõe s para configuração AWS IoT Greengrass em outras plataformas, como Amazon EC2 e Docker.	14 de fevereiro de 2020
Aprimoramento da ingestão de dados usando regras AWS IoT Core	Foram adicionadas informaçõ es detalhadas sobre como usar e como solucionar problemas com a ação da AWS IoT SiteWise regra, que você pode usar para ingerir dados de mensagens MQTT por meio dela. AWS IoT Core	14 de fevereiro de 2020
Lançado o SiteWise conector IoT versão 5	A versão 5 do SiteWise conector IoT está disponíve l. Esta versão corrige um problema de compatibilidade com o software AWS IoT Greengrass Core v1.9.4.	12 de fevereiro de 2020

Lançado o SiteWise conector IoT versão 4	A versão 4 do SiteWise conector IoT está disponível. Essa versão corrige um problema com a reconexão do servidor OPC-UA.	7 de fevereiro de 2020
Modelagem de ativos industriais reestruturada	Reestruturação da seção Atualizando ativos e modelos em vários tópicos dentro de Modelando ativos industriais. • Estados de ativos e modelos • Mapeamento de fluxos de dados industriais para propriedades de ativos • Atualizar valores de atributo • Associar e desassociar ativos • Atualizar ativos e modelos • Excluir ativos e modelos	4 de fevereiro de 2020
Tutorial de ingestão de dados de AWS IoT coisas	Foi adicionado um tutorial que você pode seguir para aprender a configurar uma ação de AWS IoT SiteWise regra para ingerir dados de uma frota de AWS IoT itens nova ou existente.	4 de fevereiro de 2020

Recuperação reestruturada de dados de AWS IoT SiteWise	Reestruturou a seção Recuperação de dados em duas seções de nível superior: Consultar valores e agregados de propriedades de ativos e interagir com outros serviços. AWS	21 de janeiro de 2020
Tutorial de publicação de atualizações de valor de propriedade no Amazon DynamoDB	Adição de um tutorial para saber como usar as notificaç ões de valor de propriedade, a fim de armazenar dados de ativos no DynamoDB.	8 de janeiro de 2020
Usando expressões de fórmula	Adição da referência de expressão de fórmula para organizar as constantes e as funções disponíveis para uso nas propriedades de métrica e de transformação. Reestrutu ração de Propriedades de ativos em tópicos separados, para cada tipo de propriedade.	7 de janeiro de 2020
Usando filtros de nó OPC-UA	Foram adicionadas informaçõ es sobre como usar filtros de nó OPC-UA para melhorar o desempenho do gateway SiteWise Edge ao adicionar fontes do gateway SiteWise Edge.	3 de janeiro de 2020
Atualizando um conector	Foram adicionadas informaçõ es sobre como atualizar um gateway SiteWise Edge quando uma nova versão do conector for lançada.	30 de dezembro de 2019

Lançado o SiteWise conector IoT versão 3	A versão 3 do SiteWise conector IoT está disponíve l. Essa versão remove o requisito de permissões iot:*.	17 de dezembro de 2019
Lançado o SiteWise conector IoT versão 2	A versão 2 do SiteWise conector IoT está disponível. Essa versão adiciona suporte para vários recursos de segredo OPC-UA.	10 de dezembro de 2019
Criando painéis (AWS CLI)	Foram adicionadas informaçõ es sobre como criar um painel AWS IoT SiteWise Monitor usando AWS CLI o.	6 de dezembro de 2019

AWS IoT SiteWise versão 2 lançada	Prévia lançada para a versão 2 do AWS IoT SiteWise. Agora você pode ingerir dados via OPC-UA, MQTT e HTTP, modelar seus dados em hierarquias de ativos e visualizar seus dados com o Monitor. SiteWise • Reformulação da seção modelagem de ativos para alterar ativos, modelos de ativos e hierarquias de ativos. • A seção de ingestão de dados foi atualizada para incluir etapas do AWS IoT Greengrass conector e seções de ingestão de dados sem gateway. • Foi adicionada a AWS IoT SiteWise Monitorseção e um guia de aplicativo separado que mostra como usar o aplicativo web SiteWise Monitor. • Adição das seções Consultar dados de AWS IoT SiteWise e Interagindo com outros serviços AWS. • Reformulação da seção conceitos básicos para corresponder à experiência de demonstração atualizad a.	2 de dezembro de 2019

AWS IoT SiteWise versão 1 lançada	Lançada prévia inicial para a versão 1 do AWS IoT SiteWise.	25 de fevereiro de 2019

Glossário do AWS

Para obter a terminologia mais recente da AWS, consulte o glossário da AWS na Referência do Glossário da AWS.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.