



Guia do usuário

AWS IoT SiteWise



AWS IoT SiteWise: Guia do usuário

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestige a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

O que AWS IoT SiteWise é	1
Como AWS IoT SiteWise funciona	2
Ingerir dados industriais	2
Modelar ativos para contextualizar dados coletados	3
Analisar usando consultas, alarmes e previsões	4
Visualizar operações	4
Armazenamento de dados	5
Integração com outros serviços da	5
Casos de uso para AWS IoT SiteWise	5
Fabricação	6
Alimentos e bebidas	6
Energia e serviços de utilidade pública	6
Trabalhando com AWS SDKs	6
Conceitos	8
Conceitos básicos	14
Requisitos	14
Configurar uma AWS conta	15
Inscreva-se para um Conta da AWS	15
Criar um usuário com acesso administrativo	15
Usar a demonstração de início rápido	18
Crie a AWS IoT SiteWise demonstração	18
Exclua a AWS IoT SiteWise demonstração	20
Tutoriais	22
Calcular OEE	22
Pré-requisitos	22
Como calcular a OEE	23
Ingerir dados	25
Pré-requisitos	27
Etapa 1: criar uma AWS IoT política	27
Etapa 2: criar qualquer AWS IoT coisa	29
Etapa 3: criar um modelo de ativo do dispositivo	31
Etapa 4: criar um modelo de ativo da frota de dispositivos	33
Etapa 5: criar e configurar um ativo de dispositivo	35
Etapa 6: criar e configurar um ativo de frota de dispositivos	35

Etapa 7: criar uma regra no AWS IoT Core para enviar dados aos ativos do dispositivo	36
Etapa 8: executar o script de cliente do dispositivo	40
Etapa 9: limpar os recursos após o tutorial	47
Visualize e compartilhe dados no Monitor SiteWise	48
Pré-requisitos	49
Etapa 1: Criar um portal no SiteWise Monitor	50
Etapa 2: fazer login em um portal	54
Etapa 3: criar um projeto de parque eólico	56
Etapa 4: criar um painel para visualizar dados do parque eólico	60
Etapa 5: explorar o portal	67
Etapa 6: limpar os recursos após o tutorial	68
Publicar no Amazon DynamoDB	71
Pré-requisitos	71
Etapa 1: Configurar AWS IoT SiteWise para publicar atualizações de valores de propriedades	72
Etapa 2: criar uma regra no AWS IoT Core	74
Etapa 3: criar uma tabela do DynamoDB	77
Etapa 4: configurar a ação de regra do DynamoDB	79
Etapa 5: explorar os dados no DynamoDB	80
Etapa 6: limpar os recursos após o tutorial	81
Ingerir dados para AWS IoT SiteWise	85
Gerenciar streams de dados	86
Definir permissões e configurações	87
Associar um fluxo de dados a uma propriedade do ativo	88
Desassociar um fluxo de dados de uma propriedade do ativo	89
Criar um fluxo de dados	90
Atualizar um alias de propriedade do ativo	91
Cenários comuns	92
Ingira dados com AWS IoT SiteWise APIs	95
BatchPutAssetPropertyValue API	95
CreateBulkImportJob API	98
AWS IoT Core Regras de uso	106
Conceder o acesso necessário	107
Configurar a ação de regra	108
Reduzir custos com a ingestão básica	117
Use AWS IoT Events ações	118

Use o gerenciador de AWS IoT Greengrass streams	119
Use gateways SiteWise Edge	120
Conceitos principais do Gateway	120
Benefícios da implementação do SiteWise Edge	121
Hospede automaticamente um gateway	122
Requisitos	123
Criar um gateway	128
Instale o software de gateway	131
Gateways V3 habilitados para MQTT	134
Streams clássicos, gateways V2	191
Adicionar fontes de dados	205
Componentes para SiteWise Edge	249
Filtrar ativos do	250
Suporte de proxy e lojas fiduciárias	252
Use APIs	258
Hospedar um gateway no Siemens Industrial Edge	276
Segurança	277
Siemens Secure Storage e o aplicativo AWS IoT SiteWise Edge	277
Destinos para Siemens Industrial Edge dispositivos	278
Migrar da aplicação de pré-visualização	280
Solução de problemas	281
AWS IoT SiteWise Registro de alterações do aplicativo Edge	281
Requisitos	282
Criar um gateway	283
Criar uma Siemens Databus user	284
Acessar a aplicação	285
Instalar a aplicação	286
Atualizar a configuração de uma aplicação instalada	288
Destinos e filtros de caminho	289
Entenda os destinos	290
Entenda os filtros de caminho	293
Adicione um destino em tempo real	297
Adicione um destino em buffer usando o Amazon S3	305
Adicionar filtros de caminho	312
Gerenciar destinos	316
Gerenciar gateways	322

Gerencie seu gateway SiteWise Edge com o AWS IoT SiteWise console	323
Gerencie gateways SiteWise Edge usando AWS OpsHub para AWS IoT SiteWise	323
Acesse seu gateway SiteWise Edge usando as credenciais do sistema operacional local ...	325
Gerenciar o certificado de gateway SiteWise Edge	328
Alterar a versão dos pacotes de componentes do SiteWise Edge Gateway	328
Listar gateways SiteWise Edge	329
Descreva um gateway SiteWise Edge	330
Crie um gateway SiteWise Edge	330
Atualizar um gateway SiteWise Edge	331
Atualizar a configuração da capacidade do gateway	332
Tag: recursos do gateway	334
Listar tags para um gateway	335
Remover tags de um gateway	336
Atualizar a versão de um AWS IoT SiteWise componente	336
Excluir um gateway SiteWise Edge	337
Backup e restauração de gateways	339
Backups diários de dados métricos	339
Restaurar um gateway SiteWise Edge	340
Restaurar AWS IoT SiteWise dados	340
Valide backups e restaurações bem-sucedidos	341
Gateways legados (AWS IoT Greengrass Version 1)	342
Modelar ativos industriais	344
Estados de ativos e modelos	346
Verificar o status de um ativo	346
Verificar o status de um modelo de ativo ou de componente	348
Versões do modelo de ativo	350
Recuperar a versão ativa de um modelo de ativo ou modelo de componente (console)	351
Recuperar a versão ativa de um modelo de ativo ou modelo de componente (AWS CLI)	352
Modelos compostos personalizados (componentes)	353
Modelos compostos personalizados em linha	354
Component-model-based modelos compostos personalizados	356
Usar caminhos para fazer referência a propriedades do modelo composto personalizado ...	357
Configurar objeto IDs	359
Trabalhar com objeto UUIDs	360
Use externo IDs	360
Criar modelos do	362

Criar modelos de ativos em AWS IoT SiteWise	363
Criar modelos de componente	378
Definir propriedades de dados	382
Criar modelos compostos personalizados (componentes)	465
Criar ativos	469
Criar um ativo (console)	470
Criar um ativo (AWS CLI)	471
Configurar um novo ativo	472
Pesquisar ativos do	473
Pré-requisitos	473
Pesquisa avançada em Console do AWS IoT SiteWise	473
Atualizar valores de atributo	476
Associar e desassociar ativos	479
Associar e desassociar ativos (console)	480
Associar e desassociar ativos (AWS CLI)	481
Atualizar ativos e modelos	483
Atualizar ativos em AWS IoT SiteWise	483
Atualizar modelos de ativo e modelos de componente	485
Atualizar modelos compostos personalizados (componentes)	491
Bloqueio positivo para gravações do modelo de ativo	494
Excluir ativos e modelos em AWS IoT SiteWise	498
Excluir ativos	498
Excluir modelos de ativo	501
Operações em massa com ativos e modelos	503
Principais conceitos e terminologia	503
Funções compatíveis	504
Pré-requisitos das operações em massa	505
Executar um trabalho de importação em massa	508
Executar um trabalho de exportação em massa	510
Acompanhamento do progresso dos trabalhos e tratamento de erros	513
Exemplos de importação de metadados	519
Exemplos de exportação de metadados	535
Esquema do trabalho de transferência de metadados	537
Monitorar dados com alarmes	556
Tipos de alarmes	556
Estados de alarme	558

Propriedades do estado do alarme	559
Definir alarmes em modelos de ativo	562
Requisitos para notificações de alarmes	565
Definir AWS IoT Events alarmes	566
Definir alarmes externos	601
Configurar alarmes em ativos	603
Configurar um valor limite (console)	603
Configurar um valor limite (AWS CLI)	604
Definir configurações de notificação	606
Responder a alarmes	609
Responder a um alarme (console)	609
Responder a um alarme (API)	613
Ingerir um estado de alarme externo	613
Mapear fluxos de estado de alarme externo	614
Ingerir dados de estado do alarme	616
AWS IoT SiteWise Assistente	618
Configurar o AWS IoT SiteWise Assistente	618
Criar um conjunto de dados	620
Editar um conjunto de dados	625
Excluir um conjunto de dados	627
AWS IoT SiteWise Perguntas do assistente	628
Monitore dados com AWS IoT SiteWise Monitor	629
SiteWise Monitore as funções	630
Federação do SAML	632
SiteWise Conceitos de monitoramento	633
Comece com AWS IoT SiteWise Monitor (Classic)	635
Criar um portal	636
Configurar o portal do	637
Convidar administradores	641
Adicionar usuários ao portal	644
Criar painéis (CLI)	648
Ativar alarmes para os portais	654
Habilitar o portal na borda	657
Administrar portais	657
Comece com AWS IoT SiteWise Monitor (com reconhecimento de IA)	667
Criar um portal	669

Configurar o portal do	669
Administrar portais	672
Excluir um portal	676
Crie painéis com AWS CLI	677
Login do portal	682
Criar um projeto	682
Atualizar um projeto	683
Excluir um projeto	684
Criar um painel	684
Atualizar um painel	686
Excluir um painel	686
Configurar painel	687
Consultar dados de AWS IoT SiteWise	708
Consultar valores de ativos atuais	709
Consultar o valor atual de uma propriedade de ativo (console)	709
Consultar o valor atual de uma propriedade de ativo (AWS CLI)	709
Consultar valores históricos de propriedades de ativo	711
Consultar agregados de propriedades de ativo	712
Agregados de uma propriedade de ativo (API)	713
Agregados de uma propriedade de ativo (AWS CLI)	714
AWS IoT SiteWise linguagem de consulta	716
Pré-requisitos	716
Referência da linguagem de consulta	717
Interagir com outros serviços	726
Noções básicas sobre as propriedades de ativo em tópicos MQTT	727
Trabalhar com notificações	727
Ativar notificações de propriedades de ativo (console)	728
Ativar notificações de propriedades de ativo (AWS CLI)	728
Consultar notificações	730
Exportar dados para o Amazon S3	733
Integre a Grafana	734
Integre com AWS IoT TwinMaker	735
Habilitar a integração	736
Integrando e AWS IoT SiteWiseAWS IoT TwinMaker	736
Detectar anomalias de equipamentos	737
Adicionar uma definição de previsão (console)	739

Treinar uma previsão (console)	742
Iniciar ou interromper a inferência em uma previsão (console)	743
Adicionar uma definição de previsão (CLI)	744
Treinar uma previsão e iniciar a inferência (CLI)	747
Treinar uma previsão (CLI)	749
Iniciar ou interromper a inferência em uma previsão (CLI)	750
Gerenciar armazenamento de dados	753
Definir configurações de armazenamento	754
Impacto da retenção de dados	755
Configurar para nível morno (console)	755
Configurar para nível morno (AWS CLI)	757
Configurar para nível frio (console)	760
Configurar para nível frio (AWS CLI)	763
Solucionar problemas em configurações de armazenamento	768
Erro: Bucket não existe	769
Erro: acesso negado ao caminho do Amazon S3	769
Erro: O ARN da função não pode ser presumido	770
Erro: falha ao acessar o bucket do Amazon S3 entre regiões	770
Caminhos de arquivo e esquemas de dados salvos na camada fria	770
Dados do equipamento (medições)	770
Métricas, transformações e agregados	775
Metadados de ativos	779
Metadados de hierarquia de ativos	783
Arquivos de índice de dados de armazenamento	786
Exemplos de código	787
Conceitos básicos	791
Olá AWS IoT SiteWise	792
Conheça os conceitos básicos	796
Ações	859
Segurança	936
Proteção de dados	937
Privacidade do tráfego entre redes	938
AWS IoT SiteWise Melhoria do serviço comercial assistente	938
Criptografia de dados	938
Criptografia inativa	939
Criptografia em trânsito	942

Gerenciamento de chaves	944
Gerenciamento de identidade e acesso	945
Público	946
Autenticar com identidades	946
Como AWS IoT SiteWise funciona com o IAM	950
Políticas gerenciadas	969
Perfis vinculados a serviço	973
Configurar permissões para alarmes	991
Prevenção confusa de delegados entre serviços em AWS IoT SiteWise	997
Solução de problemas de identidade e acesso da	999
Validação de conformidade	1001
Resiliência	1002
Segurança da infraestrutura	1002
Análise de configuração e vulnerabilidade	1003
Endpoints da VPC	1004
Operações de API do compatíveis	1004
Criar um VPC endpoint de interface	1007
Acesso AWS IoT SiteWise por meio de uma interface VPC endpoint	1007
Criar uma política de endpoint da VPC	1009
Práticas recomendadas de segurança	1010
Usar credenciais de autenticação nos servidores OPC UA	1010
Usar modos de comunicação criptografados para os servidores OPC UA	1010
Mantém os componentes atualizados	1011
Criptografe o sistema de arquivos do seu gateway SiteWise Edge	1011
Acesso seguro à sua configuração de borda	1011
Proteger dados no Siemens Industrial Edge Management	1012
Conceda aos usuários do SiteWise Monitor as permissões mínimas possíveis	1012
Não exponha informações confidenciais	1012
Siga as melhores práticas de AWS IoT Greengrass segurança	1013
Consulte também	1013
Registrar e monitorar	1014
Monitorar logs de serviço	1014
Gerenciar o login AWS IoT SiteWise	1016
Exemplo: entradas do arquivo de AWS IoT SiteWise log	1018
Monitore os registros do gateway SiteWise Edge	1018
Use Amazon CloudWatch Logs	1018

Usar logs de serviço	1020
Monitore com CloudWatch métricas da Amazon	1022
AWS IoT Greengrass Version 2 métricas de gateway	1022
Registre chamadas de API com AWS CloudTrail	1032
AWS IoT SiteWise informações em CloudTrail	1033
AWS IoT SiteWise eventos de dados em CloudTrail	1033
AWS IoT SiteWise eventos de gerenciamento em CloudTrail	1036
Exemplo: entradas do arquivo de AWS IoT SiteWise log	1036
Marcar com tag os recursos do	1039
Use tags em AWS IoT SiteWise	1039
Marque com o AWS Management Console	1039
Marque com a AWS IoT SiteWise API	1040
Usar etiquetas com políticas do IAM	1041
Solução de problemas	1043
Solução de problemas de um gateway	1043
Configurar e acessar os registros SiteWise do gateway Edge	1043
Solução de problemas SiteWise do Edge Gateway	1044
Solução de problemas do aplicativo AWS IoT SiteWise Edge em Siemens Industrial Edge	1050
Solução de problemas de integrações de código aberto no Edge	1051
Solução de AWS IoT Greengrass problemas	1054
Solucionar problemas em um portal	1054
Usuários e administradores não podem acessar o portal do AWS IoT SiteWise	1054
Solucionar problemas de uma ação de AWS IoT SiteWise regra	1056
Configurar AWS IoT Core registros	1056
Configurar uma ação de erro na republicação	1057
Solucionar problemas em regras	1059
Solucionar problemas em uma regra (AWS IoT SiteWise)	1061
Solucionar problemas em uma regra (DynamoDB)	1063
Solucionar problemas de importação e exportação em massa	1066
Endpoints e cotas	1068
Endpoints	1068
Cotas	1068
AWS IoT SiteWise Limites de limitação da API Assistant	1087
Cotas para detecção de anomalias	1088
Histórico de documentos	1089
.....	mcxii

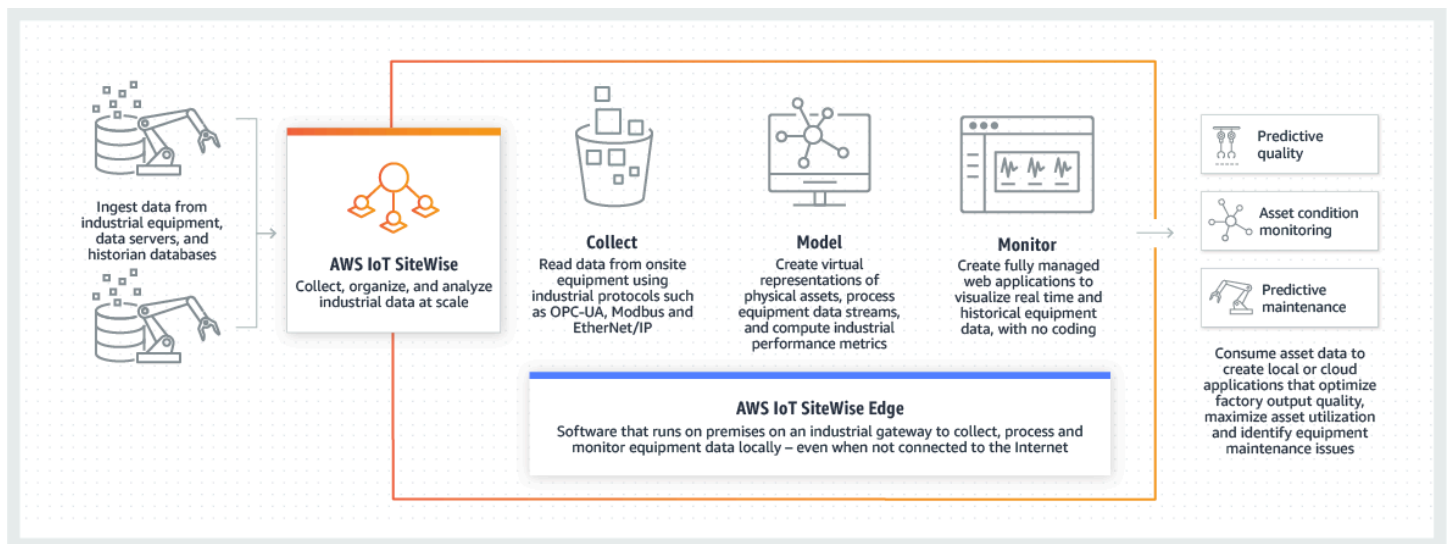
O que AWS IoT SiteWise é

AWS IoT SiteWise é um serviço gerenciado com o qual você pode coletar, armazenar, organizar e monitorar 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.

Com AWS IoT SiteWise Monitor isso, seus usuários operacionais podem criar aplicativos da 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 será útil se você tiver acesso limitado à internet ou precisar manter os dados privados.

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



Tópicos

- [Como AWS IoT SiteWise funciona](#)
- [Casos de uso para AWS IoT SiteWise](#)
- [Usando esse serviço com um AWS SDK](#)
- [AWS IoT SiteWise conceitos](#)

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 modelos de ativo, você define os dados brutos para consumir e como processá-los em métricas úteis. Crie e visualize ativos e modelos da operação industrial no [console do AWS IoT SiteWise](#). Você também pode configurar modelos de ativos para coletar e processar dados na borda ou na AWS nuvem.

Tópicos

- [Ingerir dados industriais](#)
- [Modelar ativos para contextualizar dados coletados](#)
- [Analisar usando consultas, alarmes e previsões](#)
- [Visualizar operações](#)
- [Armazenamento de dados](#)
- [Integração com outros serviços da](#)

Ingerir dados industriais

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

- Ingestão direta de servidores no local: utilize protocolos como o OPC UA para ler dados diretamente de dispositivos no local. 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 obter mais informações, consulte [AWS IoT SiteWise Requisitos de gateway auto-hospedado do Edge](#).

Observe que protocolos como Modbus TCP e Ethernet/IP (EIP) são suportados por meio de nossa parceria com a Domatica no contexto de. 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 obter mais informações, consulte [Configurar uma fonte OPC UA no SiteWise Edge](#).

- Ingestão adaptável via Amazon S3 com operações em massa: ao trabalhar com grandes quantidades de ativos ou modelos de ativo, use operações em massa para importar e exportar recursos em massa dos buckets do Amazon S3. Para obter 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 obter mais informações, consulte [Ingerir dados para AWS IoT SiteWise usar 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 obter mais informações, consulte [Ingira dados de AWS IoT SiteWise AWS IoT Events](#).
- AWS IoT SiteWise API: Seus aplicativos no Edge ou na nuvem podem enviar dados diretamente para AWS IoT SiteWise. Para obter mais informações, consulte [Ingira dados com AWS IoT SiteWise APIs](#).

Modelar ativos para contextualizar dados coletados

Depois de ingerir dados, você poderá usá-los para criar representações virtuais dos ativos, processos e instalações, criando modelos das 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 filhos associados. Os ativos são criados com base em modelos de ativo. Os modelos de ativo são estruturas declarativas que padronizam os formatos de ativo. Reutilize componentes de ativos para organização e manutenção dos modelos. Para obter mais informações, consulte [Modelar ativos industriais](#).

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

- As transformações funcionam durante o recebimento de dados de equipamentos.

- As métricas são calculadas em intervalos definidos por você.

As métricas e as transformações são aplicáveis a ativos individuais ou vários ativos. O AWS IoT SiteWise calcula automaticamente agregados estatísticos muito usados, como média, soma e contagem, em vários períodos relevantes para os dados, as métricas e as transformações dos equipamentos.

Os ativos podem ser sincronizados usando AWS IoT TwinMaker. Para obter mais informações, consulte [Integrando e AWS IoT SiteWiseAWS IoT TwinMaker](#).

Analisar 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 as causas principais.

- Defina alarmes específicos para alertar a equipe quando houver desvio de desempenho dos equipamentos ou processos, garantindo a rápida identificação e resolução dos problemas. Para obter mais informações, consulte [Monitore dados com alarmes em AWS IoT SiteWise](#).
- 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 obter 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 nos equipamentos ou nas condições operacionais. Com a detecção de anomalias, você pode determinar medidas de manutenção preventiva para as operações. Essa integração permite que os clientes sincronizem dados entre o AWS IoT SiteWise e o Amazon Lookout for Equipment. Para obter mais informações, consulte [Detectar anomalias com o Lookout for Equipment](#).

Visualizar operações

Configure o SiteWise Monitor para criar aplicativos web para seus funcionários operacionais. Os aplicativos web ajudam os funcionários a visualizar as operações. Processe níveis variados de acesso para os funcionários usando o Centro de Identidade do IAM 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 ter mais informações sobre como visualizar as operações, consulte [Monitore 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 quente que é otimizado para aplicações em tempo real.
- Um nível de armazenamento morno que é otimizado para workloads analíticas.
- Um nível de armazenamento frio gerenciado pelo cliente usando o Amazon S3 para aplicações 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. Depois, defina políticas de retenção de dados para mover dados históricos para o armazenamento de nível morno ou frio. Para obter mais informações, consulte [Gerencie o armazenamento de dados em AWS IoT SiteWise](#).

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 obter mais informações, consulte [Interaja com outros AWS serviços](#).

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 consistentemente 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 das 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 e contam com operadores de fábrica e de equipamentos em um local central para monitorar os processos e equipamentos. Por exemplo, as unidades de refrigeração avaliam o manuseio e a validade dos ingredientes. Elas monitoram a criação de resíduos nas 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 dos equipamentos de qualquer lugar para identificar possíveis problemas, enviar recursos precisos e impedir e corrigir problemas com mais rapidez.

Usando esse serviço com um AWS SDK

AWS kits de desenvolvimento de software (SDKs) estão disponíveis para muitas linguagens de programação populares. Cada SDK fornece uma API, exemplos de código e documentação que permitem que os desenvolvedores criem facilmente aplicações em seu idioma de preferência.

Documentação do SDK	Exemplos de código
AWS SDK para C++	AWS SDK para C++ exemplos de código
AWS CLI	AWS CLI exemplos de código
AWS SDK para Go	AWS SDK para Go exemplos de código
AWS SDK para Java	AWS SDK para Java exemplos de código
AWS SDK para JavaScript	AWS SDK para JavaScript exemplos de código
AWS SDK para Kotlin	AWS SDK para Kotlin exemplos de código
AWS SDK para .NET	AWS SDK para .NET exemplos de código
AWS SDK para PHP	AWS SDK para PHP exemplos de código
Ferramentas da AWS para PowerShell	Ferramentas da AWS para PowerShell exemplos de código
AWS SDK para Python (Boto3)	AWS SDK para Python (Boto3) exemplos de código
AWS SDK para Ruby	AWS SDK para Ruby exemplos de código
AWS SDK para Rust	AWS SDK para Rust exemplos de código
SDK da AWS para SAP ABAP	SDK da AWS para SAP ABAP exemplos de código
AWS SDK for Swift	AWS SDK for Swift exemplos de código

Exemplo de disponibilidade

Não consegue encontrar o que precisa? Solicite um exemplo de código usando o link [Fornecer feedback](#) na parte inferior desta página.

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 obter mais informações, consulte [Consulte agregados de propriedades de ativos em AWS IoT SiteWise](#).

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, um modelo e uma data de instalação. Ele também pode ter valores de séries temporais para disponibilidade, desempenho, qualidade, temperatura, pressão e assim por diante. Agrupe os ativos em hierarquias, permitindo que os ativos acessem os dados armazenados nos respectivos ativos filhos. Para obter mais informações, consulte [Modelar ativos industriais](#).

Hierarquia de ativos

Defina hierarquias de ativos para criar representações lógicas das operações industriais. Para fazer isso, defina uma hierarquia em um modelo de ativo e associe os ativos criados com base nesse modelo à hierarquia especificada. As métricas nos ativos pais podem combinar dados das propriedades dos ativos filhos, permitindo que você calcule métricas que oferecem informações sobre a operação geral ou sobre uma parte específica dela. Para obter mais informações, consulte [Definir hierarquias de modelos de ativo](#).

Modelo de ativo

Cada ativo é criado usando um modelo de ativo. Os modelos de ativo são estruturas que definem e padronizam o formato dos ativos. Eles garantem informações consistentes em vários ativos do mesmo tipo, para que você possa processar dados nos ativos que representem 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 obter mais informações, consulte [Modelar ativos industriais](#).

Decida onde as propriedades de um modelo de ativo serão processadas configurando o modelo de ativo para a borda. Utilize esse recurso para processar e monitorar dados de ativos nos dispositivos locais.

Propriedade de ativo

As propriedades do ativo são estruturas em 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 obter mais informações, consulte [Definir propriedades de dados](#).

Configure as propriedades de ativo para computação na borda. Para obter mais informações sobre o processamento de dados na borda, consulte [Configurar uma fonte OPC UA no SiteWise Edge](#).

Atributo

Os atributos são propriedades de um ativo que normalmente permanecem constantes, como o fabricante ou a localização do dispositivo. Os atributos podem ter valores predefinidos. Cada ativo criado com base em um modelo de ativo inclui os valores padrão dos atributos definidos nesse modelo. Para obter mais informações, consulte [Definir 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. Ao observar os painéis, os visualizadores podem personalizar o intervalo de tempo para analisar dados específicos.

Conjunto de dados

Os conjuntos de dados são coleções de dados que representam dados de séries temporais, dados e non-time-series dados não relacionados ao equipamento, como horários de turnos, registros de manutenção e bancos de dados de funcionários. Eles oferecem suporte a dados externos e usam recursos AWS IoT SiteWise analíticos. Ele inclui fontes do conjunto de dados, esquema do conjunto de dados e parâmetros do conjunto de dados. O AWS IoT SiteWise Assistant usa conjuntos de dados que consomem índices do Amazon Kendra.

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 obter mais informações, consulte [Gerencie fluxos de dados para AWS IoT SiteWise](#).

Destinos

Os destinos no SiteWise Edge representam os endpoints para os quais você deseja enviar sua telemetria ou dados processados. SiteWise O Edge oferece suporte ao AWS IoT SiteWise hot tier, à ingestão em buffer ou a um bucket do Amazon S3 como destinos. Você pode configurar destinos para assinar tópicos específicos do MQTT usando filtros de caminho. Para obter mais informações, consulte [AWS IoT SiteWise Entenda os destinos Edge](#).

Fórmula

Cada propriedade de [transformação](#) e [métrica](#) tem uma fórmula que define como essa propriedade transforma ou agrega os dados. Essas fórmulas incluem entradas de propriedade, operadores e funções oferecidas pelo AWS IoT SiteWise. Para obter mais informações, consulte [Usar expressões de fórmula](#).

Medição

As medições são propriedades de ativo que representam fluxos de dados de séries temporais brutos dos sensores de um dispositivo ou equipamento. Para obter mais informações, consulte [Definir fluxos de dados de equipamentos \(medições\)](#).

Métrica

As métricas são propriedades de um ativo que representam dados de séries temporais agregados. Cada métrica é acompanhada de 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 obter mais informações, consulte [Agregar dados de propriedades e outros ativos \(métricas\)](#).

MQTT

O MQTT (Message Queuing Telemetry Transport) é um protocolo de mensagens leve para sensores e dispositivos.

Pacotes

SiteWise Os gateways Edge usam pacotes para determinar como coletar, processar e rotear dados. Para obter mais informações sobre os pacotes disponíveis para seu gateway SiteWise Edge, consulte [the 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.

Pacote de processamento de dados

Use o pacote de processamento de dados para processar, armazenar e recuperar seus dados na borda por até 30 dias. Troque dados processados na borda de e para aplicativos locais por meio SiteWise do Edge. APIs

OPC UA

O OPC UA (Open Platform Communications Unified Architecture) é um protocolo de comunicação para automação industrial.

Filtros de caminho

Use filtros de caminho em um gateway para assinar tópicos do MQTT e publicar em destinos AWS IoT SiteWise compatíveis. Fontes, pipelines de processamento de dados e destinos baseados em MQTT trocam dados usando tópicos do MQTT em um gateway V3 auto-hospedado e habilitado para MQTT. Você pode definir filtros de tópicos para especificar os dados que deseja ingerir ou rotear para destinos diferentes.

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 de projeto só podem visualizar painéis nos projetos aos quais possuem 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 obter mais informações, consulte [Gerencie fluxos de dados para AWS IoT SiteWise](#).

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 obter mais informações, consulte [Interaja com outros AWS serviços](#).

SiteWise Gateway Edge

Um gateway SiteWise Edge é instalado nas instalações do cliente para coletar, manipular e direcionar dados. Um gateway SiteWise Edge se conecta às suas fontes de dados industriais por meio de vários protocolos 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. Para obter mais informações, consulte [Use gateways AWS IoT SiteWise Edge](#).

Transformação

As transformações são propriedades de um ativo que representam dados de séries temporais transformados. Cada transformação é acompanhada de uma expressão matemática ([fórmula](#)) que define como converter pontos de dados de uma forma para outra. Os pontos de dados transformados mantêm uma one-to-one relação com os pontos de dados de entrada. Para obter mais informações, consulte [Transformar 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 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.

Comece 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 obter mais informações, consulte [Use a AWS IoT SiteWise demonstração](#).

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

- [Ingira dados para AWS IoT SiteWise extrair coisas AWS IoT](#)
- [Visualize e compartilhe dados de parques eólicos no Monitor SiteWise](#)
- [Publicar atualizações de valores de propriedade no Amazon DynamoDB](#)

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

- [Ingerir dados para AWS IoT SiteWise](#)
- [Modelar ativos industriais](#)
- [Configure os recursos de borda no AWS IoT SiteWise Edge](#)
- [Monitore dados com AWS IoT SiteWise Monitor](#)
- [Consultar dados de AWS IoT SiteWise](#)
- [Interaja com outros AWS serviços](#)

Tópicos

- [Requisitos](#)
- [Configurar uma AWS conta](#)

Requisitos

Você deve ter uma AWS conta para começar AWS IoT SiteWise. Se ainda não tiver uma, consulte a seção a seguir para conferir instruções sobre como configurar uma conta.

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

Configurar uma AWS conta

Tópicos

- [Inscreva-se para um Conta da AWS](#)
- [Criar um usuário com acesso administrativo](#)

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 a <https://portal.aws.amazon.com/billing/inscrição>.
2. Siga as instruções online.

Parte do procedimento de inscrição envolve receber uma chamada telefônica ou uma mensagem de texto e inserir um código de verificação pelo teclado do telefone.

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

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando <https://aws.amazon.com/e> escolhendo 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 Console](#) como proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.

Para obter ajuda ao fazer login usando o usuário-raiz, consulte [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. Habilita o Centro de Identidade do IAM.

Para obter instruções, consulte [Habilitar o AWS IAM Identity Center](#) no Guia do usuário do AWS IAM Identity Center .

2. No Centro de Identidade do IAM, conceda o acesso administrativo a 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 o seu usuário do Centro de Identidade do IAM, use o URL de login enviado ao seu endereço de e-mail quando o usuário do Centro de Identidade do IAM foi criado.

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 a 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 [Criar um conjunto de permissões](#) 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 [Adicionar grupos](#) no Guia do usuário do AWS IAM Identity Center .

Use 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

Assim que criar a demonstração, você vai começar a receber cobrança pelos recursos que essa demonstração cria e consome.

Tópicos

- [Crie a AWS IoT SiteWise demonstração](#)
- [Exclua a AWS IoT SiteWise demonstração](#)

Crie 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. Talvez você veja esses recursos em sua AWS conta. 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 TSiteWiseDemoAssetslo 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](#).

Exclua a AWS IoT SiteWise demonstração

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 IoTSiteWiseDemoAssetsda 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 necessários 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 foram projetados para ambientes de teste e usam nomes fictícios para empresas, modelos, ativos, propriedades e assim por diante. O objetivo é fornecer orientação geral. Os tutoriais não se destinam ao uso direto em um ambiente de produção sem revisão e adaptação cuidadosas para atender às necessidades exclusivas da organização.

Tópicos

- [Calcule o OEE em AWS IoT SiteWise](#)
- [Ingira dados para AWS IoT SiteWise extrair coisas AWS IoT](#)
- [Visualize e compartilhe dados de parques eólicos no Monitor SiteWise](#)
- [Publicar atualizações de valores de propriedade no Amazon DynamoDB](#)

Calcule 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 $\text{Availability} * \text{Quality} * \text{Performance}$. 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 [Ingerir 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 as 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.

Métricas

- `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.

Note

Se a OEE for definida como uma transformação, os valores de saída serão calculados para cada um dos valores de entrada. Existe a possibilidade de gerar valores inesperados, pois a avaliação da transformação leva em consideração os valores mais recentes disponíveis para todas as propriedades contribuintes na fórmula. Para atualizações de propriedades com o mesmo carimbo de data/hora, os valores de saída podem ser substituídos por atualizações de outras propriedades de entrada. Por exemplo, quando a disponibilidade, a qualidade e o desempenho são calculados, a OEE é calculada com os últimos pontos de dados disponíveis para as outras duas propriedades. Esses valores contribuintes compartilham carimbos de data/hora e levam a valores de saída incorretos da OEE. A ordem não é garantida para o cálculo de transformações.

Ingerir dados para AWS IoT SiteWise extrair 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:

- Configurar regras adicionais para fazer streaming de dados para [AWS IoT Events](#), [Amazon DynamoDB](#), and other 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 Guia do desenvolvedor do AWS IoT .

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 obter mais informações, consulte [Ingerir dados para AWS IoT SiteWise usar regras AWS IoT Core](#).

Tópicos

- [Pré-requisitos](#)
- [Etapa 1: criar uma AWS IoT política](#)
- [Etapa 2: criar e configurar uma coisa do AWS IoT](#)
- [Etapa 3: criar um modelo de ativo do dispositivo](#)
- [Etapa 4: criar um modelo de ativo da frota de dispositivos](#)
- [Etapa 5: criar e configurar um ativo de dispositivo](#)
- [Etapa 6: criar e configurar um ativo de frota de dispositivos](#)
- [Etapa 7: criar uma regra no AWS IoT Core para enviar dados aos ativos do dispositivo](#)
- [Etapa 8: executar o script de cliente do dispositivo](#)
- [Etapa 9: limpar os recursos após o tutorial](#)

Pré-requisitos

Para concluir este tutorial, você precisará do seguinte:

- Uma AWS conta. Se você não tiver uma, consulte [Configurar uma AWS conta](#).
- Um computador de desenvolvimento executando Windows, macOS, 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 o botão Conectar dispositivo 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. *account-id* Substitua *region* e por sua região e ID da conta, como **us-east-1-123456789012** e.

```
{
  "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 ter mais informações sobre as 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 `$aws/things/thing-name/shadow/`. Essa política incorpora uma variável da política de coisas conhecida como `${iot:Connection.Thing.ThingName}`. Essa variável substitui o nome da coisa conectada em cada tópico. A instrução `iot:Connect` define limitações sobre quais dispositivos podem estabelecer conexões, garantindo que a variável da política de coisas só possa substituir nomes que começam 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 Criar.

Etapa 2: criar e configurar 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 avança, lembre-se de que os princípios que 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 Guia do desenvolvedor do AWS IoT .

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 à esquerda, 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, escolha 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 e 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 necessários 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 Concluído.

Agora você registrou AWS IoT alguma coisa no seu computador. Siga uma das seguintes etapas:

- 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.
- Repita 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.
- Repita 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: criar um modelo de ativo do dispositivo

Neste procedimento, você cria um modelo de ativo AWS IoT SiteWise para representar seus dispositivos que transmitem dados de uso da CPU e da memória. Para processar dados em ativos que representam grupos de dispositivos, os modelos de ativo impõem informações consistentes em vários ativos do mesmo tipo. Para obter mais informações, consulte [Modelar 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 obter mais informações, consulte [Definir fluxos de dados de equipamentos \(medições\)](#).

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 obter mais informações, consulte [Agregar 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 obter mais informações, consulte [Usar 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 da frota de dispositivos

Neste procedimento, você cria um modelo de ativo AWS IoT SiteWise para simbolizar sua coleção de dispositivos. Nesse modelo de ativo, estabeleça uma estrutura que permite vincular vários ativos de dispositivo a um ativo abrangente da frota. Depois disso, descreva métricas no modelo de ativo da frota para consolidar dados de todos os ativos de dispositivo conectados. Essa abordagem oferece insights abrangentes sobre o desempenho coletivo de toda a 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 obter mais informações, consulte [Definir hierarquias de modelos de ativo](#).

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, gere um ativo de dispositivo baseado no modelo de ativo do dispositivo. Depois, defina aliases de propriedade para cada propriedade de medição. Um alias de propriedade é uma string exclusiva que identifica uma propriedade de ativo. Posteriormente, você poderá identificar uma propriedade para upload de dados usando os aliases em vez do ID de ativo e do ID de propriedade. Para obter mais informações, consulte [Gerencie fluxos de dados para AWS IoT SiteWise](#).

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. Escolha 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, crie um ativo de frota de dispositivos com base no modelo de ativo da frota de dispositivos. Depois, vincule os ativos de dispositivo individuais ao ativo da frota. Essa associação

permite que as propriedades de métrica do ativo da frota compilem e analisem dados de vários dispositivos. Esses dados oferecem 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. Escolha 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, estabeleça uma regra no 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 processar a

mensagem de atualização, extrair os valores de propriedade e transmiti-los aos ativos de dispositivo no 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. Escolha 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))}`**.

A entrada identifica de IDs forma exclusiva 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 **`${state.reported.cpu}`**. Em modelos de substituição, use o operador `.` para recuperar um valor de dentro de uma estrutura JSON.
- h. Selecione Add entry (Adicionar entrada) para adicionar uma nova entrada à propriedade de uso de memória e conclua as seguintes etapas novamente para essa propriedade:
- Selecione By property alias (Por alias da propriedade).
 - Em Property alias (Alias da propriedade), insira **`/tutorial/device/${topic(3)}/memory`**.
 - Em ID de entrada - opcional, insira **`${concat(topic(3), "-memory-", floor(state.reported.timestamp))}`**.
 - Em Time in seconds (Tempo em segundos), insira **`${floor(state.reported.timestamp)}`**.
 - Em Offset in nanos - opcional, insira **`${floor((state.reported.timestamp % 1) * 1E9)}`**.
 - Em Data type (Tipo de dados), selecione Double (Duplo).
 - Em Valor, informe **`${state.reported.memory}`**.
 - 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.
 - 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 obter mais informações, consulte [Solucionar problemas em uma regra \(AWS IoT SiteWise\)](#).
8. Escolha Próximo.
9. Revise as configurações do grupo de regras e selecione Criar para criar a regra.

Etapa 8: executar o script de cliente do dispositivo

Neste tutorial, você não usa 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, primeiro é necessário instalar os pacotes Python necessários. Neste procedimento, instale os pacotes Python necessários e execute o script de 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 {}".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.

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

- f. 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 em uma regra \(AWS IoT SiteWise\)](#).

Você concluiu este tutorial. Se quiser explorar visualizações dos dados em tempo real, você poderá configurar um portal no AWS IoT SiteWise Monitor. Para obter mais informações, consulte [Monitore 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 os 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. Escolha 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. Escolha 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 Excluir.
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 ativo hierárquicos, comece excluindo o modelo de ativo pai.

5. Escolha Excluir.
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.

Visualize e compartilhe 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 engloba projetos, oferecendo a flexibilidade de escolher quais dados podem ser acessados em cada projeto.

Depois, especifique as pessoas na organização que podem acessar cada portal. Os usuários fazem login nos portais usando contas do AWS IAM Identity Center para que você possa usar seu armazenamento de identidades existente ou um armazenamento gerenciado pela 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 obter mais informações, consulte [Monitore 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 com a atribuição de permissões para possuir ou visualizar o projeto e os 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](#)
- [Etapa 1: Criar um portal no SiteWise Monitor](#)
- [Etapa 2: fazer login em um portal](#)
- [Etapa 3: criar um projeto de parque eólico](#)
- [Etapa 4: criar um painel para visualizar dados do parque eólico](#)
- [Etapa 5: explorar o portal](#)
- [Etapa 6: limpar os recursos após o tutorial](#)

Pré-requisitos

Para concluir este tutorial, você precisará do seguinte:

- Um Conta da AWS. Se você não tiver uma, consulte [Configurar uma AWS conta](#).
- Um computador de desenvolvimento rodando Windows, macOS, Linux ou Unix para acessar AWS Management Console o. Para obter mais informações, consulte [O que é 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 obter mais informações, consulte [Use 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 em que você e os usuários podem fazer login com contas do AWS IAM Identity Center. Com o Centro de Identidade do IAM, você pode usar o repositório de identidades existente da sua empresa ou criar um gerenciado pela AWS. Os funcionários da sua empresa podem fazer login sem criar Contas da AWS separadas.

Para criar um portal

1. Faça login no [console do AWS IoT SiteWise](#).
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.

AWS IoT SiteWise > Monitor > Portals > Create portal

Step 1
Enable SSO

Step 2
Portal configuration

Step 3
Invite administrators

Step 4
Assign users

Enable AWS Single Sign-On (SSO)

AWS IoT SiteWise Monitor requires SSO to create a portal and invite users. Create your first user below to enable AWS Single-Sign On. Later in this process, you'll have the opportunity to create other users by using the AWS SSO console. [Learn more](#)

Create a user

Email address

First name

Last name

Upon creation this application will enable AWS Organizations and Single Sign-On. [Learn more](#)

[Cancel](#) [Create user](#)

- 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.

The screenshot shows the 'Invite administrators' page in the AWS IoT SiteWise console. The breadcrumb trail is 'AWS IoT SiteWise > Monitor > Portals > Create portal'. The left sidebar shows three steps: 'Step 1: Portal configuration', 'Step 2: Invite administrators' (which is the active step), and 'Step 3: Assign users'. The main heading is 'Invite administrators'. Below the heading, there is a description: 'Select the users that you want to be portal administrators. When invited, portal administrators control users' access to the operational data of your Sitewise assets. [Learn more](#)'. A button 'Send invite to selected users' is in the top right. Below this is a section titled 'Users (1)' with a search bar 'Find resources'. A table lists users with columns 'Display name' and 'Email'. The first user, 'John Doe' with email 'john.doe@example.com', has a checked checkbox. Below the table is a section 'Selected users (1)'. At the bottom right, there are 'Cancel' and 'Next' buttons, with the 'Next' button highlighted by a red circle.

- 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.

Create user [X]

Create a new AWS user. You can assign this user access to AWS applications and services

Email address
mary.major@example.com

First name
Mary

Last name
Major

Cancel Create user

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

AWS IoT SiteWise > Monitor > Portals > WindFarmPortal > Assign users

Assign users

Users (3) Create user

	Display name	Email
☐	John Doe	john.doe@example.com
☒	Mary Major	mary.major@example.com
☒	Mateo Jackson	mateo.jackson@example.com

► **Selected users (2)**

Cancel Assign users

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

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

Etapa 2: fazer login 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.

AWS IoT SiteWise > Monitor > Portals

Portals (1) Delete View details Create portal

Your employees can use web portals to access your AWS IoT SiteWise asset data. This lets them analyze your operation and draw insights. You configure who has access to each portal.

	Name	Link	Date last modified	Date created	Status
☐	WindFarmPortal	https://a1b2c3d4-5678-90ab-cdef-1111EXAMPLE.app.iotsitewise.aws	04-28-2020	04-20-2020	Active

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. Verifique seu e-mail para ver 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.

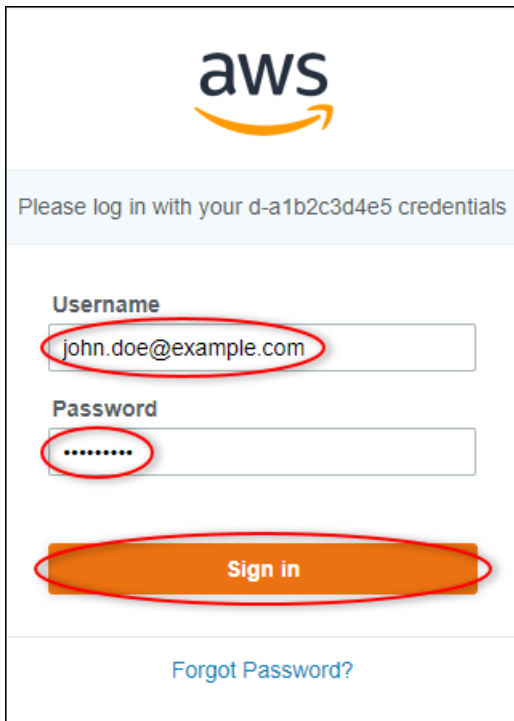
Se quiser fazer login mais tarde no portal como o segundo e o terceiro usuários do Centro de identidade do IAM que você criou anteriormente, você também pode realizar essas etapas para definir senhas para esses usuários.

 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 ter mais informações, consulte [Redefinir a senha de usuário do IAM Identity Center para um usuário final](#) no Guia do usuário do AWS IAM Identity Center .

3. Entre na sua Central de Identidade do IAM Username e Password. Se você criou seu usuário do IAM Identity Center no início deste 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. Escolha Sign in.

O portal é aberto.

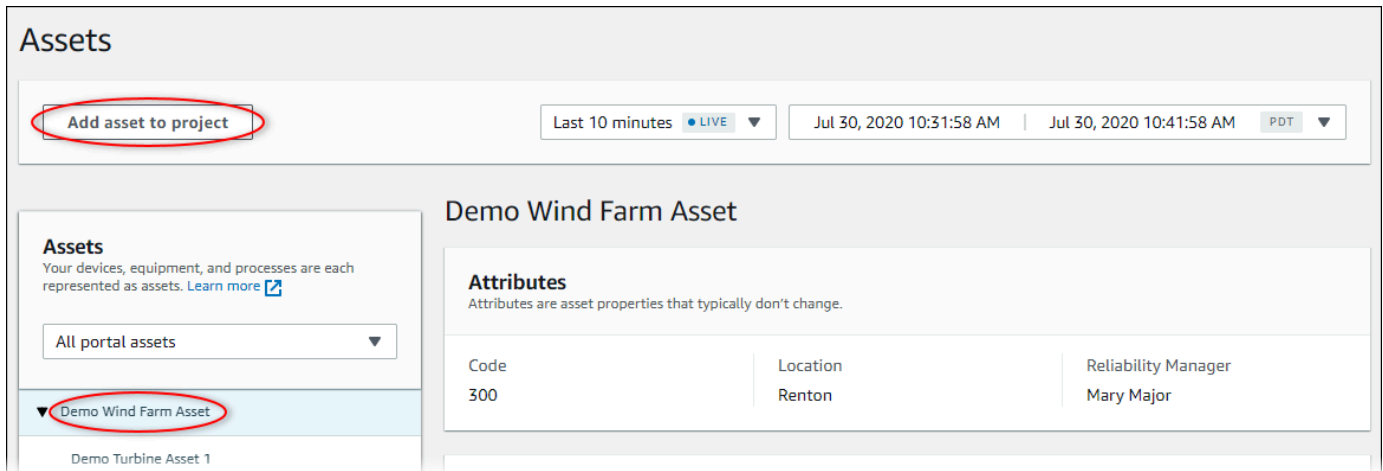
Etapa 3: criar um projeto de parque eólico

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, consulte [SiteWise Monitore as funções](#).

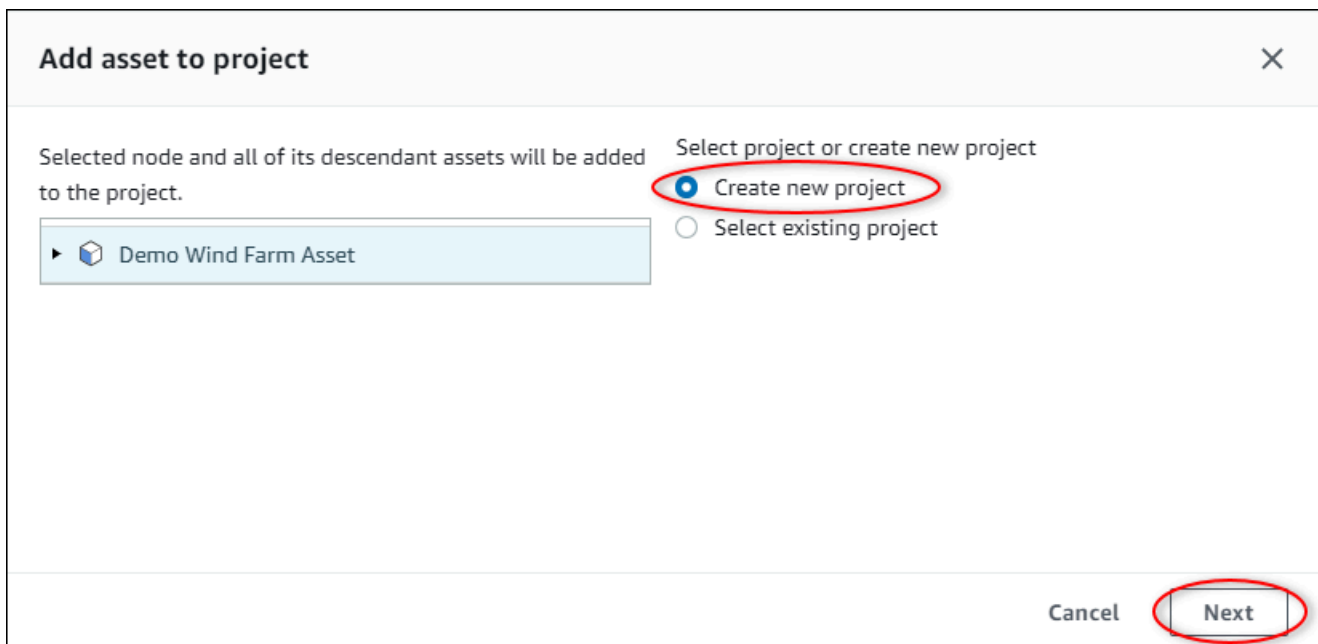
Como criar um projeto de parque de energia eólica

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 históricos e em tempo real 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.

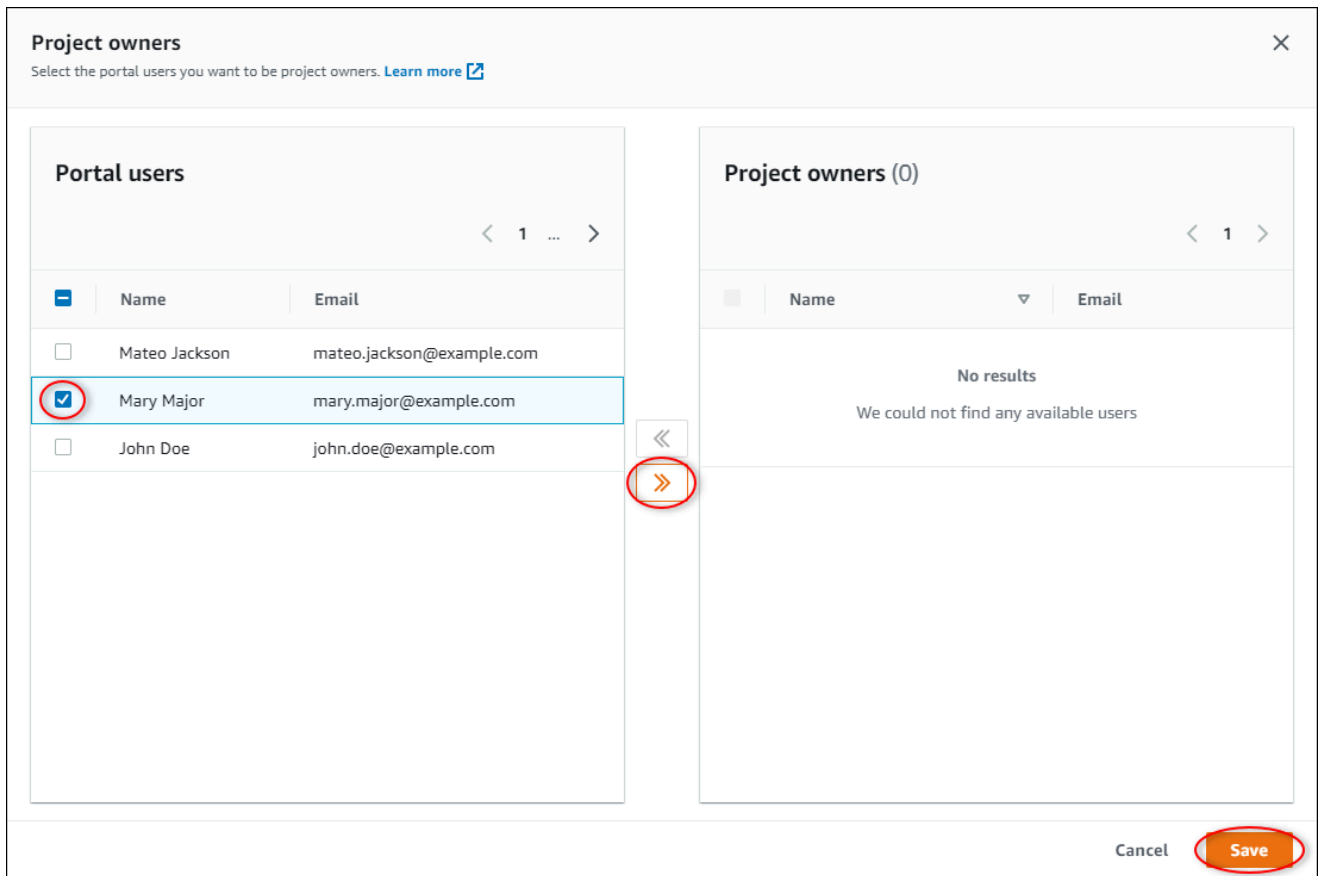
Note

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, em seguida, escolha o ícone >>.



- c. Escolha Salvar.

Seu usuário do IAM Identity Center Mary Major pode entrar neste portal para editar os painéis neste projeto e compartilhar esse projeto com outros usuários neste 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, em seguida, escolha o ícone >>.
- f. Escolha Salvar.

Seu usuário do IAM Identity Center Mateo Jackson pode entrar neste portal para visualizar, mas não editar, os painéis no projeto do parque eólico.

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

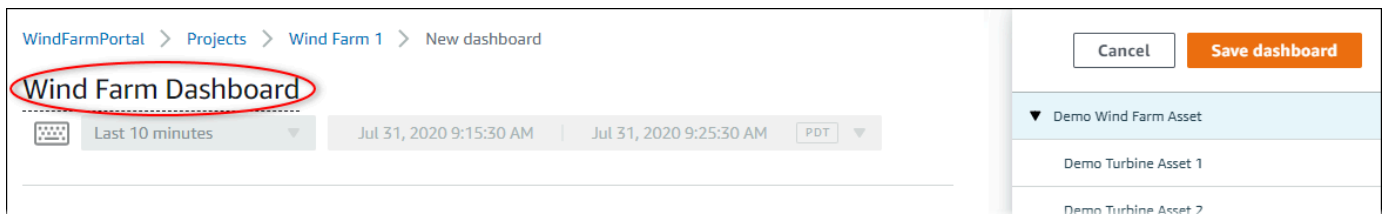
Neste procedimento, você cria painéis para visualizar os dados de demonstração do parque de energia eólica. Os painéis contêm visualizações personalizáveis dos dados de ativos do seu projeto. Cada visualização pode ter um tipo diferente, como um gráfico de linhas, gráfico de barras ou exibição de indicador-chave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

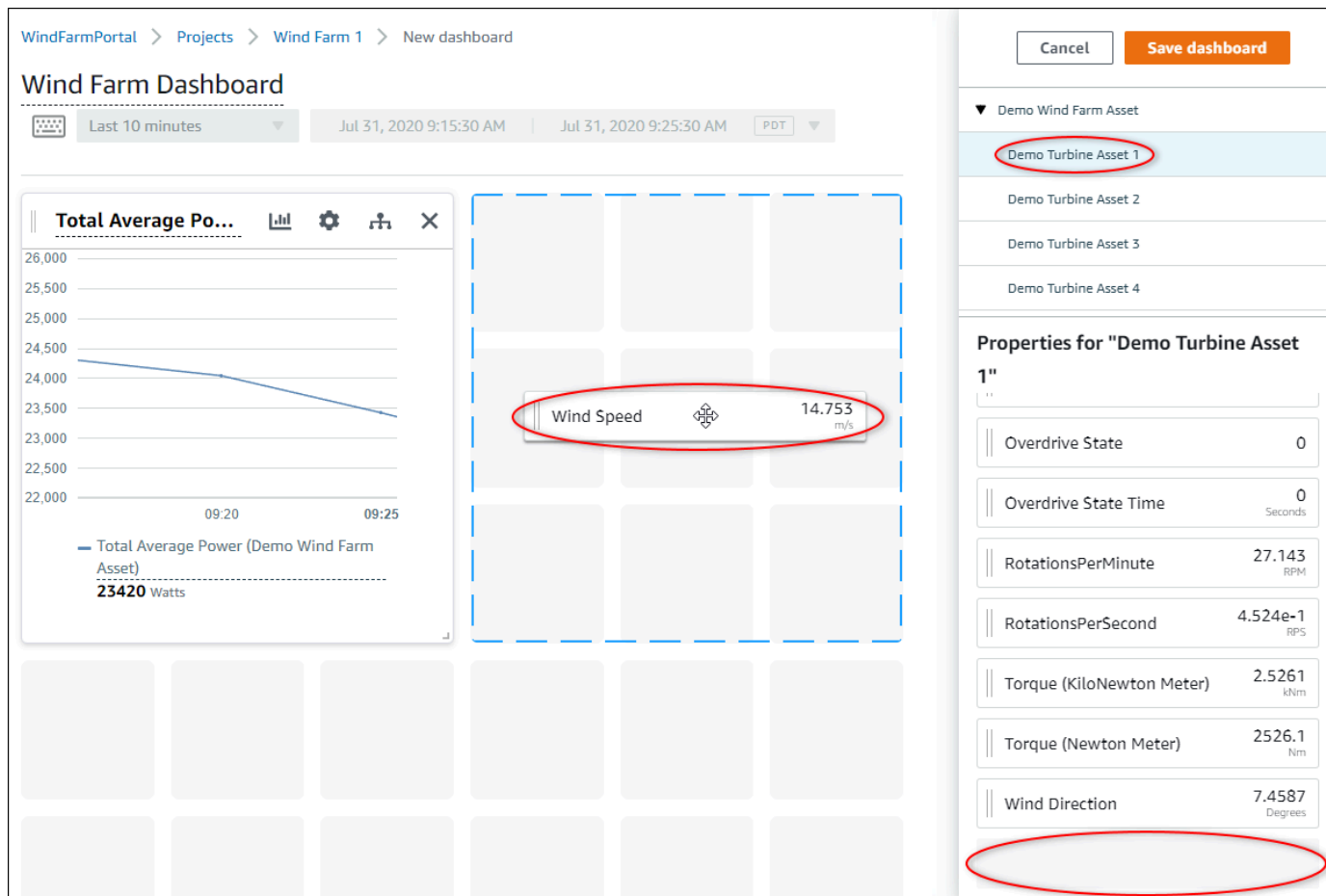
2. Insira um nome para seu painel.



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

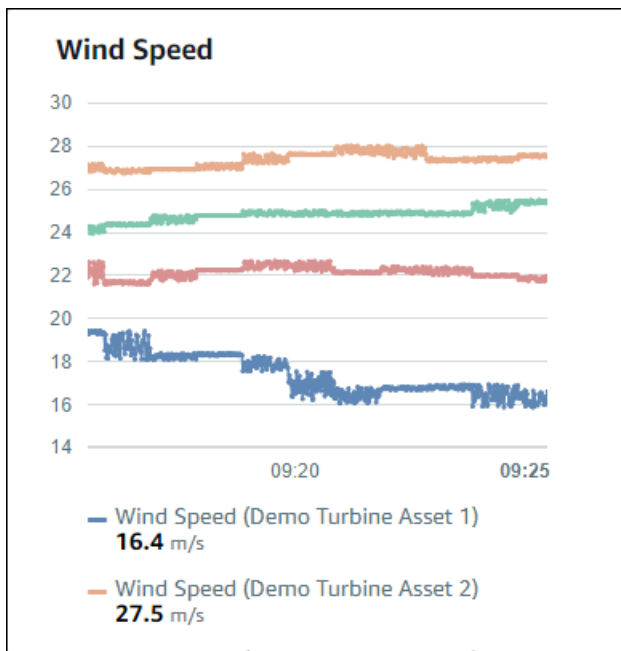
The screenshot displays the 'Wind Farm Dashboard' in the AWS IoT SiteWise console. The breadcrumb navigation at the top reads: 'WindFarmPortal > Projects > Wind Farm 1 > New dashboard'. The dashboard title is 'Wind Farm Dashboard'. Below the title, there are filters for 'Last 10 minutes', a date range from 'Jul 31, 2020 9:15:30 AM' to 'Jul 31, 2020 9:25:30 AM', and a time zone dropdown set to 'PDT'. The main area is a grid of 18 placeholder widgets. One widget, 'Total Average Power', is highlighted with a red oval and shows a value of '24038 Watts'. On the right, a sidebar contains a 'Cancel' button, a 'Save dashboard' button, and a list of assets under the heading 'Demo Wind Farm Asset': 'Demo Turbine Asset 1', 'Demo Turbine Asset 2', 'Demo Turbine Asset 3', and 'Demo Turbine Asset 4'. Below this is a section titled 'Properties for "Demo Wind Farm Asset"' containing two property cards: 'Code' with a value of '300' and 'Total Overdrive State Time' with a value of '0 seconds'. The 'Total Overdrive State Time' card is also highlighted with a red oval.

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

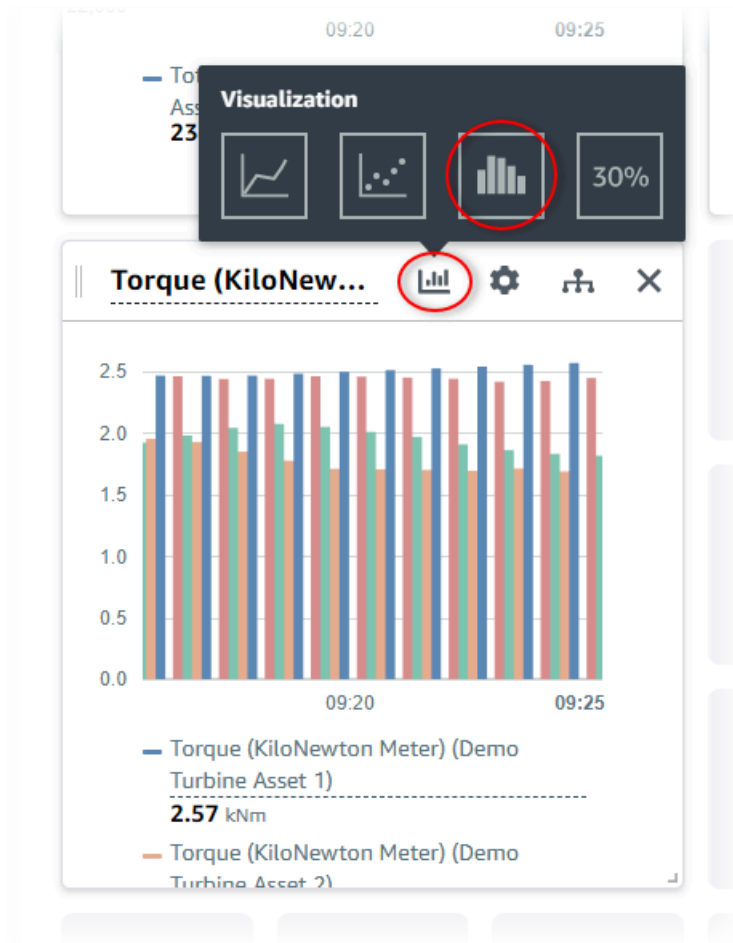


- Adicionar Wind Speed à nova visualização da velocidade do vento para cada Demo Turbine Asset 2, 3, e 4 (nessa ordem).

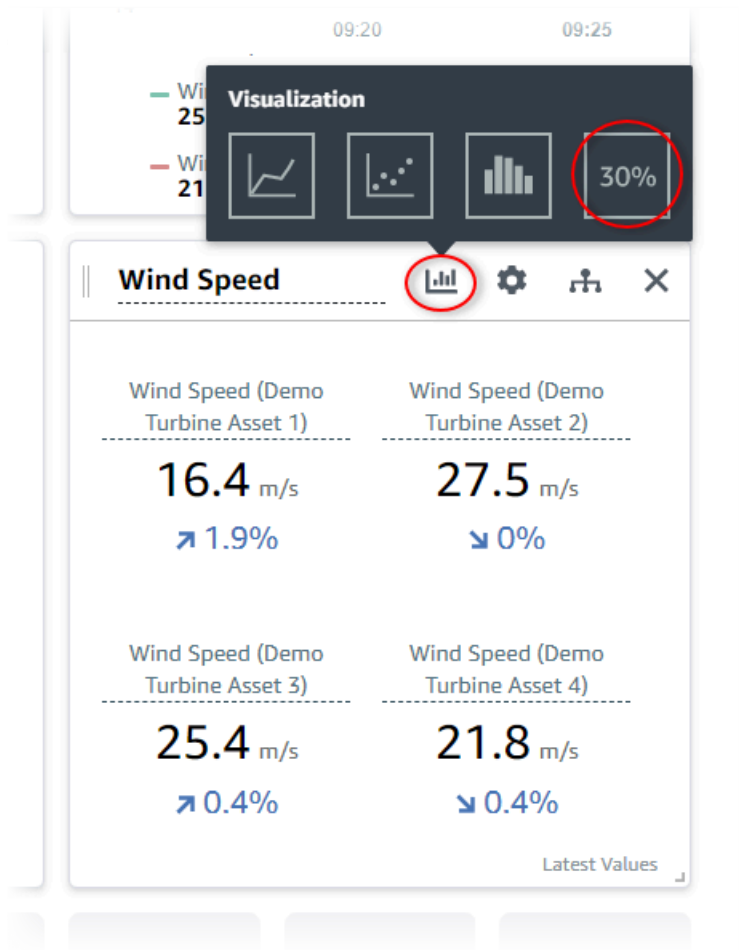
Sua Wind Speed visualização deve ser semelhante à captura de tela a seguir.



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

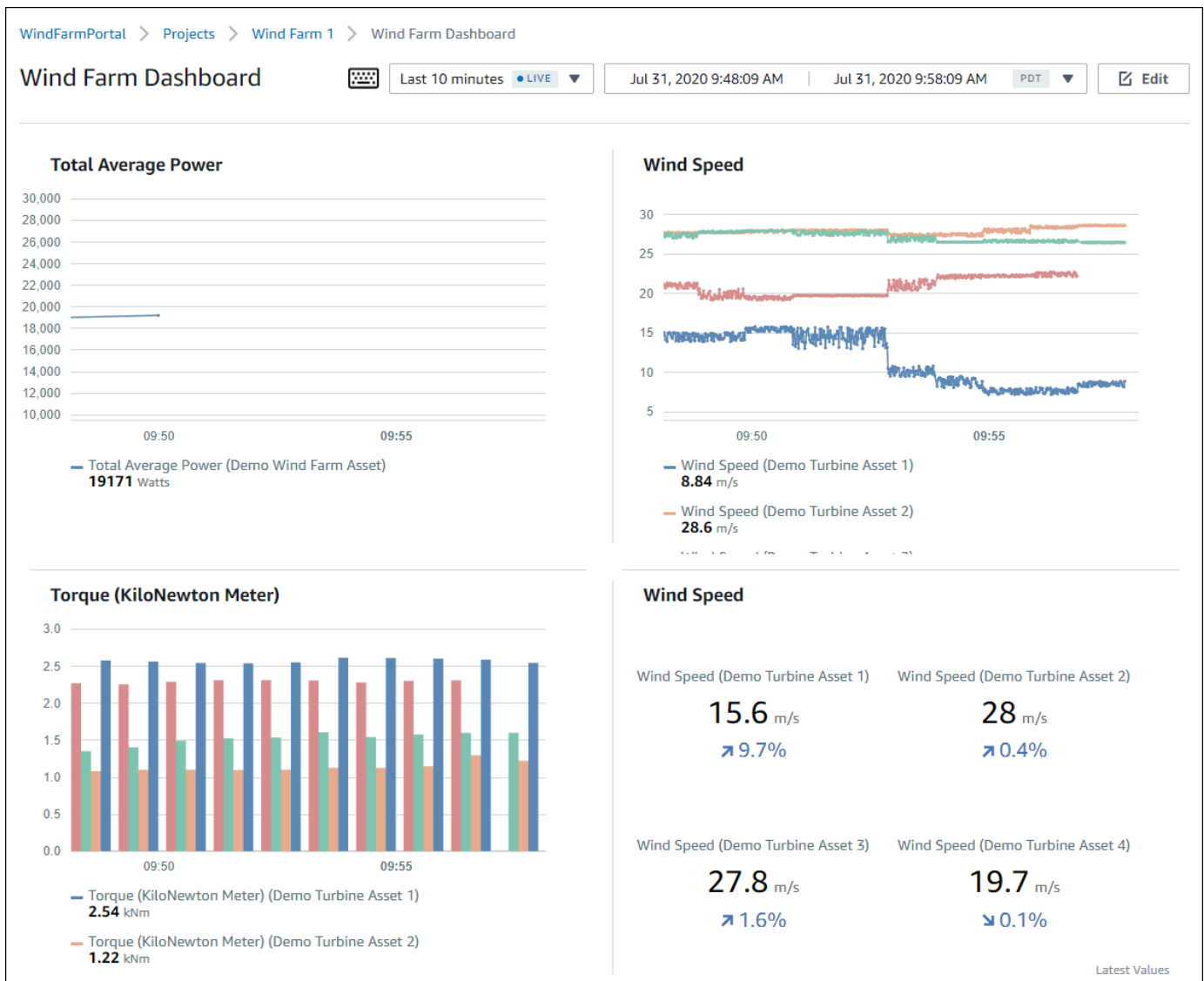


8. Repita as etapas 4 e 5 para as turbinas eólicas. Wind Directionpropriedades para criar uma visualização da direção do vento.
9. Escolha o ícone do tipo de visualização para o Wind Directionvisualização e, em seguida, escolha o ícone do gráfico de KPI (30%).



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.

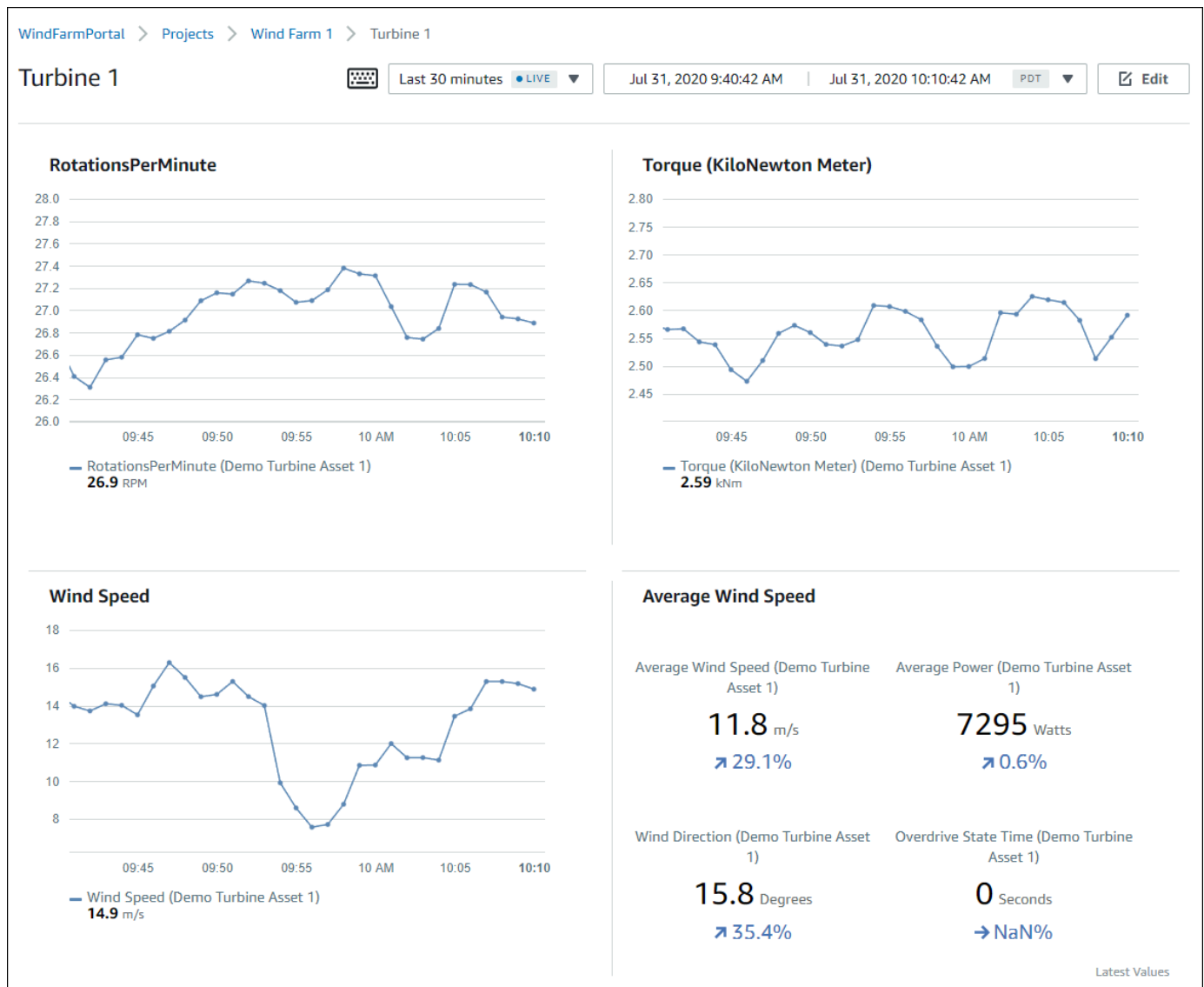
Seu painel deve ser semelhante à imagem a seguir.



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: explorar o portal

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

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 obter mais informações, consulte [Etapa 2: fazer login 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 obter mais informações, consulte [Exclua a AWS IoT SiteWise demonstração](#).

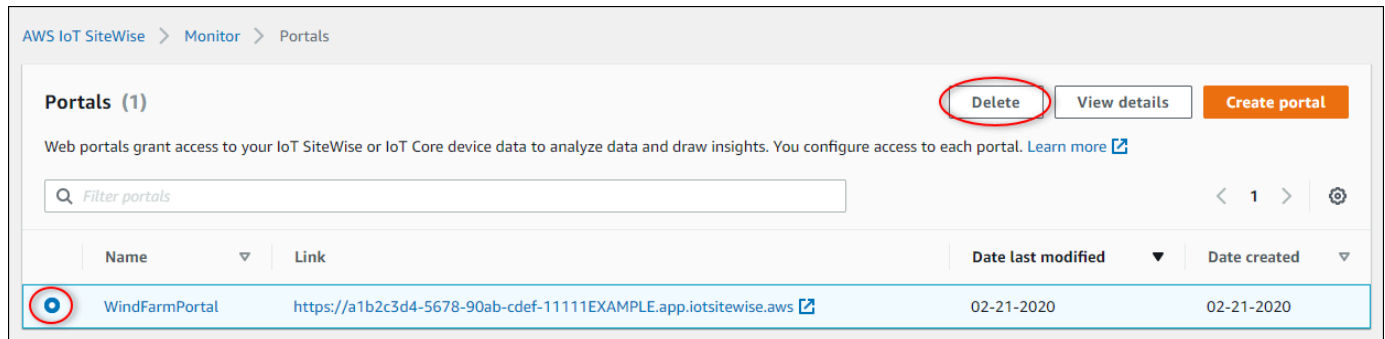
Use os procedimentos a seguir para excluir o portal e os usuários do Centro de identidade do IAM.

Para excluir um portal

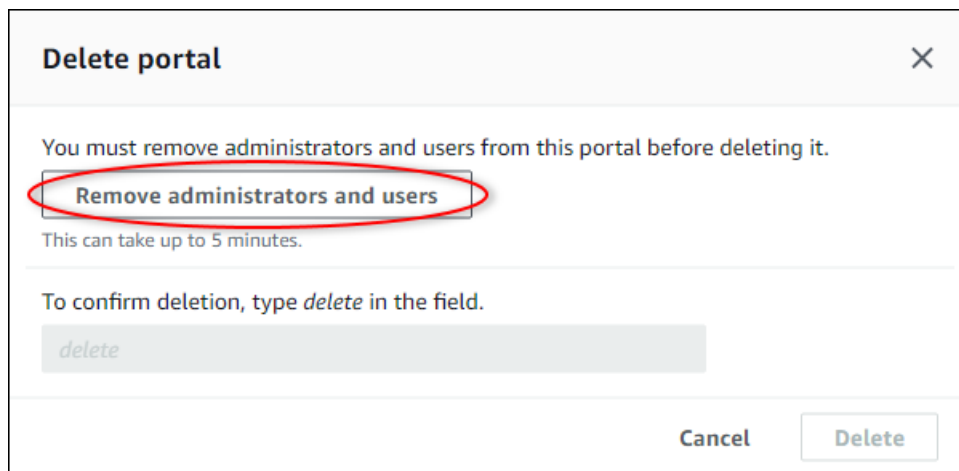
1. Navegue até o [console do AWS IoT SiteWise](#).

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

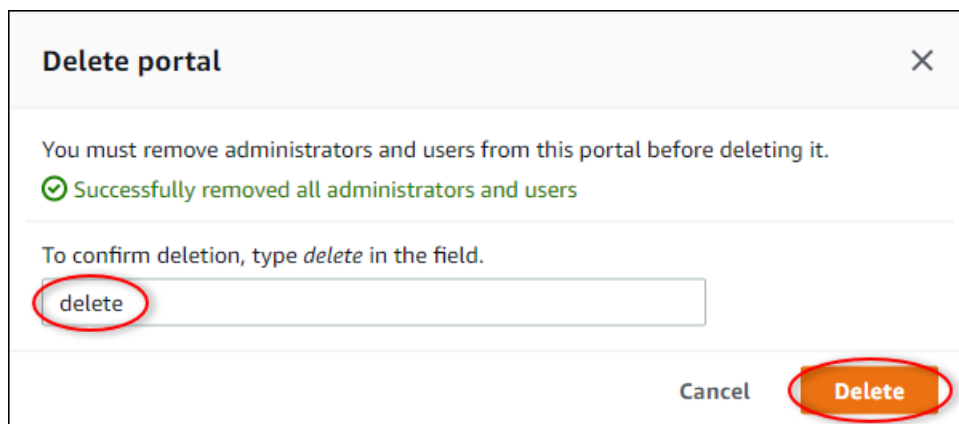
Quando você exclui um portal ou projeto, os ativos associados a projetos excluídos não são afetados.



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

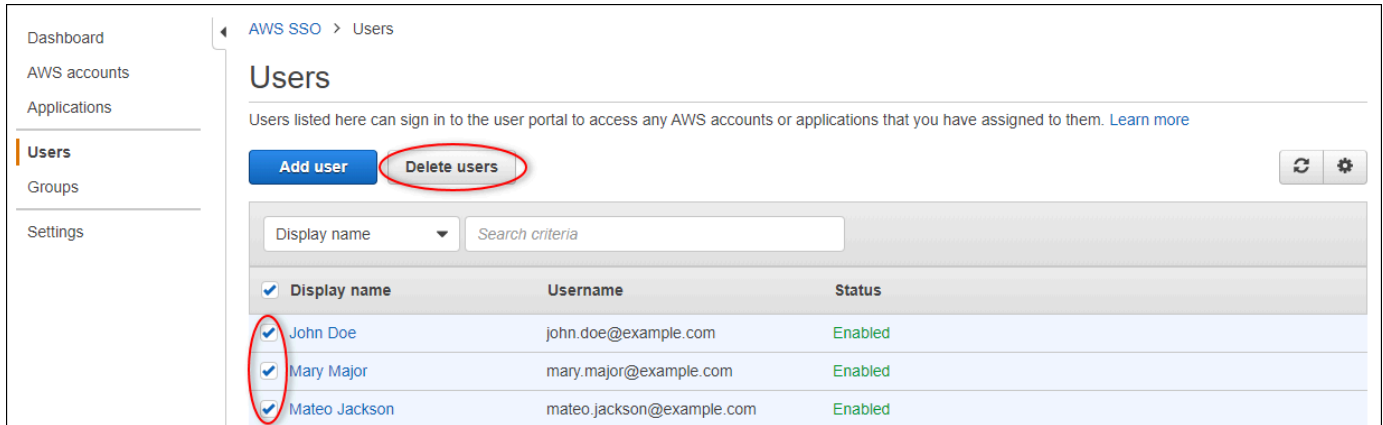


5. Digite **delete** para confirmar a exclusão e escolha Excluir.

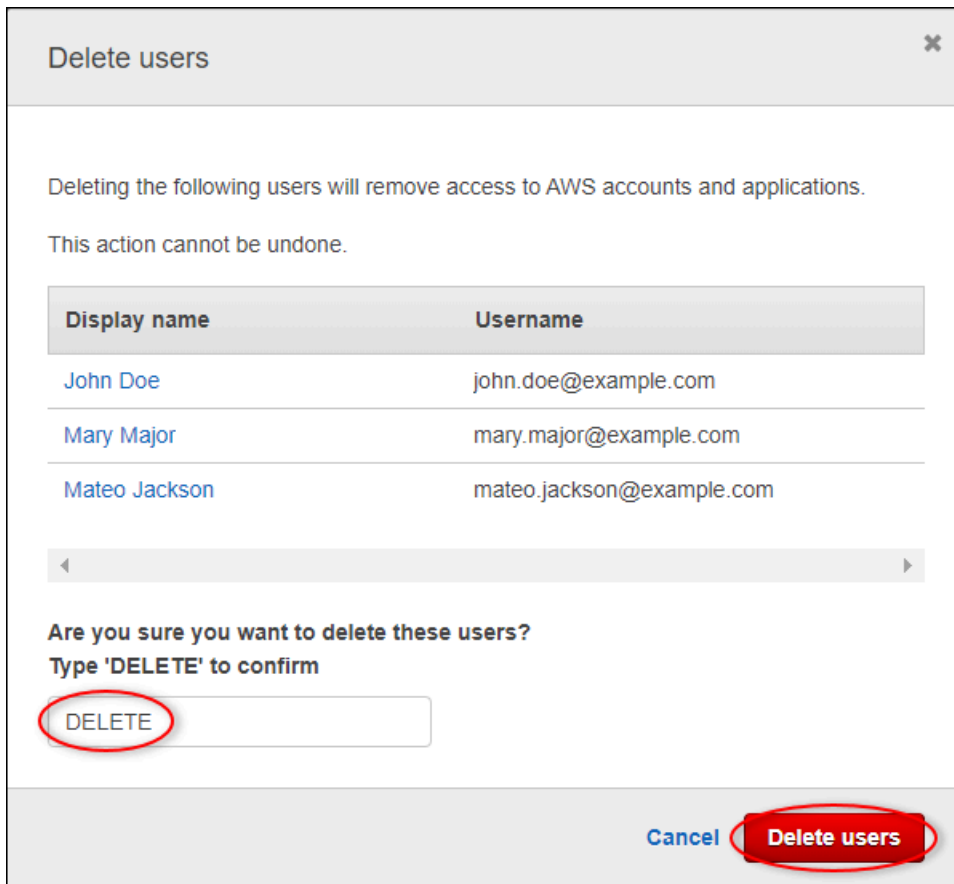


Excluir usuários do IAM Identity Center

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 valores de propriedade no Amazon DynamoDB

Este tutorial apresenta uma maneira 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 poderá criar software personalizado que consome os dados de ativos, como um mapa em tempo real de velocidade e direção do vento em um parque eólico inteiro. Se você quiser monitorar e visualizar os dados sem implementar uma solução de software personalizada, consulte [Monitore 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 obter mais informações, consulte [Interaja com outros AWS serviços](#).

Tópicos

- [Pré-requisitos](#)
- [Etapa 1: Configurar AWS IoT SiteWise para publicar atualizações de valores de propriedades](#)
- [Etapa 2: criar uma regra no AWS IoT Core](#)
- [Etapa 3: criar uma tabela do DynamoDB](#)
- [Etapa 4: configurar a ação de regra do DynamoDB](#)
- [Etapa 5: explorar os dados no DynamoDB](#)
- [Etapa 6: limpar os recursos após o tutorial](#)

Pré-requisitos

Para concluir este tutorial, você precisará do seguinte:

- Uma AWS conta. Se você não tiver uma, consulte [Configurar uma AWS conta](#).

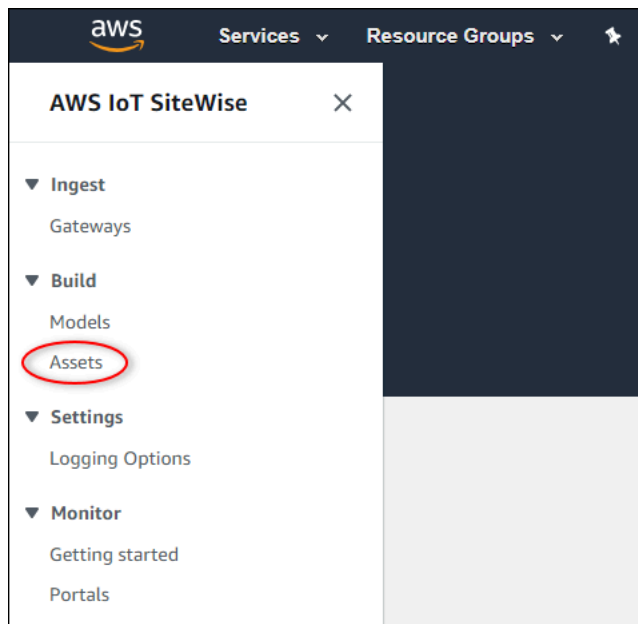
- Um computador de desenvolvimento executando Windows, macOS, Linux ou Unix para acessar o AWS Management Console Para ter mais informações, consulte [What is the AWS Management Console?](#).
- Um usuário do IAM com permissões de administrador.
- Uma demonstração em funcionamento de um parque AWS IoT 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 obter mais informações, consulte [Use a AWS IoT SiteWise demonstração](#).

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

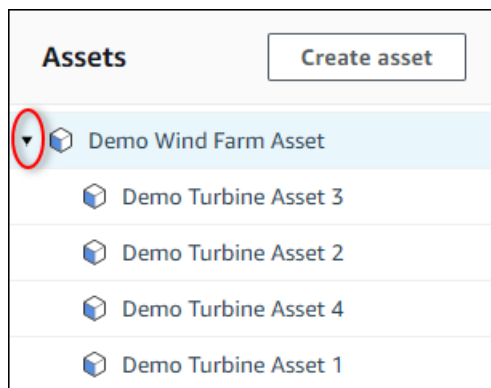
Neste procedimento, você habilita notificações de valor de propriedade em seus ativos de turbina de demonstração. Wind Speedpropriedades. Depois de ativar as notificações de valor da propriedade, AWS IoT SiteWise publica cada atualização de valor em uma mensagem MQTT no Core. AWS IoT

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

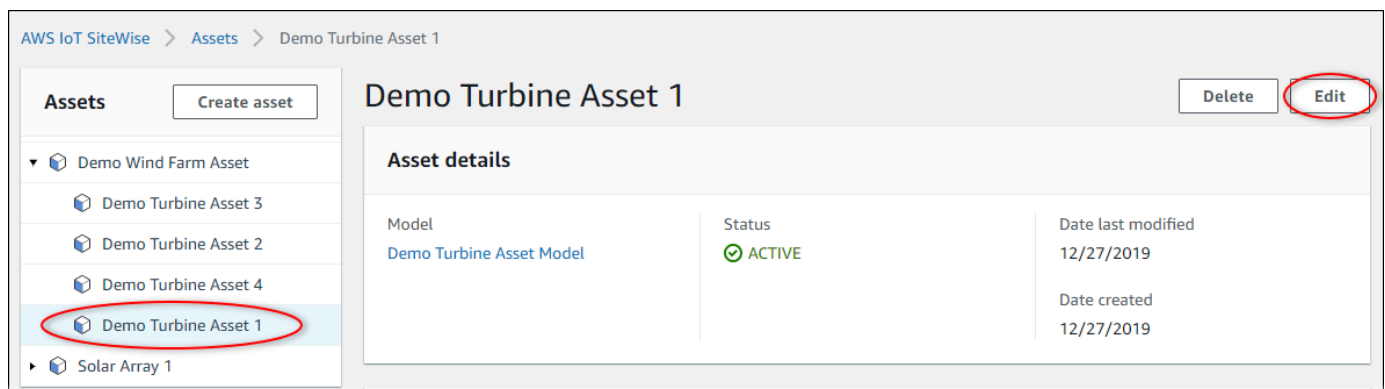
1. Faça login no [console do AWS IoT SiteWise](#).
2. Revise os [AWS IoT SiteWise endpoints e as cotas](#) em que AWS IoT SiteWise há suporte e troque de AWS região, se necessário. Mude para uma região onde você está executando a AWS IoT SiteWise demonstração.
3. No painel de navegação à esquerda, escolha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



4. Escolha a seta ao lado de Demo Wind Farm Asset para expandir a hierarquia dos ativos do parque eólico.



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



6. Atualizar a Wind SpeedO status de notificação da propriedade é ATIVADO.

"Wind Speed"

Enter a property alias

Must be less than 2048 characters.

Notification status

ENABLED

Notification will be published to topic \$aws/sitewise/asset-models/d8f8f20a-4d3a-491c-a9c5-352736979bdb/assets/db36f80f-ed03-44d9-84ef-817eb30d5497/properties/ca5b9e21-f19c-4ea1-8472-0e9400fc12bf

- Escolha Save asset (Salvar ativo) na parte inferior da página.
- Repita as etapas 5 a 7 para cada ativo da turbina de demonstração.
- Escolha uma turbina de demonstração (por exemplo, Demo Turbine Asset 1).
- Selecione Measurements (Medidas).
- Escolha o ícone de cópia ao lado do Wind Speed propriedade para copiar o tópico da notificação para sua 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.

Torque (KiloNewton Meter)	-	⊖ Disabled	-	2.128123
Wind Speed	-	✔ Enabled	\$aws/sitewise/asset-models/d8f8f...	26.49812

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

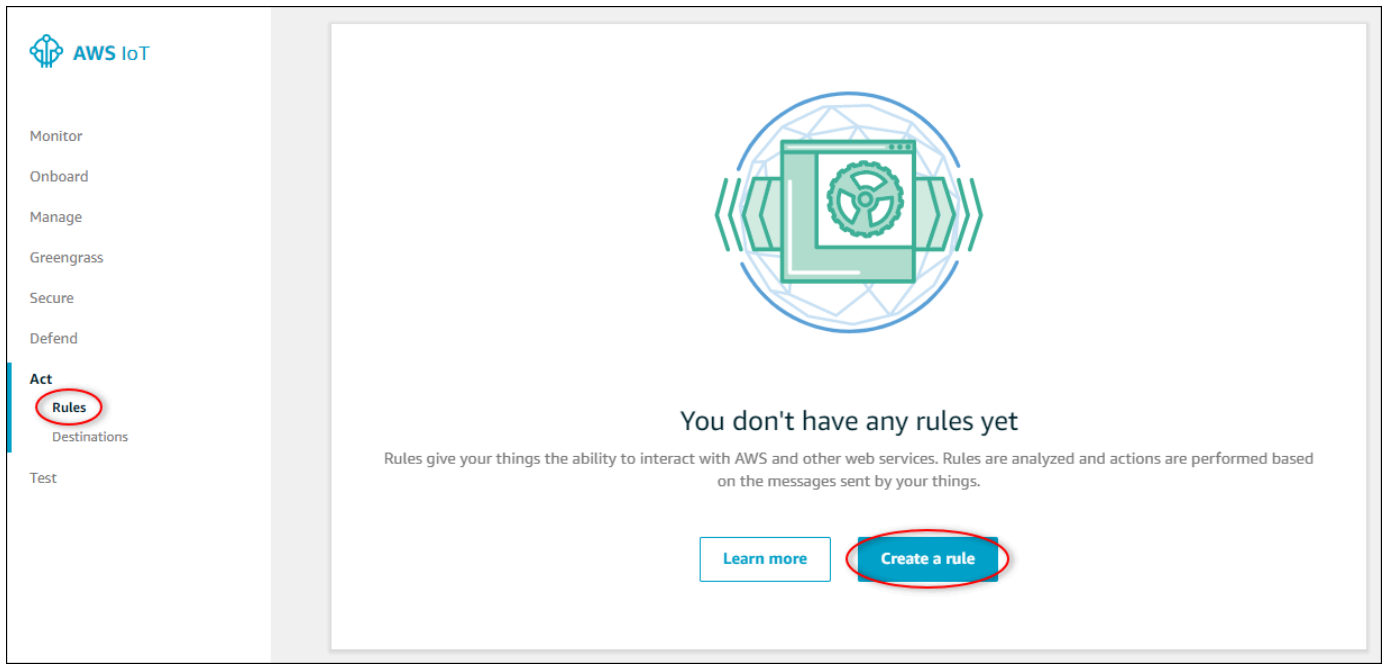
```
$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/
assets/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE/properties/a1b2c3d4-5678-90ab-
cdef-33333EXAMPLE
```

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. Depois, você pode criar 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

- Navegue até o [console do AWS IoT](#). Se um botão Get started (Começar a usar) for exibido, selecione-o.
- 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.

The image displays the 'Create a rule' form within the AWS IoT SiteWise console. The form has a blue header with the title 'Create a rule'. Below the header, there is instructional text: 'Create a rule to evaluate messages sent by your things and specify what to do when a message is received (for example, write data to a DynamoDB table or invoke a Lambda function)'. The form contains two input fields. The first field, labeled 'Name', contains the text 'WindSpeedRule' and is circled in red. The second field, labeled 'Description', contains the text 'A DynamoDBv2 rule that records wind data from wind turbine assets in AWS IoT SiteWise.' and is also circled in red.

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
```

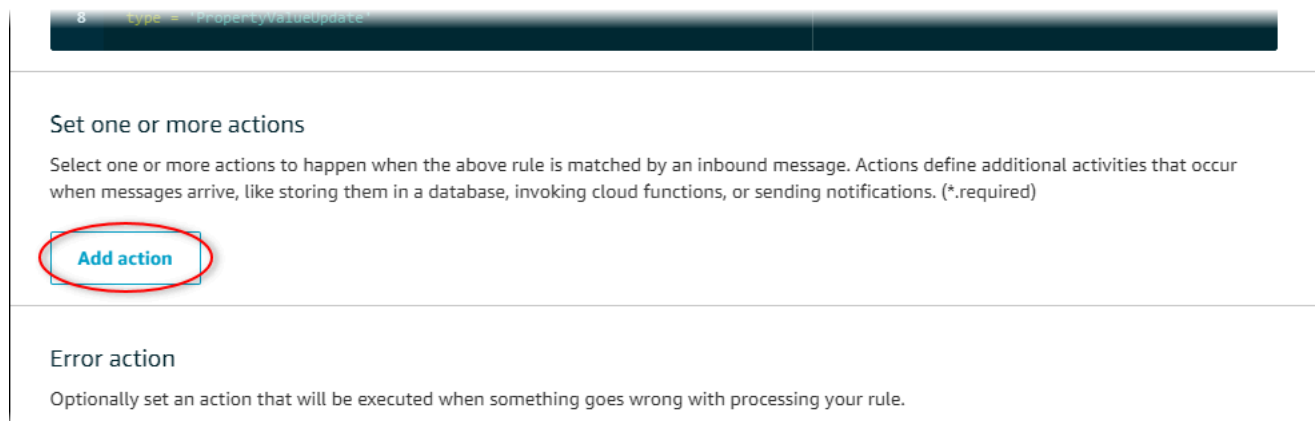
Substitua o ID de ativo (o ID depois de `assets/`) no tópico por um `+`. Isso seleciona a propriedade de velocidade do vento para todos os ativos de turbina eólica da demonstração. O filtro de tópico `+` aceita todos os nós de um único nível em um tópico. Seu tópico deve ser semelhante ao exemplo a seguir.

```
$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 `type = 'PropertyValueUpdate'`

Set one or more actions

Select one or more actions to happen when the above rule is matched by an inbound message. Actions define additional activities that occur when messages arrive, like storing them in a database, invoking cloud functions, or sending notifications. (*.required)

Add action

Error action

Optionally set an action that will be executed when something goes wrong with processing your rule.

8. Na página Selecionar uma ação, escolha Dividir mensagem em várias colunas de uma tabela do DynamoDB (Dynamo). DBv2



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, crie 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.

Create DynamoDB table

Tutorial ?

DynamoDB is a schema-less database that only requires a table name and primary key. The table's primary key is made up of one or two attributes that uniquely identify items, partition the data, and sort data within each partition.

Table name*

WindSpeedData

i

Primary key*

Partition key

timestamp

Number

i

☒ Add sort key

asset

String

i

Table settings

Default settings provide the fastest way to get started with your table. You can modify these default settings now or after your table has been created.

☒ Use default settings

- No secondary indexes.
- Provisioned capacity set to 5 reads and 5 writes.
- Basic alarms with 80% upper threshold using SNS topic "dynamodb".
- Encryption at Rest with DEFAULT encryption type.

i

You do not have the required role to enable Auto Scaling by default.
Please refer to [documentation](#).

+ Add tags

NEW!

Additional charges may apply if you exceed the AWS Free Tier levels for CloudWatch or Simple Notification Service. Advanced alarm settings are available in the CloudWatch management console.

Cancel

Create

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

- Digite **timestamp** como a chave de partição.
- Escolha o tipo Number (Número).
- Marque a caixa de seleção Add sort key (Adicionar chave de classificação).
- 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 de regra do DynamoDB

Neste procedimento, configure a ação de regra do Amazon DynamoDB para inserir dados de atualizações de valores de propriedade na 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.

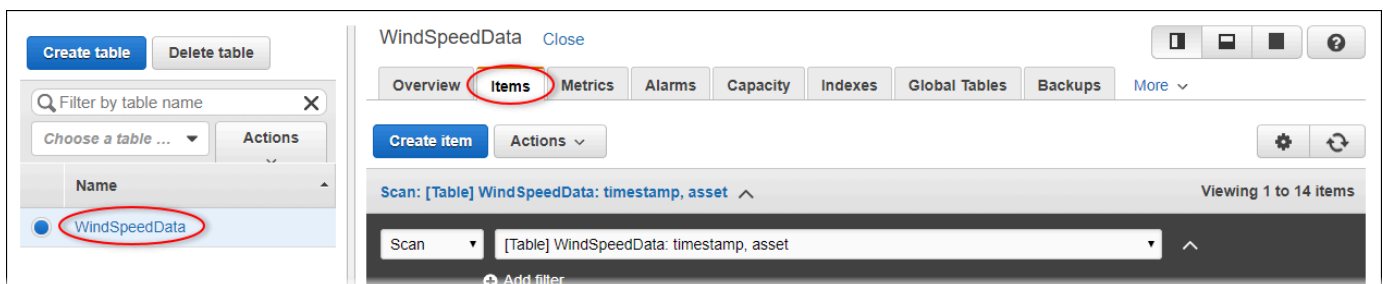
Os dados de ativo de demonstração devem começar a aparecer na tabela do DynamoDB.

Etapa 5: explorar os dados no DynamoDB

Neste procedimento, explore os dados da velocidade do vento dos ativos de demonstração na nova tabela do Amazon DynamoDB.

Como explorar dados de ativo no DynamoDB

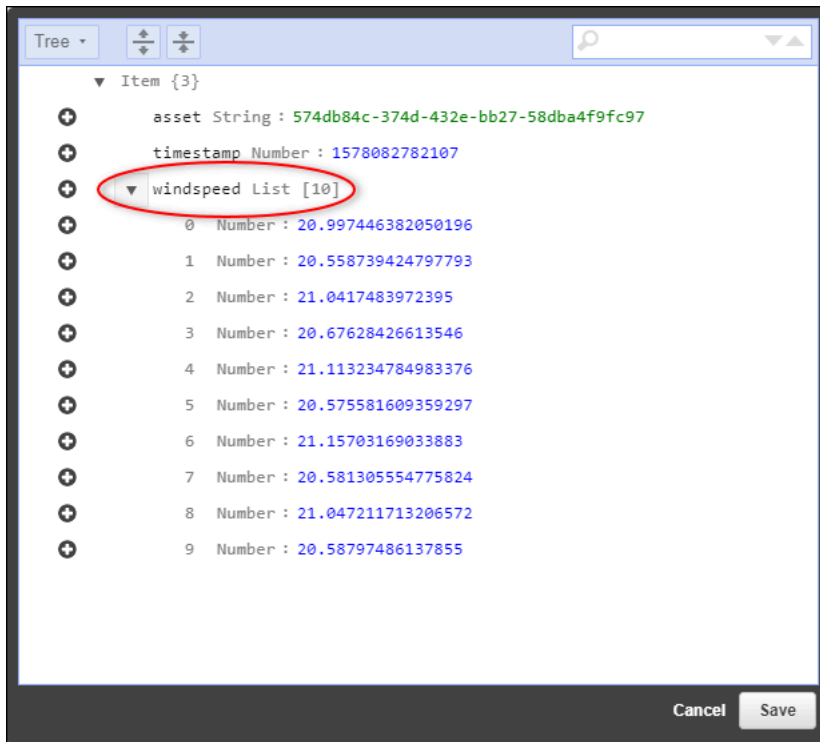
1. Retorne à guia com a tabela do DynamoDB aberta.
2. Na tabela criada anteriormente, escolha a guia Items (Itens) para exibir os dados na tabela. Atualize a página se você não vir linhas na tabela. Se as linhas não aparecerem após alguns minutos, consulte [Solucionar problemas em uma regra \(DynamoDB\)](#).



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

Start search			
	timestamp ⓘ	asset	windspeed
☐	1578093637414	db36f80f-ed03-44d9-84ef-817eb30d5497	[{"N": "40.18707553698584"}, {"N": "40.20834808480326"}, {"N": "40.21081344172715"}, {"N": "40.21828088809424"}, {"N": "40.218912043562895"}, {"N": "40.22691091326525"}, {"N": "40.22876939941959"}, {"N": "40.21820505495924"}, {"N": "40.21820505495924"}, {"N": "40.21820505495924"}]
☐	1578093637422	db36f80f-ed03-44d9-84ef-817eb30d5497	[{"N": "40.21081344172715"}, {"N": "40.21828088809424"}, {"N": "40.218912043562895"}, {"N": "40.22691091326525"}, {"N": "40.22876939941959"}, {"N": "40.21820505495924"}, {"N": "40.21820505495924"}, {"N": "40.21820505495924"}]
☐	1578093637451	db36f80f-ed03-44d9-84ef-817eb30d5497	[{"N": "40.218912043562895"}, {"N": "40.22691091326525"}, {"N": "40.22876939941959"}, {"N": "40.21820505495924"}, {"N": "40.21820505495924"}, {"N": "40.21820505495924"}]
☐	1578093637453	db36f80f-ed03-44d9-84ef-817eb30d5497	[{"N": "40.22876939941959"}, {"N": "40.21820505495924"}, {"N": "40.21820505495924"}, {"N": "40.21820505495924"}]

4. Escolha a seta ao lado do windspeedestrutura 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 obter mais informações, consulte [Consulte notificações de propriedades de ativos em AWS IoT SiteWise](#).



Agora que você concluiu o tutorial, desabilite ou exclua a regra e exclua a tabela do DynamoDB para evitar incorrer em cobranças adicionais. Para limpar os recursos, consulte [Etapa 6: limpar os recursos após o tutorial](#).

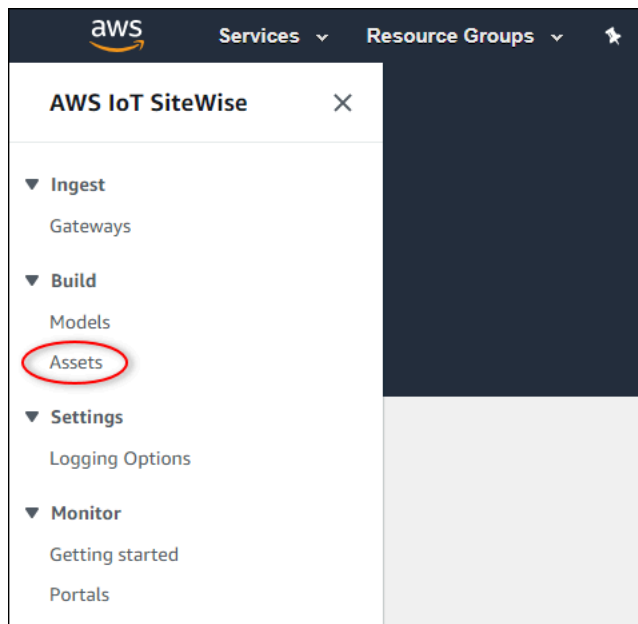
Etapa 6: limpar os recursos após o tutorial

Depois de concluir o tutorial, limpe os recursos para evitar a geração de cobranças adicionais. Os ativos de demonstração do parque eólico são excluídos no final da duração que você escolheu ao criar a demonstração. Também é possível excluir a demonstração manualmente. Para obter mais informações, consulte [Exclua a AWS IoT SiteWise demonstração](#).

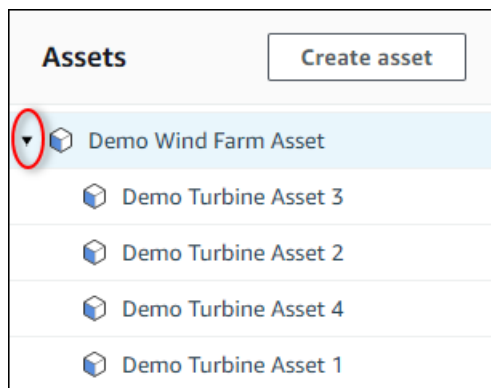
Use os procedimentos a seguir para desativar as notificações de atualização do valor da propriedade (se você não excluiu a demonstração), desativar ou excluir sua AWS IoT regra e excluir sua tabela do DynamoDB.

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

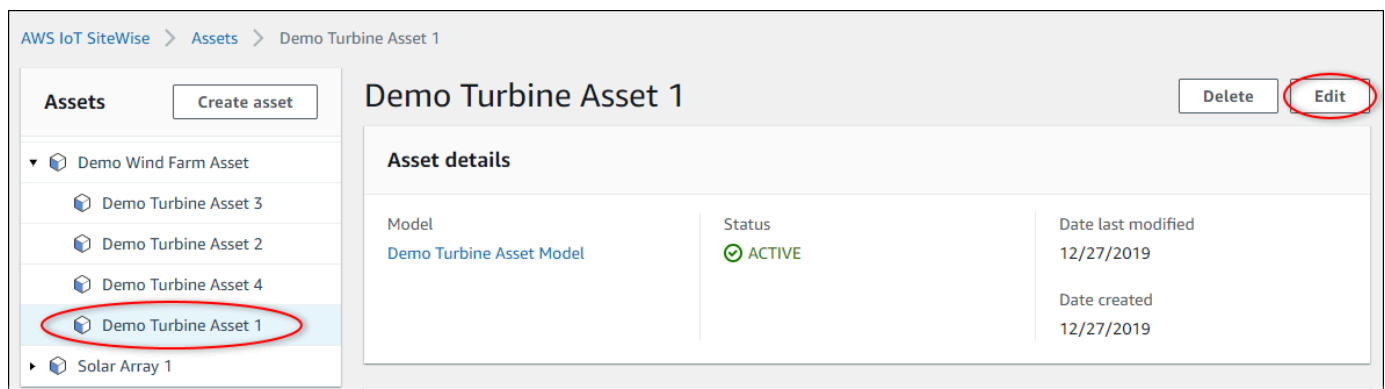
1. Navegue até o [console do AWS IoT SiteWise](#).
2. No painel de navegação à esquerda, escolha Ativos.



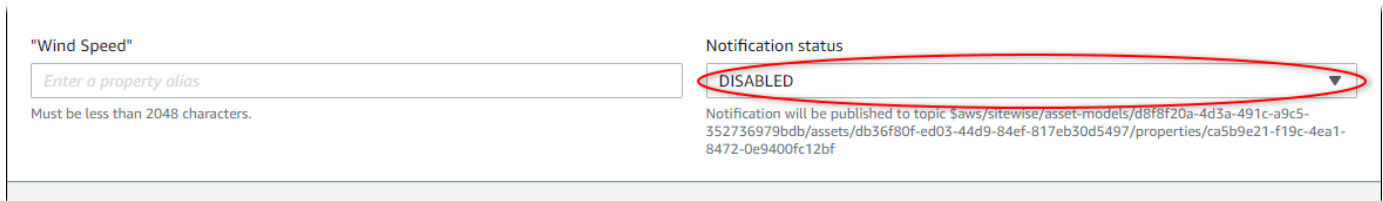
3. Escolha a seta ao lado de Demo Wind Farm Asset para expandir a hierarquia dos ativos do parque eólico.



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



5. Atualizar a Wind Speed status de notificação da propriedade como DESATIVADO.



"Wind Speed"

Enter a property alias

Must be less than 2048 characters.

Notification status

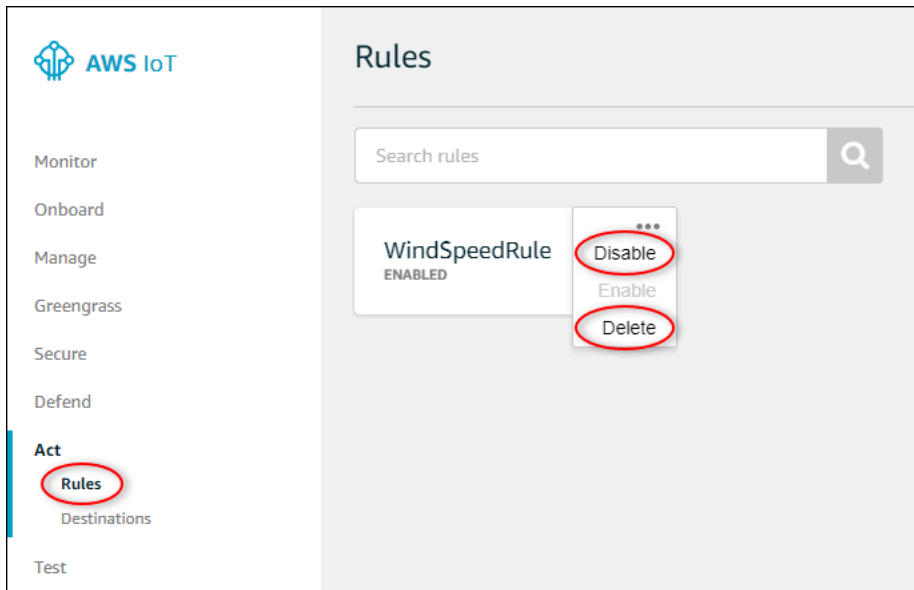
DISABLED

Notification will be published to topic \$aws/sitewise/asset-models/d8f8f20a-4d3a-491c-a9c5-352736979bdb/assets/db36f80f-ed03-44d9-84ef-817eb30d5497/properties/ca5b9e21-f19c-4ea1-8472-0e9400fc12bf

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.

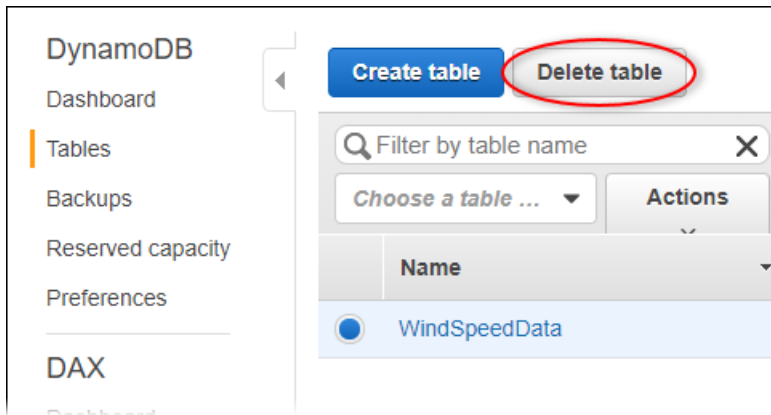
Para desativar ou excluir uma regra no AWS IoT Core

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).

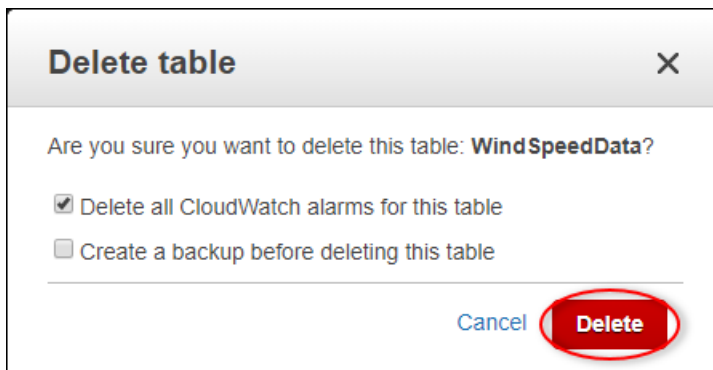


Como excluir uma tabela do DynamoDB

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



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



Ingerir 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 [Modelar 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 é compatível com a vinculação ao 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 [BatchPutAssetPropertyValue](#) API de streaming para ingestão em segundos ou a [CreateBulkImportJob](#) API 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 do ambiente on-premises ou de locais da 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.

Gerencie fluxos de dados para AWS IoT SiteWise

Um fluxo de dados é o recurso que contém dados históricos de séries temporais. Cada fluxo de dados é identificado por um alias exclusivo, facilitando o controle da origem de cada dado. Os fluxos de dados são criados automaticamente AWS IoT SiteWise quando os primeiros dados da série temporal são recebidos. Se os primeiros dados da série temporal forem identificados com um alias, AWS IoT SiteWise criará um novo fluxo de dados com esse alias, desde que nenhuma propriedade do ativo já tenha sido atribuída a esse alias. Como alternativa, se os primeiros dados da série temporal forem identificados com uma ID de ativo e uma ID de propriedade, AWS IoT SiteWise criará um novo fluxo de dados e associará esse fluxo de dados à propriedade do ativo.

Há duas maneiras de atribuir um alias a uma propriedade do ativo. O método usado depende se os dados são enviados AWS IoT SiteWise primeiro ou se um ativo é criado primeiro.

- Se os dados forem enviados AWS IoT SiteWise primeiro, isso criará automaticamente um fluxo de dados com o alias atribuído. Quando o ativo for criado posteriormente, use a [AssociateTimeSeriesToAssetProperty](#) API para associar o fluxo de dados e seu alias à propriedade do ativo.
- Se um ativo for criado primeiro, use a [UpdateAssetProperty](#) API para atribuir um alias a uma propriedade do ativo. Quando os dados são enviados posteriormente AWS IoT SiteWise, o fluxo de dados é criado automaticamente e associado à propriedade do ativo.

No momento, só é possível 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 medições 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.

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

- [Definir permissões e configurações](#)
- [Associar um fluxo de dados a uma propriedade do ativo](#)
- [Desassociar um fluxo de dados de uma propriedade do ativo](#)
- [Criar um fluxo de dados](#)
- [Atualizar um alias de propriedade do ativo](#)
- [Cenários comuns](#)

Definir permissões e configurações

Os fluxos de dados são criados automaticamente AWS IoT SiteWise quando os primeiros dados da série temporal são recebidos. Se os dados ingeridos não estiverem associados a uma propriedade do ativo, AWS IoT SiteWise criará um novo fluxo de dados desassociado que pode ser configurado para ser associado a uma propriedade do ativo. Configure o controle de acesso do gateway para o qual os dados são enviados AWS IoT SiteWise, usando políticas do IAM para especificar o tipo de dados a serem ingeridos.

A política do IAM a seguir desativa a ingestão de dados dissociados do gateway, ao mesmo tempo em que permite a ingestão de dados em fluxos de dados associados a uma propriedade do ativo:

Exemplo Política de usuário do IAM que desativa a ingestão de dados dissociados do gateway

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowPutAssetPropertyValuesUsingAssetIdAndPropertyId",
      "Effect": "Allow",
      "Action": "iotsitewise:BatchPutAssetPropertyValue",
      "Resource": "arn:aws:iotsitewise:*:*:asset/*"
    },
    {
      "Sid": "AllowPutAssetPropertyValuesUsingAliasWithAssociatedAssetProperty",
      "Effect": "Allow",
      "Action": "iotsitewise:BatchPutAssetPropertyValue",
      "Resource": "arn:aws:iotsitewise:*:*:time-series/*",
      "Condition": {
        "StringLikeIfExists": {
```

```

        "iotsitewise:isAssociatedWithAssetProperty": "true"
    }
  },
  {
    "Sid": "DenyPutAssetPropertyValuesUsingAliasWithNoAssociatedAssetProperty",
    "Effect": "Deny",
    "Action": "iotsitewise:BatchPutAssetPropertyValue",
    "Resource": "arn:aws:iotsitewise:*:*:time-series/*",
    "Condition": {
      "StringLikeIfExists": {
        "iotsitewise:isAssociatedWithAssetProperty": "false"
      }
    }
  }
]
}

```

Exemplo Política de usuário do IAM que desativa toda a ingestão de dados do gateway

```

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

```

Associar um fluxo de dados a uma propriedade do ativo

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. Escolha um fluxo de dados filtrando pelo alias do fluxo de dados ou selecionando fluxos de dados desassociados no menu suspenso do filtro.
4. Selecione o fluxo de dados a ser atualizado. Você pode selecionar vários fluxos de dados. Clique em Gerenciar fluxos de dados no canto superior direito.
5. Selecione o fluxo de dados a ser associado em Atualizar associações de fluxo de dados e clique no botão Escolher medição.
6. Na seção Escolher medida, encontre a propriedade de medição do ativo correspondente. Selecione a medida e clique em Escolher.
7. Execute as etapas 4 e 5 para outros fluxos de dados selecionados na etapa 3. Atribua propriedades de ativos a todos os fluxos de dados.
8. Escolha Atualizar para confirmar as alterações. Um banner de confirmação bem-sucedido é exibido para confirmar a atualização.

AWS CLI

Para associar um fluxo de dados (identificado por seu alias) a uma propriedade do ativo (identificada por seu IDs), execute o seguinte comando:

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

Desassociar um fluxo de dados de uma propriedade do ativo

Console

Use o AWS IoT SiteWise console para desassociar seu fluxo de dados de uma propriedade do ativo.

Para desassociar fluxos de dados de uma propriedade do ativo (console)

1. Navegue até o [console do AWS IoT SiteWise](#).
2. No painel de navegação, selecione Fluxos de dados.
3. Escolha um fluxo de dados filtrando pelo alias do fluxo de dados ou selecionando fluxos de dados associados no menu suspenso do filtro.
4. Selecione o fluxo de dados a ser desassociado. A coluna de alias do fluxo de dados deve conter um alias. As colunas Nome do ativo e Nome da propriedade do ativo devem conter os valores da propriedade do ativo à qual o fluxo de dados está associado. Você pode selecionar vários fluxos de dados.
5. Clique em Gerenciar fluxos de dados no canto superior direito.
6. Na seção Atualizar associações de fluxo de dados, clique em X na coluna Nome da medida. Um submitted status deve aparecer na coluna Status.
7. Escolha Atualizar para confirmar as alterações. O fluxo de dados agora está desassociado da propriedade do ativo e o alias agora é usado para identificar o fluxo de dados.

AWS CLI

Para desassociar um fluxo de dados de uma propriedade do ativo (identificada por seu ID s e seu alias), execute o seguinte comando:

```
aws iotsitewise disassociate-time-series-from-asset-property \
  --alias <asset-property-alias> \
  --assetId <asset-ID> \
  --propertyId <property-ID>
```

O fluxo de dados agora está desassociado da propriedade do ativo e o alias é usado para identificar o fluxo de dados. O alias não está mais associado à propriedade do ativo, pois agora está associado ao fluxo de dados.

Criar um fluxo de dados

Quando uma propriedade é removida de um modelo de ativo, AWS IoT SiteWise exclui as propriedades e seus fluxos de dados de todos os ativos gerenciados pelo modelo de ativo. Ele também exclui todas as propriedades e seus fluxos de dados de um ativo quando o ativo é excluído.

Se os dados de um fluxo de dados precisarem ser preservados, eles deverão ser desassociados da propriedade do ativo antes de serem excluídos.

Warning

Quando uma propriedade é excluída de um ativo, o fluxo de dados associado também é excluído. Para preservar o fluxo de dados, desassocie-o primeiro da propriedade do ativo, antes de excluir a propriedade do modelo do ativo ou excluir o ativo.

Console

Use o AWS IoT SiteWise console para desassociar seu fluxo de dados de uma propriedade do ativo.

Para excluir um fluxo de dados (console)

1. Navegue até o [console do AWS IoT SiteWise](#).
2. No painel de navegação, selecione Fluxos de dados.
3. Escolha um fluxo de dados filtrando pelo alias do fluxo de dados.
4. Selecione o fluxo de dados a ser excluído. Você pode selecionar vários fluxos de dados.
5. Escolha o botão Excluir para excluir o fluxo de dados.

AWS CLI

Use a [DeleteTimeSeries](#) API para excluir um fluxo de dados específico, usando seu alias.

```
aws iotsitewise delete-time-series \  
  --alias <data-stream-alias>
```

Atualizar um alias de propriedade do ativo

Os aliases devem ser exclusivos em uma AWS região. Isso inclui aliases de propriedades de ativos e fluxos de dados. Não atribua um alias a uma propriedade do ativo, se outra propriedade ou fluxo de dados estiver usando esse alias.

Console

Use o AWS IoT SiteWise console para atualizar um alias de propriedade do ativo.

Para atualizar um alias de propriedade do ativo (console)

1. Navegue até o [console do AWS IoT SiteWise](#).
2. No painel de navegação, selecione Ativos.
3. Selecione o ativo na tabela.
4. Clique no botão Edit (Editar).
5. Selecione o tipo de propriedade na tabela Propriedades.
6. Encontre a propriedade e digite o novo alias no campo de texto do alias da propriedade.
7. Clique no botão Salvar para salvar as alterações.

AWS CLI

Para atualizar um alias em uma propriedade do ativo, execute o seguinte comando:

```
aws iotsitewise update-asset-property \  
  --asset-id <asset-ID> \  
  --property-id <property-ID> \  
  --property-alias <asset-property-alias> \  
  --property-notification-state <ENABLED|DISABLED>
```

Note

Se as notificações de propriedade estiverem habilitadas no momento, elas deverão ser fornecidas novamente para garantir que continuem sendo ativadas.

Cenários comuns

Mover um fluxo de dados

Para alterar a associação de um fluxo de dados com outra propriedade do ativo, primeiro desassocie o fluxo de dados da propriedade atual do ativo. Ao desassociar um fluxo de dados de uma propriedade do ativo, deve haver um alias atribuído a essa propriedade do ativo.

```
aws iotsitewise disassociate-time-series-from-asset-property \  
  --alias <asset-property-alias> \  
  --assetId <asset-ID> \  
  --propertyId <property-ID>
```

Agora, reatribua o fluxo de dados à nova propriedade do ativo.

```
aws iotsitewise associate-time-series-from-asset-property \  
  --alias <data-stream-alias> \  
  --assetId <new-asset-ID> \  
  --propertyId <new-property-ID>
```

Erro ao atribuir um alias a uma propriedade do ativo

Ao usar a `UpdateAssetProperty` API para atribuir um alias a uma propriedade, você pode ver a seguinte mensagem de erro:

```
Given alias <data-stream-alias> for property <property-name> with ID <property-ID>  
already in use by another property or data stream
```

Essa mensagem de erro indica que o alias não está atribuído à propriedade porque ele é usado atualmente por outra propriedade ou por um fluxo de dados.

Isso acontece se os dados estiverem sendo ingeridos AWS IoT SiteWise com um alias. Quando os dados são enviados com um alias que não está sendo usado por outro fluxo de dados ou propriedade do ativo, um novo fluxo de dados é criado com esse alias. As duas opções abaixo resolvem o problema.

- Use a `AssociateTimeSeriesToAssetProperty` API para associar o fluxo de dados com seu alias à propriedade do ativo.
- Interrompa temporariamente a ingestão de dados e exclua o fluxo de dados. Use a `UpdateAssetProperty` API para atribuir o alias à propriedade do ativo e, em seguida, reative a ingestão de dados.

Erro ao associar um fluxo de dados a uma propriedade do ativo

Ao associar um fluxo de dados a uma propriedade do ativo, a seguinte mensagem de erro é exibida.

```
assetProperty <property-name> with assetId <asset-ID> propertyId <property-ID> contains  
data
```

Essa mensagem de erro indica que a propriedade do ativo já está associada a um fluxo de dados contendo dados. Esse fluxo de dados deve ser desassociado ou excluído antes de associar outro fluxo de dados a essa propriedade do ativo.

 Note

Ao desassociar um fluxo de dados de uma propriedade do ativo, o alias atribuído à propriedade é fornecido ao fluxo de dados. Para que esse alias permaneça atribuído à propriedade, atribua um novo alias a essa propriedade antes de desassociar o fluxo de dados.

Para preservar os dados armazenados na propriedade do ativo, faça o seguinte:

- Certifique-se de que nenhum dado esteja sendo ingerido na propriedade do ativo, para evitar a criação de um novo fluxo de dados.
- Use a `UpdateAssetProperty` API para definir um novo alias que é fornecido ao fluxo de dados atualmente atribuído.
- Use a `DisassociateTimeSeriesFromAssetProperty` API para desassociar o fluxo de dados atual da propriedade do ativo.
- Use a `AssociateTimeSeriesToAssetProperty` API para associar o fluxo de dados desejado à propriedade do ativo.

Se os dados armazenados na propriedade do ativo precisarem ser excluídos, faça o seguinte:

- Certifique-se de que nenhum dado esteja sendo ingerido na propriedade do ativo, para evitar a criação de um novo fluxo de dados.
- Use a `DeleteTimeSeries` API para excluir o fluxo de dados atualmente atribuído.
- Use a `AssociateTimeSeriesToAssetProperty` API para associar o fluxo de dados desejado à propriedade do ativo.

Ingira dados com AWS IoT SiteWise APIs

Use AWS IoT SiteWise APIs para enviar dados industriais com data e hora para os atributos e propriedades de medição de seus ativos. APIs Aceita estruturas contendo carga útil timestamp-quality-value (TQV).

BatchPutAssetPropertyValue API

Use a operação [BatchPutAssetPropertyValue](#) para fazer upload dos seus dados. Com essa operação, você pode fazer upload de várias entradas de dados de uma só vez para coletar dados de vários dispositivos e enviar tudo em uma única solicitação.

Important

A [BatchPutAssetPropertyValue](#) operação 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 [BatchPutAssetPropertyValue](#) na Referência de API do AWS IoT SiteWise .

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

- O `assetId` e `propertyId` da propriedade de 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 propriedade, consulte [Gerencie fluxos de dados para AWS IoT SiteWise](#).

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 útil em `batch-put-payload.json` tem o seguinte conteúdo.

```
{
  "enablePartialEntryProcessing": true,
  "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"
        }
      ]
    },
    {
      "entryId": "unique entry ID",
      "propertyAlias": "/company/windfarm/3/turbine/7/rpm",
      "propertyValues": [
        {
          "value": {
```



```
    "nullValue":{"valueType": "D"}
      },
      "timestamp": {
        "timeInSeconds": 1575691200
      },
      "quality": "BAD"
    }
  ]
}
]
```

Especificar `enablePartialEntryProcessing` como `true` permite a ingestão de todos os valores que não resultam em falha. O comportamento padrão é `false`. Se um valor for inválido, a entrada inteira falhará na ingestão.

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 `value`, `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`
 - `nullValue`
- `nullValue`— Uma estrutura com o campo a seguir indicando o tipo do valor da propriedade com valor Nulo e qualidade de BAD ou. UNCERTAIN
 - `valueType`— Enumeração de {"B", "D", "S", "I"}
- `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](#).

CreateBulkImportJob API

Use a API `CreateBulkImportJob` 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

Dados anteriores a 1º de janeiro de 1970 00:00:00 UTC não são suportados.
Para identificar uma propriedade de 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 “Gerenciar streams de dados”](#).

- `ALIAS`: o alias que identifica a propriedade, como um caminho do fluxo de dados do servidor OPC UA (por exemplo, `/company/windfarm/3/turbine/7/temperature`). Para obter mais informações, consulte [Gerencie fluxos de dados para AWS IoT SiteWise](#).
- `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 AWS IoT SiteWise em massa (AWS CLI)

Use a operação de [CreateBulkImportJob](#) API para transferir dados do Amazon S3 para o AWS IoT SiteWise. A [CreateBulkImportJob](#) API permite a ingestão de grandes volumes de dados históricos e a ingestão em buffer de fluxos de dados analíticos em pequenos lotes. Ela oferece um primitivo econômico para ingestão de dados. O exemplo a seguir usa a 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 obter mais informações, consulte [Defina as configurações de armazenamento em AWS IoT SiteWise](#).

A [CreateBulkImportJob](#) API suporta a ingestão de dados históricos AWS IoT SiteWise com a opção de definir o `adaptive-ingestion-flag` parâmetro.

- Quando definido como `false`, a API ingere dados históricos sem acionar computações ou notificações.
- Quando definido como `true`, a API ingere novos dados, calcula métricas e transforma os dados para otimizar análises e notificações contínuas dentro de sete dias.

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

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

Exemplo Configuração do trabalho de importação em massa

Estes são exemplos das definições de configuração:

- Substitua *adaptive-ingestion-flag* por `true` ou `false`.
 - Se definido como `false`, o trabalho de importação em massa ingere dados históricos no 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 carimbo de data/hora dentro de sete dias.
- *delete-files-after-import-flag* `true` Substitua por `para` para excluir os dados do bucket de dados do Amazon S3 após a ingestão no armazenamento de nível AWS IoT SiteWise quente.
- Substitua `amzn-s3-demo-bucket` pelo *-for-errors* nome do bucket Amazon S3 para o qual os erros associados a esse trabalho de importação em massa são enviados.
- Substitua `amzn-s3-demo-bucket` pelo *-for-errors-prefix* prefixo do bucket 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 `amzn-s3-demo-bucket` pelo *-data* nome do bucket 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.
- *column-name* Substitua pelo nome da coluna especificado no arquivo.csv.
- *job-name* Substitua 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 `amzn-s3-demo-bucket` pelo *-data* nome do bucket Amazon S3 que contém seus dados. Além disso, *amzn-s3-demo-bucket-for-errors* substitua 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:::amzn-s3-demo-bucket-data",
          "arn:aws:s3:::amzn-s3-demo-bucket-data/*",
        ],
        "Effect": "Allow"
      },
      {
        "Action": [
          "s3:PutObject",
          "s3:GetObject",
          "s3:GetBucketLocation"
        ],
        "Resource": [
          "arn:aws:s3:::amzn-s3-demo-bucket-for-errors",
          "arn:aws:s3:::amzn-s3-demo-bucket-for-errors/*"
        ],
        "Effect": "Allow"
      }
    ]
  }
}

```

```

{
  "adaptiveIngestion": adaptive-ingestion-flag,
  "deleteFilesAfterImport": delete-files-after-import-flag,
  "errorReportLocation": {
    "bucket": "amzn-s3-demo-bucket-for-errors",
    "prefix": "amzn-s3-demo-bucket-for-errors-prefix"
  },
  "files": [
    {
      "bucket": "amzn-s3-demo-bucket-data",
      "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"
}
```

Descreva um trabalho de importação em AWS IoT SiteWise massa (AWS CLI)

Use a operação [DescribeBulkImportJob](#) da API para recuperar informações sobre um trabalho específico de importação em massa em AWS IoT SiteWise. Essa operação retorna detalhes, como status do trabalho, hora de criação e informações de erro em caso de falha no trabalho. Você pode usar essa operação para monitorar o progresso do trabalho e solucionar problemas. Para usar `DescribeBulkImportJob`, você precisa do ID do trabalho da operação `CreateBulkImportJob`. A API retorna as seguintes informações:

- Lista de arquivos que estão sendo importados, incluindo seus locais e chaves de bucket do Amazon S3
- Local do relatório de erros (se aplicável).
- Detalhes de configuração do trabalho, como formato de arquivo e nomes de colunas CSV.
- Carimbos de data/hora da criação do trabalho e da última atualização.
- Status atual do trabalho (por exemplo, se o trabalho está em andamento, concluído ou com falha).
- ARN do perfil do IAM para o trabalho de importação.

Para trabalhos concluídos, revise os resultados para confirmar a integração de dados bem-sucedida. Se um trabalho falhar, examine os detalhes do erro para realizar o diagnóstico e resolver os problemas.

job-ID Substitua pela ID do trabalho de importação em massa que você deseja recuperar.

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

Example Retorno

```
{
  "files":[
    {
      "bucket":"amzn-s3-demo-bucket1",
      "key":"100Tags12Hours.csv"
    },
    {
      "bucket":"amzn-s3-demo-bucket2",
      "key":"BulkImportData1MB.csv"
    },
    {
      "bucket":" amzn-s3-demo-bucket3",
      "key":"UnmodeledBulkImportData1MB.csv"
    }
  ],
  "errorReportLocation":{
    "prefix":"errors/",
    "bucket":"amzn-s3-demo-bucket-for-errors"
  },
  "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 AWS IoT SiteWise massa (AWS CLI)

Use a operação [ListBulkImportJobs](#) da API para recuperar uma lista de resumos para trabalhos de importação em massa em AWS IoT SiteWise. Essa operação oferece uma maneira eficiente de monitorar e gerenciar os processos de importação de dados. Ela retorna as seguintes informações importantes sobre cada trabalho:

- ID do trabalho. Um identificador exclusivo para cada trabalho de importação em massa.
- Nome do trabalho. O nome atribuído ao trabalho quando ele foi criado.
- Status atual. O estado atual do trabalho (por exemplo, CONCLUÍDO, EM EXECUÇÃO, COM FALHA)

`ListBulkImportJobs` é particularmente útil para obter uma visão geral abrangente de todos os seus trabalhos de importação em massa. Isso pode ajudar você a monitorar várias importações de dados, identificar trabalhos que exijam atenção e manter um fluxo de trabalho organizado. A operação oferece suporte à paginação, permitindo que você recupere um grande número de resumos de trabalhos de maneira eficiente. Você pode usar o trabalho IDs retornado por essa operação com a [DescribeBulkImportJob](#) operação para recuperar informações mais detalhadas sobre trabalhos específicos. Esse processo de duas etapas permite que você primeiro tenha uma visão geral de todos os trabalhos, depois se aprofunde nos detalhes dos trabalhos de interesse. Ao usar `ListBulkImportJobs`, você pode aplicar filtros para restringir os resultados. Por exemplo, você pode filtrar trabalhos com base no status para recuperar apenas trabalhos concluídos ou em execução. Esse recurso ajuda você a se concentrar nas informações mais relevantes para a tarefa atual. A operação também retornará um `nextToken` se houver mais resultados disponíveis. Você pode usar esse token em chamadas subsequentes para recuperar o próximo conjunto de resumos de trabalhos, permitindo que você repita todos os trabalhos de importação em massa, mesmo que tenha um grande número deles. O exemplo a seguir demonstra como usar `ListBulkImportJobs` com o AWS CLI para recuperar uma lista de trabalhos concluídos.

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

Example Resposta para filtro de trabalhos concluídos

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

Esse comando demonstra como usar `ListBulkImportJobs` para recuperar uma lista de trabalhos concluídos com falhas. O máximo está definido como 50 resultados e estamos usando uma opção de próximo token para resultados paginados.

```
aws iotsitewise list-bulk-import-jobs --filter COMPLETED_WITH_FAILURES --max-results 50
--next-token "string"
```

Ingerir dados para AWS IoT SiteWise usar 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 [BatchPutAssetPropertyValue](#) operação 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 apresenta as etapas necessárias para configurar uma regra que faz a ingestão de dados por meio de sombras de dispositivo, consulte [Ingira dados para AWS IoT SiteWise extrair coisas AWS IoT](#).

Você também pode enviar dados AWS IoT SiteWise de outros AWS serviços. Para obter mais informações, consulte [Interaja com outros AWS serviços](#).

Tópicos

- [AWS IoT Conceda o acesso necessário](#)
- [Configurar a ação da AWS IoT SiteWise regra](#)
- [Reduza custos com o Basic Ingest em AWS IoT SiteWise](#)

AWS IoT Conceda 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 `Condition` da política para conceder acesso a todos os 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": "*"
    }
  ]
}
```

Configurar 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. É possível fazer upload de várias entradas de dados em diferentes propriedades de ativo ao mesmo tempo a fim de enviar atualizações a 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 de ativo e o

ID de propriedade usando o Console do AWS IoT SiteWise. Se você souber o ID do ativo, poderá usar o AWS CLI to call [DescribeAsset](#) para 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 [Gerencie fluxos de dados para AWS IoT SiteWise](#).

Para o carimbo de data/hora em cada entrada, use o carimbo de data/hora informado pelo seu equipamento ou o carimbo de data/hora informado pelo 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 timestamp. Para obter 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](#)
- [Conversão de time stamps em formato de string](#)
- [Convertendo strings de time stamp de precisão de nanossegundos](#)
- [Configurações de regra de exemplo](#)
- [Solucionar problemas de ação de regra do](#)

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 o sensor ou equipamento informar dados de tempo 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 obter 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 sua ação da regra. Você pode criar uma AWS Lambda função que converta o timestamp de uma string em Time in seconds (**`timeInSeconds`**) e Offset in nanos (`offsetInNanos`). Depois, use [aws_lambda\(functionArn, inputJson\)](#) nos parâmetros de ação de regra para invocar essa função do Lambda e usar a saída na regra.

Note

Esta seção contém instruções avançadas que presumem que você esteja familiarizado com como criar os recursos a seguir:

- Funções do Lambda. Para ter mais informações, consulte [Criar sua primeira função do Lambda](#) no Guia do desenvolvedor do AWS Lambda .
- AWS IoT regras com a ação da AWS IoT SiteWise regra. Para obter mais informações, consulte [Ingerir dados para AWS IoT SiteWise usar 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 runtime Python 3, como o Python 3.11 (python3.11).
- Permissões — Crie uma função com permissões básicas do Lambda () AWS LambdaBasicExecutionRole.
- Camadas — Adicione a AWS SDKPandascamada -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 timestamp não estiverem no formato ISO 8601, você pode implementar uma solução com pandas que define o formato do timestamp. Para obter mais informações, consulte [pandas.to_datetime](https://pandas.pydata.org/pandas-docs/stable/timeseries.html#timeseries-timestamp-convert).

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 AWS da 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 [Solucionar 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 esse exemplo para definir uma regra para a ingestão de dados do tipo duplo em todas as turbinas eólicas de 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 mensagem a seguir ao alias de propriedade de uma 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 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 mensagem a seguir a `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 obter mais informações, consulte [Solucionar problemas de uma ação de AWS IoT SiteWise regra](#).

Reduza custos com o Basic Ingest em AWS IoT SiteWise

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.

Ingira dados de AWS IoT SiteWiseAWS 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.

Note

Aviso de fim do suporte: em 20 de maio de 2026, AWS encerrará o suporte para AWS IoT Events. Depois de 20 de maio de 2026, você não poderá mais acessar o AWS IoT Events console ou os AWS IoT Events recursos. Para obter mais informações, consulte [AWS IoT Events Fim do suporte](#).

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 alterações, anomalias ou condições específicas em toda a frota de IoT.
- Aumente a eficiência operacional e permita o gerenciamento proativo do 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. Ela também pode capacitar você com insights práticos.

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](#)

Use o gerenciador de AWS IoT Greengrass stream em AWS IoT SiteWise

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 colem 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 console do AWS IoT SiteWise . 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 obter mais informações, consulte [Use gateways AWS IoT SiteWise Edge](#).

Para ter mais informações sobre como configurar um destino para dados da fonte local, consulte [AWS IoT SiteWise Entenda os destinos Edge](#).

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

- [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](#)

Use gateways AWS IoT SiteWise Edge

AWS IoT SiteWise O Edge estende os recursos de nuvem para ambientes industriais periféricos, permitindo o processamento, a análise e a tomada de decisões locais de dados. SiteWise O Edge se integra AWS IoT SiteWise a outros AWS serviços para fornecer soluções abrangentes de IoT industrial. Os gateways servem como intermediários entre seu equipamento industrial e AWS IoT SiteWise.

SiteWise Os gateways Edge são executados em dois destinos de implantação diferentes:

- AWS IoT Greengrass V2
- Siemens Industrial Edge

Você pode usar um gateway SiteWise Edge para coletar dados na borda e publicá-los na nuvem. Para gateways em execução AWS IoT Greengrass, você também pode processar dados na borda usando modelos e ativos de ativos.

O aplicativo AWS IoT SiteWise Edge on Siemens Industrial Edge suporta a integração entre equipamentos industriais AWS IoT SiteWise para que você possa agregar e processar dados brutos da máquina e executar análises localmente antes de enviar dados refinados para a AWS nuvem.

Conceitos-chave dos gateways SiteWise Edge

SiteWise O Edge tem vários recursos úteis para computação de ponta em ambientes industriais.

Coleta e processamento de dados locais

Oferece suporte à coleta de dados de ativos industriais usando protocolos como OPC-UA e MQTT. Os gateways são executados em dispositivos AWS IoT Greengrass Core ou Siemens Industrial Edge.

Operação off-line

Continua coletando e processando dados durante interrupções na Internet, sincronizando com a nuvem quando a conectividade é restaurada.

Computação de ponta com AWS IoT Greengrass componentes

Usa o SiteWise editor de IoT para encaminhar dados para a nuvem e para o AWS IoT SiteWise processador para transformações e cálculos locais. Tanto o editor quanto o processador são

AWS IoT Greengrass V2 componentes. Para obter mais informações sobre AWS IoT Greengrass componentes, consulte [componentes AWS fornecidos](#).

Integração com AWS IoT SiteWise para ampliar os recursos de nuvem

Funciona com os recursos da AWS IoT SiteWise nuvem, estendendo modelos de ativos, análises e painéis até o limite.

Para gateways com um pacote de processamento de dados ativado, você pode usar AWS OpsHub for AWS IoT SiteWise para gerenciar centralmente seus gateways SiteWise Edge. AWS OpsHub fornece recursos de gerenciamento e monitoramento remotos. Para obter mais informações, consulte [Gerencie gateways SiteWise Edge usando AWS OpsHub para AWS IoT SiteWise](#).

Integração de fontes de dados de parceiros

Conecte uma fonte de dados de parceiro ao seu gateway e receba dados do parceiro em seu gateway SiteWise Edge e na AWS nuvem. Para obter mais informações, consulte [Fontes de dados de parceiros nos gateways SiteWise Edge](#).

Visualização local na borda

Fornecer painéis personalizados para insights em tempo real na borda.

Monitore os dados localmente em suas instalações usando os portais SiteWise Monitor em seus dispositivos locais. Para obter mais informações, consulte [Habilitando seu AWS IoT SiteWise portal na borda](#).

Benefícios da implementação do SiteWise Edge

SiteWise O Edge oferece inúmeras vantagens que podem melhorar significativamente as operações industriais e os processos de tomada de decisão.

- Informações operacionais em tempo real sem atrasos no processamento da nuvem
- Continuidade operacional em ambientes desconectados
- Custos reduzidos de largura de banda e armazenamento por meio do pré-processamento de borda
- Maior confiabilidade com a capacidade de tomar decisões locais baseadas em dados

Hospede automaticamente um gateway AWS IoT SiteWise Edge com AWS IoT Greengrass V2

Configure o AWS IoT SiteWise Edge para coletar, processar e visualizar dados de equipamentos industriais localmente antes de enviá-los para a nuvem. Use AWS IoT Greengrass Version 2 de hospedagem própria.

Um gateway AWS IoT SiteWise Edge atua como intermediário entre seu equipamento industrial e AWS IoT SiteWise. Em execução AWS IoT Greengrass Version 2, o gateway SiteWise Edge oferece suporte à coleta e processamento de dados no local. Monitore os dados localmente em suas instalações por meio dos portais SiteWise Monitor em seus dispositivos locais com o pacote de processamento de dados ativado e AWS OpsHub instalado.

Há dois tipos de gateways auto-hospedados:

Gateway V3 habilitado para MQTT

A arquitetura de gateway V3 habilitada para MQTT fornece recursos aprimorados de ingestão de dados. Ele utiliza o protocolo MQTT para comunicação eficiente de dados e oferece destinos de dados configuráveis. Isso inclui opções para ingestão de dados em buffer usando o Amazon S3, bem como ingestão de dados em tempo real. Você pode implementar filtros de caminho para se inscrever em tópicos específicos do MQTT, permitindo a coleta de dados direcionada. Observe que o gateway V3 habilitado para MQTT não suporta o recurso Data Processing Pack. Para obter mais informações, consulte [Gateways V3 habilitados para MQTT para Edge AWS IoT SiteWise](#).

Streams clássicos, gateway V2

O gateway Classic Streams, V2, representa a arquitetura tradicional do gateway AWS IoT SiteWise Edge. É adequado para implantações existentes do SiteWise Edge e usuários acostumados com o fluxo de trabalho estabelecido. Embora o Classic streams, o gateway V2 ofereça suporte ao pacote de processamento de dados, observe que os dados gerados pelo pacote de processamento de dados não podem ser ingeridos por meio do Amazon S3. Use o gateway Classic Streams V2 se precisar manter a compatibilidade com implantações existentes ou se precisar da funcionalidade do pacote de processamento de dados. Para obter mais informações, consulte [Streams clássicos, gateways V2 para Edge AWS IoT SiteWise](#).

Tópicos

- [AWS IoT SiteWise Requisitos de gateway auto-hospedado do Edge](#)

- [Crie um gateway SiteWise Edge auto-hospedado](#)
- [Instale o software AWS IoT SiteWise Edge Gateway em seu dispositivo local](#)
- [Gateways V3 habilitados para MQTT para Edge AWS IoT SiteWise](#)
- [Streams clássicos, gateways V2 para Edge AWS IoT SiteWise](#)
- [Adicione fontes de dados ao seu gateway AWS IoT SiteWise Edge](#)
- [AWS IoT Greengrass componentes para AWS IoT SiteWise Edge](#)
- [Filtrar ativos em um gateway SiteWise Edge](#)
- [Configure o suporte de proxy e gerencie repositórios confiáveis para o AWS IoT SiteWise Edge](#)
- [Use AWS IoT SiteWise APIs na borda](#)

AWS IoT SiteWise Requisitos de gateway auto-hospedado do 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, crie um gateway no Nuvem AWS e execute o software SiteWise Edge gateway para configurar seu dispositivo local. Quando você usa o AWS Management Console para criar o gateway SiteWise Edge, um script de instalação é fornecido. Execute esse script em seu dispositivo de gateway de destino para configurar o software e as dependências necessários.

Requisitos locais do dispositivo

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

- Compatível com 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:

- SO: 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.

- No mínimo 4 GB de RAM.
- Espaço mínimo de 10 GB em disco disponível para o software SiteWise Edge Gateway.
- Configure seu dispositivo local para garantir que as portas adequadas estejam acessíveis. 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](#).
- Ambiente de Execução Java (JRE) versão 11 ou posterior. 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). É recomendável usar o [Amazon Corretto](#) ou o [OpenJDK](#).

Buckets do Amazon S3 para lista de permissões para dispositivos locais

Configure seu dispositivo local para fornecer acesso por firewall ao seguinte bucket do Amazon S3. Configure o acesso com base nas respectivas regiões dos seus dispositivos.

Região	Endpoint
Ásia-Pacífico (Tóquio)	https://iot-sitewise-gateway-ap-northeast-1-785558802005.s3.ap-northeast-1.amazonaws.com
Ásia-Pacífico (Seul)	https://iot-sitewise-gateway-ap-northeast-2-310055672453.s3.ap-northeast-2.amazonaws.com

Região	Endpoint
Ásia-Pacífico (Mumbai)	https://iot-sitewise-gateway-ap-south-1-677656657204.s3.ap-south-1.amazonaws.com
Ásia-Pacífico (Singapura)	https://iot-sitewise-gateway-ap-southeast-1-475191558554.s3.ap-southeast-1.amazonaws.com
Ásia-Pacífico (Sydney)	https://iot-sitewise-gateway-ap-southeast-2-396319432685.s3.ap-southeast-2.amazonaws.com
Canadá (Central)	https://iot-sitewise-gateway-ca-central-1-842060018567.s3.ca-central-1.amazonaws.com
China (Pequim)	https://iot-sitewise-gateway-cn-north-1-237124890262.s3.cn-north-1.amazonaws.com.cn
Europa (Frankfurt)	https://iot-sitewise-gateway-eu-central-1-748875242063.s3.eu-central-1.amazonaws.com
Europa (Irlanda)	https://iot-sitewise-gateway-eu-west-1-383414315062.s3.eu-west-1.amazonaws.com
Leste dos EUA (Norte da Virgínia)	https://iot-sitewise-gateway-us-east-1-223558168232.s3.us-east-1.amazonaws.com https://iot-sitewise-gateway-us-east-1-223558168232.s3.amazonaws.com/
Leste dos EUA (Ohio)	https://iot-sitewise-gateway-us-east-2-005072661813.s3.us-east-2.amazonaws.com
AWS GovCloud (Oeste dos EUA)	https://iot-sitewise-gateway-us-gov-west-1-599984565679.s3.us-gov-west-1.amazonaws.com/
Oeste dos EUA (Oregon)	https://iot-sitewise-gateway-us-west-2-502577205460.s3.us-west-2.amazonaws.com

Requisitos do pacote de processamento de dados

- Se você planeja usar o pacote de processamento de 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 Microsoft Windows.
 - Ter pelo menos 256 GB de espaço livre em disco.
 - O dispositivo local deve permitir tráfego de entrada da rede na porta 443.
 - 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 ter mais informações, consulte [Configuração](#) no Guia do desenvolvedor do AWS IoT Greengrass Version 2 .

- Os requisitos mínimos de espaço em disco e capacidade computacional dependem de uma grande variedade de fatores exclusivos da implementação e do 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

Configurar permissões para usar gateways SiteWise Edge

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 das permissões

O perfil 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": "*"
}
```

Crie um gateway SiteWise Edge auto-hospedado

Use o AWS IoT SiteWise console ou AWS CLI para criar um gateway SiteWise Edge auto-hospedado. 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, consulte [Hospede um gateway SiteWise Edge em Siemens Industrial Edge](#).

Crie um gateway SiteWise Edge

Console

1. Navegue até o [console do AWS IoT SiteWise](#).
2. No painel de navegação, escolha Gateways de borda.
3. Escolha Criar gateway.
4. Em Escolher destino de implantação, escolha gateway auto-hospedado.
5. Selecione Gateway V3 habilitado para MQTT ou Streams clássicos, gateway V2. Para obter mais informações sobre cada opção, consulte [Hospede automaticamente um gateway AWS](#)

[IoT SiteWise Edge com AWS IoT Greengrass V2](#). O gateway V3 habilitado para MQTT é recomendado por seus recursos prontos para o futuro.

6. Na seção Configuração do gateway, insira um nome para seu gateway SiteWise Edge ou use o nome gerado por AWS IoT SiteWise.
7. 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 só está disponível em plataformas x86. Ele está disponível apenas nos streams clássicos, gateway V2

8. (Opcional) Para processar e organizar dados na borda, em Recursos de borda, 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 a capacidade de borda no SiteWise Edge](#)

9. (Opcional) Em 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 você quiser usar um dispositivo de núcleo do Greengrass existente ou criar um manualmente.
 1. Escolha um dispositivo principal do Greengrass ou escolha Criar dispositivo principal do Greengrass para criar um no console. AWS IoT Greengrass V2 Para obter mais informações, consulte [Configurar dispositivos principais do AWS IoT Greengrass V2](#) no Guia do desenvolvedor do AWS IoT Greengrass Version 2 .
10. Escolha Criar gateway.

11. 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**

Você não pode regenerar esse arquivo. Não se esqueça de salvar o arquivo do instalador em um local seguro, pois você vai usá-lo depois.

AWS CLI

Para criar um gateway auto-hospedado usando o AWS CLI, forneça um nome para o gateway, especifique a plataforma e a versão do gateway. Há muitas outras opções que você pode especificar ao criar um gateway. Para obter mais informações, consulte [create-gateway](#) na Referência de Comandos para AWS CLI AWS IoT SiteWise

Para usar esse exemplo, substitua os espaços reservados para entrada do usuário por suas próprias informações.

```
aws iotsitewise create-gateway \
  --gateway-name your-gateway-name \
  --gateway-platform greengrassV2={coreDeviceThingName=your-core-device-thing-name, coreDeviceOperatingSystem=LINUX_AMD64} \
  --gateway-version 3 \
  [--cli-input-json your-configuration]
```

- `gateway-name`— Um nome exclusivo para o gateway.
- `gateway-platform`— Especifica a configuração da plataforma de gateway. Para gateways auto-hospedados, insira `greengrassV2`. Para obter mais informações, consulte [Opções](#) na seção `create-gateway` do AWS CLI Command Reference for AWS IoT SiteWise
- `coreDeviceThingName`— O nome da AWS IoT para seu dispositivo AWS IoT Greengrass V2 principal.
- `coreDeviceOperatingSystem`— O sistema operacional do dispositivo principal em AWS IoT Greengrass V2. A especificação do sistema operacional é necessária `gateway-version 3` e não aplicável `paragateway-version 2`. As opções incluem: `LINUX_AARCH64`, `LINUX_AMD64`, e `WINDOWS_AMD64`

- `gateway-version`— A versão do gateway.
 - Para criar um gateway V3 habilitado para MQTT, use 3 para a versão do gateway.
 - Para criar fluxos clássicos, gateway V2, use 2 para a versão do gateway.
- `cli-input-json`— Um arquivo JSON contendo parâmetros de solicitação.

Agora que você criou o gateway SiteWise Edge, [instale o software AWS IoT SiteWise Edge Gateway em seu dispositivo local](#).

Instale o software AWS IoT SiteWise Edge Gateway em seu dispositivo local

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

Important

Verifique se o dispositivo local está conectado à internet.

Linux

O procedimento a seguir usa SSH para estabelecer conexão com o dispositivo local. Você também pode usar uma unidade flash USB ou outras ferramentas para transferir o arquivo 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

Para se conectar ao dispositivo usando SSH, cumpra os pré-requisitos a seguir.

- 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 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 *username* e por um nome de usuário *IP* 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.
- *IP-address* Substitua 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:

- Microsoft WindowsServer 2019 ou posterior instalado
- Privilégios de administrador
- PowerShell versão 5.1 ou posterior instalada
- SiteWise O instalador do gateway Edge foi 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 PowerShell na 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
```

A próxima etapa depende do tipo de gateway auto-hospedado que você precisa. Continue para [Gateways V3 habilitados para MQTT para Edge AWS IoT SiteWise](#) ou [Streams clássicos, gateways V2 para Edge AWS IoT SiteWise](#).

Gateways V3 habilitados para MQTT para Edge AWS IoT SiteWise

AWS IoT SiteWise pode usar gateways V3 habilitados para MQTT, representando um avanço significativo na arquitetura do gateway Edge. SiteWise Esse tipo de gateway aproveita o protocolo MQTT (Message Queuing Telemetry Transport) para comunicação de dados, fornecendo maior flexibilidade e eficiência em implantações industriais de IoT.

O gateway V3 habilitado para MQTT usa o MQTT para transferência de dados, permitindo um protocolo de rede leve de publicação e assinatura que transporta mensagens de forma eficiente entre dispositivos e a nuvem. Você pode configurar vários destinos de dados, incluindo ingestão de dados em tempo real diretamente no Amazon AWS IoT SiteWise S3 e ingestão de dados em buffer. Para permitir a coleta precisa de dados, você pode implementar filtros de caminho para se inscrever em tópicos específicos do MQTT.

Os gateways V3 habilitados para MQTT vêm com um destino pré-configurado em tempo real com filtros definidos como “#” (todos os tópicos), que você pode personalizar ou remover conforme necessário. Para simplificar o gerenciamento de dados, somente um destino em tempo real pode existir em cada gateway.

A arquitetura habilitada para MQTT difere significativamente dos fluxos clássicos, gateway V2. Enquanto a V2 usa uma abordagem baseada em fluxo, a V3 emprega o MQTT, oferecendo destinos de dados e opções de filtragem mais configuráveis. No entanto, observe que a V3 não oferece suporte ao pacote de processamento de dados, que está disponível na V2.

O gateway V3 habilitado para MQTT oferece várias vantagens:

- Escalabilidade aprimorada, devido à natureza leve do MQTT, permitindo melhor manuseio de vários dispositivos e transmissão de dados de alta frequência.
- Controle de dados aprimorado por meio de filtros de caminho, permitindo o gerenciamento granular da coleta de dados e reduzindo a transferência e o processamento desnecessários de dados.

- Manipulação flexível de dados, permitindo a configuração entre processamento em tempo real e armazenamento em buffer com base em necessidades específicas.
- Alinhamento com os padrões modernos de comunicação de IoT, preparando o terreno para futuras melhorias e integrações.

Considere adotar o gateway V3 habilitado para MQTT para novas implantações, especialmente quando você precisar de opções flexíveis de ingestão de dados e controle preciso sobre a coleta de dados.

 Note

Para implantações ou cenários existentes que exigem o pacote de processamento de dados, o Classic Streams, o gateway V2 continua sendo uma opção viável.

Ao oferecer os dois tipos de gateway, AWS IoT SiteWise garante que você possa escolher a solução que melhor atenda às suas necessidades específicas de IoT industrial, independentemente de você priorizar recursos avançados de MQTT ou compatibilidade com sistemas existentes.

Destinos e filtros de caminho

Veja os tópicos a seguir para saber mais sobre destinos e filtros de caminho em gateways habilitados para MQTT:

- [AWS IoT SiteWise Entenda os destinos Edge](#)
- [Adicione um destino em tempo real do AWS IoT SiteWise Edge](#)
- [Adicione um destino em AWS IoT SiteWise buffer usando o Amazon S3](#)
- [Entenda os filtros de caminho para destinos AWS IoT SiteWise do Edge](#)
- [Adicione filtros de caminho aos destinos AWS IoT SiteWise do Edge](#)
- [Gerenciar destinos AWS IoT SiteWise do Edge](#)

Conecte aplicativos externos ao corretor EMQX

Este guia explica como conectar aplicativos externos ao seu gateway AWS IoT SiteWise Edge por meio de um agente EMQX em seu gateway V3 implantado e habilitado para MQTT. Os aplicativos

externos podem incluir ferramentas de monitoramento personalizadas, software de visualização de terceiros ou sistemas legados que precisam interagir com seus dados industriais na borda.

Abordaremos as etapas de configuração para Linux e Microsoft Windows ambientes, incluindo configuração de implantação do EMQX, configuração de TLS para conexões seguras e regras de autorização para controlar o acesso a tópicos específicos.

Note

A EMQX não é fornecedora nem fornecedora do Edge. AWS IoT SiteWise

Important

Para proteger as conexões com seu gateway, é altamente recomendável usar a autenticação baseada em certificado por meio do recurso de autenticação do dispositivo AWS IoT Greengrass cliente. Esse método fornece segurança robusta por meio da autenticação TLS mútua (mTLS). Para obter mais informações, consulte [Conectar dispositivos cliente a dispositivos principais](#) no Guia do AWS IoT Greengrass Version 2 desenvolvedor.

Se você não conseguir usar a autenticação baseada em certificado, siga este guia para configurar a autenticação usando nomes de usuário e senhas.

Pré-requisitos

- Um gateway V3 compatível com SiteWise Edge MQTT que foi implantado e está on-line
- Acesso ao host do gateway
- Acesso aos AWS IoT Greengrass consoles AWS IoT SiteWise e

Tópicos

- [Formato de carga útil de mensagem para o corretor EMQX no Edge AWS IoT SiteWise](#)
- [Configurar o corretor EMQX](#)
- [Conecte um aplicativo ao corretor EMQX no Edge AWS IoT SiteWise](#)
- [Configurar regras de autorização para o AWS IoT SiteWise Edge no EMQX](#)

Formato de carga útil de mensagem para o corretor EMQX no Edge AWS IoT SiteWise

Para que o componente do SiteWise editor de IoT consuma dados do seu aplicativo externo e os publique AWS IoT SiteWise na nuvem, a carga útil enviada ao agente deve atender a requisitos específicos.

Compreender o formato da carga útil é fundamental para uma comunicação bem-sucedida do MQTT com AWS IoT SiteWise o Edge. Embora o processo de configuração da conexão seja abordado nas seções posteriores, apresentaremos primeiro os requisitos de carga útil para ajudá-lo a planejar sua implementação.

Requisitos de tópicos do MQTT

Não há restrições na estrutura de tópicos do MQTT, incluindo o número de níveis ou caracteres usados. No entanto, recomendamos que o tópico corresponda ao `propertyAlias` campo na carga.

Example Exemplo de alias de propriedade

Se o tópico do MQTT `forsite1/line1/compressor1/temperature`, garanta as `propertyAlias` correspondências.

```
{
  "assetId": "compressor_asset_01",
  "propertyAlias": "site1/line1/compressor1/temperature",
  "propertyId": "temperature_sensor_01",
  "propertyValues": [
    {
      "quality": "GOOD",
      "timestamp": {
        "offsetInNanos": 0,
        "timeInSeconds": 1683000000
      },
      "value": {
        "doubleValue": 23.5
      }
    }
  ]
}
```

Estrutura de carga útil JSON

[A carga útil da mensagem MQTT é escrita em JSON e segue o formato de PutAssetPropertyValueEntry mensagem definido na Referência da AWS IoT SiteWise API.](#)

```
{
  "assetId": "string",
  "propertyAlias": "string",
  "propertyId": "string",
  "propertyValues": [
    {
      "quality": "string",
      "timestamp": {
        "offsetInNanos": number,
        "timeInSeconds": number
      },
      "value": {
        "booleanValue": boolean,
        "doubleValue": number,
        "integerValue": number,
        "stringValue": "string"
      }
    }
  ]
}
```

Note

Para que uma mensagem seja considerada válida, somente uma das seguintes condições pode ser verdadeira:

- O `propertyAlias` está definido, ou
- Ambos `assetId` `propertyId` estão definidos

O `PutAssetPropertyValueEntry` tem um `entryId` campo que não é obrigatório neste contexto.

Configurar o corretor EMQX

Esta seção aborda como adicionar nomes de usuário e senhas. Também aborda como estabelecer uma conexão TLS de uma fonte externa usando o nome de usuário e a senha adicionados. Você pode configurar o corretor EMQX usando Linux ou Microsoft Windows

 Note

Para configurar o broker, você precisa de um dispositivo principal configurado com a configuração EMQX padrão em seu gateway V3 habilitado para MQTT.

 Important

Depois de concluir esse procedimento, é altamente recomendável configurar as regras de autorização. Para obter mais informações, consulte [Configurar regras de autorização para o AWS IoT SiteWise Edge no EMQX](#). As regras de autorização para usuários adicionais aumentam a segurança.

Atualize a configuração de implantação do EMQX para autenticação

Para atualizar a configuração de implantação do EMQX para autenticação

1. Navegue até o [console do AWS IoT SiteWise](#).
2. Na navegação à esquerda, escolha Gateways Edge na seção Edge.
3. Escolha o gateway a ser configurado.
4. Na seção Configuração do gateway Edge, copie o valor do seu dispositivo principal do Greengrass. Guarde-o para uso posterior.
5. Abra o [console de AWS IoT](#).
6. No painel de navegação à esquerda, na seção Gerenciar, escolha dispositivos Greengrass e, em seguida, Implantações.
7. Encontre o valor do dispositivo principal que você salvou anteriormente e escolha esse link para abrir a implantação.
8. Escolha o botão suspenso Ações e, em seguida, Revisar.
9. Leia a mensagem que aparece e escolha Revisar implantação. A página Especificar destino é exibida.
10. Escolha Avançar até chegar à etapa Configurar componentes.
11. Selecione o botão `aws.greengrass.clientdevices.mqtt.EMQX` de rádio.
12. Escolha o botão Configurar componente. Uma página de configuração é exibida para o componente.

13. Em Atualização de configuração, escolha Redefinir a configuração padrão para a versão do componente: 2.*.*.
14. Insira a seguinte configuração na seção Configuração para mesclar com base em seu sistema operacional.

Linux

```
{
  "emqxConfig": {
    "authorization": {
      "no_match": "allow"
    },
    "listeners": {
      "tcp": {
        "default": {
          "enabled": true,
          "enable_authn": false
        }
      },
      "ssl": {
        "default": {
          "enabled": true,
          "enable_authn": true,
          "ssl_options": {
            "verify": "verify_none",
            "fail_if_no_peer_cert": false
          }
        }
      }
    },
    "authentication": {
      "enable": true,
      "backend": "built_in_database",
      "mechanism": "password_based",
      "password_hash_algorithm": {
        "iterations": 210000,
        "mac_fun": "sha512",
        "name": "pbkdf2"
      },
      "user_id_type": "username"
    },
    "dashboard": {
      "listeners": {
```

```

        "http": {
            "bind": 18083
        }
    },
    "authMode": "bypass",
    "dockerOptions": "-p 8883:8883 -p 127.0.0.1:1883:1883\n-p 127.0.0.1:18083:18083 -v emqx-data:/opt/emqx/data -e\nEMQX_NODE__NAME=emqx@local",
    "requiresPrivilege": "true"
}

```

Windows

```

{
  "emqxConfig": {
    "authorization": {
      "no_match": "allow"
    },
    "listeners": {
      "tcp": {
        "default": {
          "enabled": true,
          "enable_authn": false
        }
      },
      "ssl": {
        "default": {
          "enabled": true,
          "enable_authn": true,
          "ssl_options": {
            "verify": "verify_none",
            "fail_if_no_peer_cert": false
          }
        }
      }
    },
    "authentication": {
      "enable": true,
      "backend": "built_in_database",
      "mechanism": "password_based",
      "password_hash_algorithm": {

```

```
        "iterations": 210000,  
        "mac_fun": "sha512",  
        "name": "pbkdf2"  
    },  
    "user_id_type": "username"  
},  
"dashboard": {  
    "listeners": {  
        "http": {  
            "bind": 18083  
        }  
    }  
}  
},  
"authMode": "bypass",  
"requiresPrivilege": "true"  
}
```

O `dockerOptions` campo é somente para gateways Linux.

15. Escolha Confirmar.
16. Escolha Avançar até chegar à etapa de revisão.
17. Escolha Implantar.
18. Depois que a implantação for bem-sucedida, vá para a próxima etapa.

Ativar autenticação de nome de usuário e senha

Esta seção mostra como adicionar nomes de usuário e senhas por meio da GUI do painel do EMQX.

Note

As instruções relacionadas ao EMQX fornecidas são apenas para referência. Como a documentação e os recursos do EMQX podem mudar com o tempo e não mantemos sua documentação, recomendamos consultar a [documentação oficial do EMQX para obter](#) as informações mais atuais.

EMQX Dashboard

Para habilitar a autenticação de nome de usuário e senha por meio do painel do EMQX

1. Verifique se você está dentro do host do gateway.
2. Abra uma janela do navegador e acesse <http://localhost:18083/>.
3. Insira o nome de usuário padrão **admin** e a senha padrão **public**. Para obter mais informações, consulte [Painel do EMQX na documentação do EMQX](#).
4. Após o login, você será solicitado a alterar sua senha. Atualize sua senha para continuar no painel do EMQX.
5. Na navegação à esquerda, escolha o ícone de escudo e, em seguida, Autenticação.
6. Na linha Banco de dados incorporado, escolha o botão Usuários.
7. Escolha o botão do ícone do sinal de adição para adicionar usuários. Uma tela Adicionar é exibida.
8. Insira um nome de usuário e uma senha para o usuário do aplicativo externo.
9. Escolha Salvar. O nome de usuário que você escolheu aparece na tabela da página Autenticação.

Note

As regras de autorização existentes ou padrão se aplicam ao novo usuário. É recomendável revisá-los e ajustá-los às necessidades de seus aplicativos externos.

EMQX Management with Linux

Use a ferramenta AWS IoT SiteWise EMQX CLI em. `/greengrass/v2/bin/swe-emqx-cli`

Para habilitar a autenticação de nome de usuário e senha por meio do EMQX Management usando Linux

1. Altere a senha do administrador executando o seguinte comando:

```
/greengrass/v2/bin/swe-emqx-cli admin change-pwd
```

2. Quando solicitado, faça o seguinte:

1. Digite seu usuário administrador atual (o padrão é `admin`) e a senha (o padrão é `public`).
2. Digite e confirme sua nova senha.

Se for bem-sucedido, você verá a seguinte mensagem:

```
admin password changed successfully
```

3. Adicione usuários para aplicativos externos executando o seguinte comando:

```
/greengrass/v2/bin/swe-emqx-cli users add
```

4. Quando solicitado, faça o seguinte:
 1. Insira o nome de usuário do novo usuário.
 2. Digite e confirme a senha do novo usuário.

Se for bem-sucedido, você verá a seguinte mensagem:

```
User '[username]' created successfully
```

5. Verifique a configuração do usuário executando o seguinte comando:

```
/greengrass/v2/bin/swe-emqx-cli users list
```

A saída mostra todos os usuários configurados:

```
Users:  
- [your-added-username]  
  
Total users: 1
```

EMQX Management with Windows

Use a ferramenta AWS IoT SiteWise CLI EMQX em um dos seguintes locais:

- PowerShell: `C:\greengrass\v2\bin\swe-emqx-cli.ps1`
- Prompt de comando: `C:\greengrass\v2\bin\swe-emqx-cli.bat`

Para habilitar a autenticação de nome de usuário e senha por meio do EMQX Management usando o Windows

1. Altere a senha do administrador executando o seguinte comando:

```
C:\greengrass\v2\bin\swe-emqx-cli.ps1 admin change-pwd
```

2. Quando solicitado, faça o seguinte:

1. Digite seu usuário administrador atual (o padrão é `admin`) e a senha (o padrão é `public`).
2. Digite e confirme sua nova senha.

Se for bem-sucedido, você verá a seguinte mensagem:

```
admin password changed successfully
```

3. Adicione usuários para aplicativos externos executando o seguinte comando:

```
C:\greengrass\v2\bin\swe-emqx-cli.ps1 users add
```

4. Quando solicitado, faça o seguinte:

1. Insira o nome de usuário do novo usuário.
2. Digite e confirme a senha do novo usuário.

Se for bem-sucedido, você verá a seguinte mensagem:

```
User '[username]' created successfully
```

5. Verifique a configuração do usuário executando o seguinte comando:

```
C:\greengrass\v2\bin\swe-emqx-cli.ps1 users list
```

A saída mostra todos os usuários configurados:

```
Users:
- [your-added-username]

Total users: 1
```

Conecte um aplicativo ao corretor EMQX no Edge AWS IoT SiteWise

O agente EMQX usa Transport Layer Security (TLS) na porta 8883 para criptografar todas as comunicações, garantindo que seus dados permaneçam protegidos durante a transmissão. Esta seção mostra as etapas para estabelecer conexões entre seus aplicativos e o corretor EMQX. Seguir essas etapas ajuda a manter a integridade e a confidencialidade de seus dados industriais. O processo de conexão envolve duas abordagens principais: usar a descoberta automática de IP por meio de componentes ou configurar manualmente nomes DNS e endereços IP como nomes alternativos de assunto (SANs) em seus certificados TLS. Cada método tem suas próprias vantagens, dependendo da configuração da rede e dos requisitos de segurança. Esta documentação o guiará pelas duas opções.

Tópicos

- [Configure o TLS para conexões seguras com o agente EMQX no Edge AWS IoT SiteWise](#)
- [Teste a conexão do agente EMQX no Edge AWS IoT SiteWise](#)
- [Use sua própria CA](#)
- [Abra a porta 8883 para conexões externas de firewall](#)

Configure o TLS para conexões seguras com o agente EMQX no Edge AWS IoT SiteWise

Por padrão, AWS IoT Greengrass gera um certificado de servidor TLS para o agente EMQX que é assinado pela autoridade de certificação (CA) do dispositivo principal. Para obter mais informações, consulte [Conectando dispositivos cliente a um dispositivo AWS IoT Greengrass Core com um agente MQTT](#).

Recupere o certificado TLS

Para obter o certificado CA, execute o seguinte comando no host do gateway:

Linux

Execute o seguinte comando em uma sessão de shell no host do gateway:

```
/greengrass/v2/bin/swe-emqx-cli cert
```

Esse comando exibe a localização do certificado e imprime o conteúdo do certificado.

Como alternativa, você pode salvar o certificado em um arquivo usando este comando:

```
/greengrass/v2/bin/swe-emqx-cli cert --output /path/to/certificate.pem
```

Windows

Execute o seguinte comando em uma PowerShell sessão no host do gateway:

```
C:\greengrass\v2\bin\swe-emqx-cli.ps1 cert
```

Esse comando exibe a localização do certificado e imprime o conteúdo do certificado.

Como alternativa, você pode salvar o certificado em um arquivo usando este comando:

```
C:\greengrass\v2\bin\swe-emqx-cli.ps1 cert --output C:\path\to\certificate.pem
```

A CLI localiza automaticamente o certificado, independentemente do caminho exato em seu sistema.

Copie o conteúdo do arquivo ca.pem para o aplicativo externo que você está conectando ao broker. Salve-o como BrokerCoreDeviceCA.pem.

Adicione nomes DNS/endereços IP personalizados ao certificado do servidor TLS

O nome alternativo do assunto (SAN) no certificado gerado por AWS IoT Greengrass é localhost. Ao estabelecer uma conexão TLS de fora do host do gateway, a etapa de verificação do TLS falha porque o nome do host do broker não corresponde ao nome do host do certificado do localhost servidor.

Para resolver o problema de nomes de host incompatíveis, AWS IoT Greengrass fornece duas maneiras de gerenciar os endpoints principais do dispositivo. Esta seção aborda as duas opções. Para obter informações mais detalhadas, consulte [Gerenciar endpoints de dispositivos principais](#) no Guia do AWS IoT Greengrass Version 2 desenvolvedor.

- Para se conectar ao agente EMQX usando o endereço IP do dispositivo principal, use a seção [Descoberta automática de IP](#).
- Para se conectar ao agente EMQX usando um nome DNS em vez de um endereço IP, use a seção [Gerenciamento manual](#).

Automated IP discovery

Essa opção permite que seu dispositivo principal descubra automaticamente seu endereço IP e o adicione como um nome alternativo de assunto (SAN) ao certificado do intermediário.

1. Adicione o `aws.greengrass.clientdevices.IPDetector` componente à implantação do seu dispositivo principal.
2. Implemente as alterações em seu dispositivo
3. Aguarde a conclusão da implantação.

Depois que a implantação for concluída, você poderá estabelecer uma conexão TLS segura usando o endereço IP do agente.

O endereço IP é adicionado automaticamente como SAN ao certificado do agente.

Manual DNS and IP Configuration

Você pode adicionar manualmente nomes DNS e endereços IP como nomes alternativos de assunto (SANs) ao seu certificado TLS. Esse método é útil quando você configura um nome DNS para o host do gateway.

Important

Se você estiver usando o `IPDetector` componente, remova-o da implantação antes de continuar. O `IPDetector` componente substitui as configurações manuais do endpoint.

Para configurar manualmente os endpoints

1. Navegue até o [console do AWS IoT SiteWise](#).
2. Na navegação à esquerda, escolha Gateways Edge na seção Edge.
3. Escolha o gateway a ser configurado.
4. Na seção de configuração do gateway Edge, escolha a URL do seu dispositivo principal do Greengrass. A página do dispositivo principal é exibida.
5. Escolha a guia Dispositivos do cliente.
6. Escolha Gerenciar endpoints.

7. Na caixa de diálogo Gerenciar endpoints, insira o (s) nome (s) DNS e os endereços IP que você deseja adicionar como. SANs Use a porta 8883.
8. Selecione Atualizar.

O certificado do servidor TLS do corretor é atualizado automaticamente para incluir seus novos endpoints.

Para verificar a atualização do certificado do servidor TLS usando Linux

1. Inicie uma sessão de shell em seu host de gateway.

```
docker exec emqx openssl x509 -in ./data/cert.pem -text -noout | grep -A1  
"Subject Alternative Name"
```

2. O comando retorna uma saída semelhante à seguinte:

```
X509v3 Subject Alternative Name:  
DNS: endpoint_you_added, DNS:localhost
```

3. Verifique se seu endpoint aparece na lista de SANs.

Para verificar a atualização do certificado do servidor TLS usando o Windows

1. Inicie uma sessão de shell em seu host de gateway.

```
(Get-PfxCertificate -FilePath "C:\greengrass\v2\work  
\aws.greengrass.clientdevices.mqtt.EMQX\v2\data\cert.pem").Extensions | Where-  
Object { $_.Oid.FriendlyName -eq "Subject Alternative Name" } | ForEach-Object  
{ "Subject Alternative Name:", ($_.Format($true) -split "`n")[0..1] }
```

2. O comando retorna uma saída semelhante à seguinte:

```
Subject Alternative Name:  
DNS Name=your-endpoint  
DNS Name=localhost
```

3. Verifique se o endpoint que você adicionou está na lista de SANs.

Teste a conexão do agente EMQX no Edge AWS IoT SiteWise

Depois de configurar seu agente EMQX com certificados TLS e credenciais de autenticação, é importante verificar se sua configuração funciona corretamente. Testar a conexão ajuda a garantir que suas configurações de segurança sejam implementadas adequadamente e que os clientes possam estabelecer conexões criptografadas com o agente com êxito. Esta seção demonstra como testar a conexão do seu agente usando o cliente de interface de linha de comando (CLI) Mosquitto, uma ferramenta de cliente MQTT amplamente usada que oferece suporte à criptografia e autenticação TLS.

Use o cliente Mosquitto CLI para testar a conexão do agente EMQX

Nesta etapa, usaremos o cliente CLI do mosquitto para testar nossa configuração e garantir que possamos nos conectar com êxito ao corretor usando o nome de usuário e a senha que criamos anteriormente. Para obter `BrokerCoreDeviceCA.pem` as etapas a seguir, consulte a Etapa 3: Configurando o TLS.

```
mosquitto_sub -h hostname/ip address \  
  -p 8883 \  
  -t "#" \  
  -q 1 \  
  -u username -P password \  
  --cafile BrokerCoreDeviceCA.pem
```

Note

Você pode receber um erro SSL:Verify se o hostname/IP endereço ao qual você está se conectando não corresponder ao nome alternativo do assunto (SAN) que está no certificado CA que você está passando para o cliente. Consulte “Adicionar nomes/IP endereços DNS personalizados ao certificado do servidor TLS” na Etapa 3: Configurando o TLS para saber como obter um certificado com a SAN correta.

Nesse momento, todos os usuários têm acesso para publicar e assinar todos os tópicos da corretora. Vá para [Configurar regras de autorização para o AWS IoT SiteWise Edge no EMQX](#).

Use sua própria CA

AWS IoT Greengrass descreve como configurar seu próprio componente de autenticação de dispositivo cliente para usar sua própria autoridade de certificação (CA). O componente de

autenticação do dispositivo cliente (`aws.greengrass.clientdevices.Auth`) autentica os dispositivos cliente e autoriza as ações do dispositivo cliente. Para obter mais informações, consulte [Como usar sua própria autoridade de certificação](#) no Guia do AWS IoT Greengrass Version 2 desenvolvedor.

Para usar sua própria CA, adicione o `aws.greengrass.clientdevices.Auth` componente à sua implantação para que você possa especificar uma configuração personalizada.

Abra a porta 8883 para conexões externas de firewall

Linux

Na regra de firewall do host Linux, adicione uma regra de entrada para a porta 8883 para permitir conexões de entrada de fora do host do gateway. Se houver algum firewall instalado, certifique-se de que as conexões TLS de entrada na porta 8883 sejam permitidas.

Windows

Na regra de firewall do Microsoft Windows host, adicione uma regra de entrada para a porta 8883 para permitir conexões de entrada de fora do host do gateway. Certifique-se de que a regra seja uma regra de permissão, do tipo porta, especificando a porta 8883. Você pode configurar isso de acordo com sua configuração de rede para permitir conexões de seus aplicativos externos com o broker.

Configurar regras de autorização para o AWS IoT SiteWise Edge no EMQX

O EMQX suporta a adição de regras de autorização com base em identificadores como nome de usuário, endereço IP ou ID do cliente. Isso é útil se você quiser limitar o número de aplicativos externos conectados a várias operações ou tópicos.

Tópicos

- [Configure a autorização usando o banco de dados integrado com Linux](#)
- [Configure a autorização usando o banco de dados integrado com o Windows](#)
- [Atualize a configuração de implantação do EMQX para autorização](#)
- [Adicione regras de autorização por meio do painel EMQX para usuários](#)

Configure a autorização usando o banco de dados integrado com Linux

Quando você configura as regras de autorização, há duas opções de configuração que dependem da sua configuração de implantação.

- Docker— Se você estiver executando uma Docker instalação padrão sem Litmus Edge, use a configuração do Docker bridge gateway. Normalmente, esse é o caso quando você implantou apenas AWS IoT SiteWise componentes.
- Litmus Edge— Se você Litmus Edge instalou no seu gateway, use a configuração de Litmus Edgesub-rede da rede.

Note

Se você configurar inicialmente o Docker bridge gateway e depois instalar Litmus Edge, reconfigure as regras de autorização usando a opção de Litmus Edge sub-rede de rede para garantir a comunicação adequada entre todos os componentes.

Para adicionar regras básicas de autorização

1. Verifique se o agente EMQX está implantado e em execução.
2. Inicie uma sessão de shell em seu host de gateway.

Docker without Litmus Edge

Para Docker instalação padrão sem Litmus Edge, execute:

```
/greengrass/v2/bin/swe-emqx-cli acl init
```

Litmus Edge network subnet

Se você estiver usando Litmus Edge, determine o IP da sub-rede da rede Litmus Edge:

```
docker network inspect LitmusNetwork | grep IPAM -A9
```

Observe o valor da sub-rede na saída e execute o comando a seguir.

`litmus_subnet_ip` Substitua pelo valor da sub-rede da etapa anterior.


```
/greengrass/v2/bin/swe-emqx-cli acl init litmus_subnet_ip
```

A ferramenta cria e aplica automaticamente regras de autorização para permitir conexões do endereço IP fornecido ao agente. Ele permite o acesso a todos os tópicos. Isso inclui o coletor IoT SiteWise OPC UA e o editor de IoT. SiteWise

3. Vá para [Atualize a configuração de implantação do EMQX para autorização](#).

Configure a autorização usando o banco de dados integrado com o Windows

Esta seção aborda a configuração de regras de autorização usando o banco de dados incorporado para implantações do Windows.

Para adicionar regras básicas de autorização

1. Verifique se o agente EMQX está implantado e em execução.
2. Execute a ferramenta AWS IoT SiteWise EMQX CLI:

```
C:\greengrass\v2\bin\swe-emqx-cli.ps1 acl init
```

A ferramenta cria e aplica automaticamente regras de ACL, permitindo conexões do localhost (127.0.0.1) com o broker. Ele permite o acesso a todos os tópicos. Isso inclui o coletor IoT SiteWise OPC UA e o editor de IoT. SiteWise

3. Vá para [Atualize a configuração de implantação do EMQX para autorização](#).

Atualize a configuração de implantação do EMQX para autorização

Para atualizar a configuração de implantação do EMQX para autorização

1. Navegue até o [console do AWS IoT SiteWise](#).
2. Na navegação à esquerda, escolha Gateways Edge na seção Edge.
3. Escolha o gateway a ser configurado.
4. Na seção Configuração do gateway Edge, copie o valor do seu dispositivo principal do Greengrass. Guarde-o para uso posterior.
5. Abra o [console de AWS IoT](#).

6. No painel de navegação à esquerda, na seção Gerenciar, escolha dispositivos Greengrass e, em seguida, Implantações.
7. Encontre o valor do dispositivo principal que você salvou anteriormente e escolha esse link para abrir a implantação.
8. Escolha o botão suspenso Ações e, em seguida, Revisar.
9. Leia a mensagem que aparece e escolha Revisar implantação. A página Especificar destino é exibida.
10. Escolha Avançar até chegar à etapa Configurar componentes.
11. Selecione o botão `aws.greengrass.clientdevices.mqtt.EMQX` de rádio.
12. Escolha o botão Configurar componente. Uma página de configuração é exibida para o componente.
13. Em Atualização de configuração, escolha Redefinir a configuração padrão para a versão do componente: 2.*.*.
14. Cole o conteúdo a seguir na seção Configuração para mesclar com base no seu sistema operacional.

Linux

```
{
  "emqxConfig": {
    "authorization": {
      "no_match": "deny",
      "sources": [
        {
          "type": "built_in_database"
        },
        {
          "type": "file",
          "path": "data/authz/acl.conf"
        }
      ]
    },
    "listeners": {
      "tcp": {
        "default": {
          "enabled": true,
          "enable_authn": false
        }
      }
    }
  },
}
```

```

        "ssl": {
            "default": {
                "enabled": true,
                "enable_authn": true,
                "ssl_options": {
                    "verify": "verify_none",
                    "fail_if_no_peer_cert": false
                }
            }
        },
        "authentication": {
            "enable": true,
            "backend": "built_in_database",
            "mechanism": "password_based",
            "password_hash_algorithm": {
                "iterations": 210000,
                "mac_fun": "sha512",
                "name": "pbkdf2"
            },
            "user_id_type": "username"
        },
        "dashboard": {
            "listeners": {
                "http": {
                    "bind": 18083
                }
            }
        },
        "authMode": "bypass",
        "dockerOptions": "-p 8883:8883 -p 127.0.0.1:1883:1883\n-p 127.0.0.1:18083:18083 -v emqx-data:/opt/emqx/data -e\nEMQX_NODE__NAME=emqx@local",
        "requiresPrivilege": "true"
    }
}

```

Windows

```

{
    "emqxConfig": {
        "authorization": {
            "no_match": "deny",

```

```
    "sources": [
      {
        "type": "built_in_database"
      },
      {
        "type": "file",
        "path": "C:\\greengrass\\v2\\work\\
\\aws.greengrass.clientdevices.mqtt.EMQX\\v2\\data\\authz\\acl.conf"
      }
    ]
  },
  "listeners": {
    "tcp": {
      "default": {
        "enabled": true,
        "enable_authn": false
      }
    },
    "ssl": {
      "default": {
        "enabled": true,
        "enable_authn": true,
        "ssl_options": {
          "verify": "verify_none",
          "fail_if_no_peer_cert": false
        }
      }
    }
  },
  "authentication": {
    "enable": true,
    "backend": "built_in_database",
    "mechanism": "password_based",
    "password_hash_algorithm": {
      "iterations": 210000,
      "mac_fun": "sha512",
      "name": "pbkdf2"
    },
    "user_id_type": "username"
  },
  "dashboard": {
    "listeners": {
      "http": {
        "bind": 18083
      }
    }
  }
}
```

```
    }  
  }  
},  
"authMode": "bypass",  
"requiresPrivilege": "true"  
}
```

15. Escolha Confirmar.
16. Escolha Avançar até chegar à etapa de revisão.
17. Escolha Implantar.

 Note

A partir desse momento, você não poderá editar o arquivo ACL para atualizar as regras de autorização. Como alternativa, você pode prosseguir [Adicione regras de autorização por meio do painel EMQX para usuários](#) após uma implantação bem-sucedida.

Adicione regras de autorização por meio do painel EMQX para usuários

Você pode adicionar ou atualizar regras de autorização usando o painel do EMQX ou a ferramenta CLI do AWS IoT SiteWise EMQX. A ferramenta AWS IoT SiteWise CLI do EMQX gerencia a autorização usando o banco de dados integrado do EMQX.

 Note

Adicionar regras de autorização é uma etapa de configuração avançada que requer compreensão dos padrões de tópicos e controle de acesso do MQTT. Para obter mais informações sobre a criação de regras de autorização usando o banco de dados integrado do EMQX, consulte [Usar banco de dados integrado nos documentos](#) do EMQX.

 Note

As instruções relacionadas ao EMQX fornecidas são apenas para referência. Como a documentação e os recursos do EMQX podem mudar com o tempo e não mantemos sua

documentação, recomendamos consultar a [documentação oficial do EMQX para obter](#) as informações mais atuais.

EMQX dashboard

Este procedimento mostra como você pode adicionar regras de autorização no painel do EMQX.

O painel do EMQX só pode ser acessado de dentro do host do gateway. Se você tentar se conectar de fora do host do gateway, não conseguirá acessar o painel.

Para adicionar regras de autorização usando o painel EMQX

1. Verifique se você está dentro do host do gateway.
2. Abra uma janela do navegador e acesse <http://localhost:18083/>.
3. Faça login no painel do EMQX. Esse procedimento pressupõe que você tenha alterado suas credenciais de login padrão para algo de sua escolha. Para obter mais informações sobre a configuração inicial, consulte [Ativar autenticação de nome de usuário e senha](#).
4. Escolha o ícone de escudo e, em seguida, Autorização no menu suspenso.
5. Escolha o botão Permissões na linha Banco de dados incorporado.
6. Na seção Autorização de banco de dados integrada, adicione ou atualize as regras de autorização do usuário de acordo com suas necessidades comerciais. Para obter mais orientações sobre a criação de regras, consulte a seção [Usar banco de dados integrado](#) na documentação do EMQX.

AWS IoT SiteWise CLI tool using Linux

Para gerenciar as regras de autorização usando a ferramenta AWS IoT SiteWise CLI EMQX no Linux:

- Adicione regras de autorização para um usuário usando o seguinte formato:

```
/greengrass/v2/bin/swe-emqx-cli auth add your-username your-action your-permission your-topic [your-action-permission-topic]
```

Example Adicionar regras de autorização para um usuário

Este exemplo mostra como adicionar regras para um usuário chamado `system1`:

```
/greengrass/v2/bin/swe-emqx-cli auth add system1 \  
  publish allow "sensors/#" \  
  subscribe allow "control/#" \  
  all deny "#"
```

Example : Exibir regras de autorização para um usuário

Para ver as regras de autorização para os `system1` usuários, execute o seguinte comando:

```
/greengrass/v2/bin/swe-emqx-cli auth list system1
```

Example : Veja todas as regras de autorização existentes

Para ver todas as regras de autorização que você tem atualmente, execute o seguinte comando:

```
/greengrass/v2/bin/swe-emqx-cli auth list
```

Example : exclua todas as regras de autorização de um usuário

Para excluir todas as regras de autorização aplicadas a um usuário específico, execute o seguinte comando:

```
/greengrass/v2/bin/swe-emqx-cli auth delete system1
```

Você é solicitado a confirmar a exclusão.

AWS IoT SiteWise CLI tool using Windows

Para gerenciar regras de autorização usando a ferramenta AWS IoT SiteWise CLI EMQX em: Windows PowerShell

- Adicione regras de autorização para um usuário usando o seguinte formato:

```
C:\greengrass\v2\bin\swe-emqx-cli.ps1 auth add your-username your-action your-  
permission your-topic [your-action-permission-topic]
```

Example : Adicionar regras de autorização para um usuário

Este exemplo mostra como adicionar regras para um usuário chamado `system1`:

```
C:\greengrass\v2\bin\swe-emqx-cli.ps1 auth add system1 `
  publish allow "sensors/#" `
  subscribe allow "control/#" `
  all deny "#"
```

Example : Exibir regras de autorização para um usuário

Para ver as regras de autorização para os `system1` usuários, execute o seguinte comando:

```
C:\greengrass\v2\bin\swe-emqx-cli.ps1 auth list system1
```

Example : Veja todas as regras de autorização existentes

Para ver todas as regras de autorização que você tem atualmente, execute o seguinte comando:

```
C:\greengrass\v2\bin\swe-emqx-cli.ps1 auth list
```

Example : exclua todas as regras de autorização de um usuário

Para excluir todas as regras de autorização aplicadas a um usuário específico, execute o seguinte comando:

```
C:\greengrass\v2\bin\swe-emqx-cli.ps1 auth delete system1
```

Você é solicitado a confirmar a exclusão.

Processe e visualize dados com o SiteWise Edge e ferramentas de código aberto

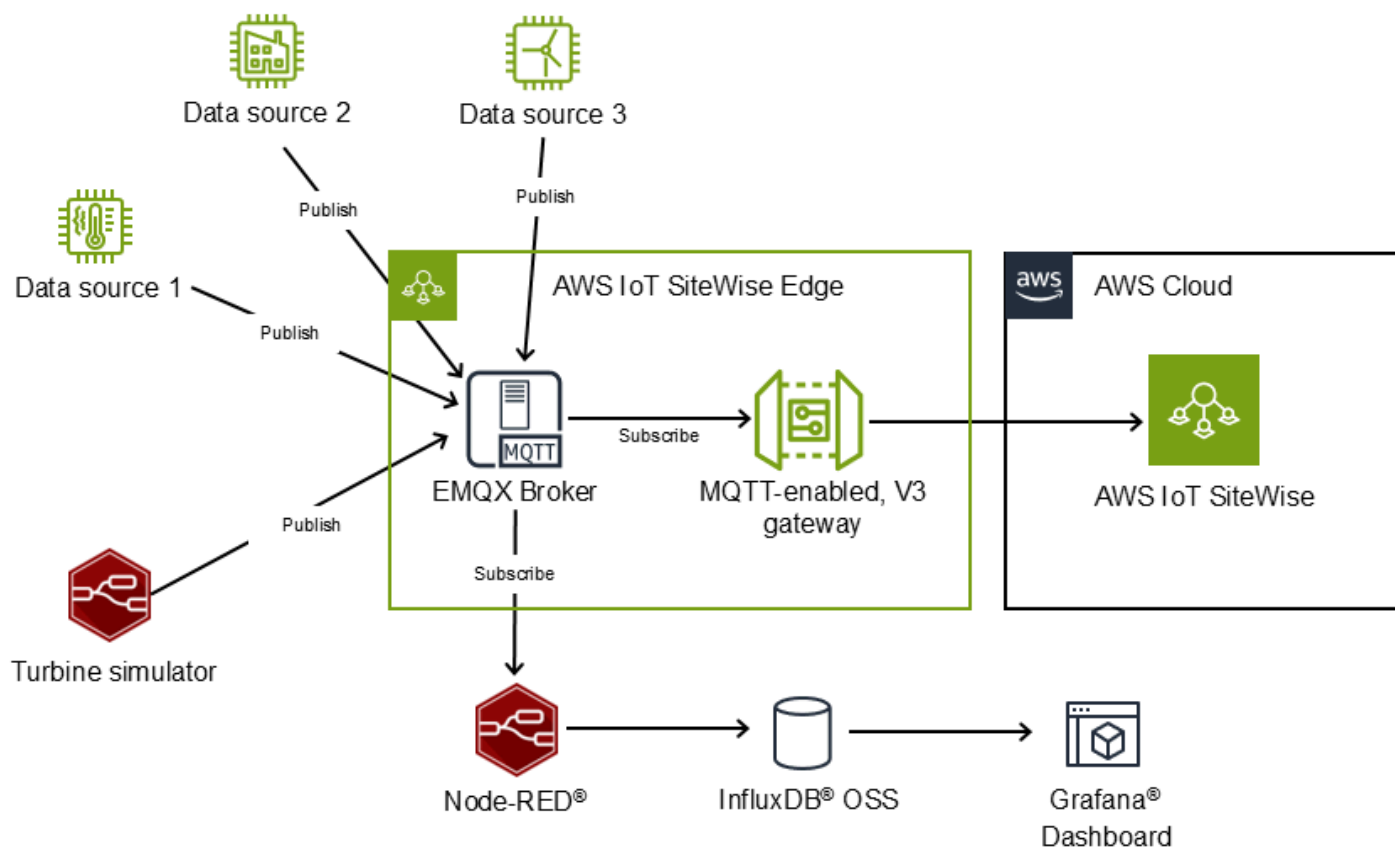
Configure gateways habilitados para AWS IoT SiteWise Edge MQTT com ferramentas de código aberto para processamento e visualização locais para aprimorar seus recursos de gerenciamento de dados industriais.

Com o SiteWise Edge, você pode criar um pipeline de processamento de dados local usando ferramentas externas de código aberto. [Use o Node-RED® para armazenar dados de séries temporais com o InfluxDB® e monitorar as operações por meio dos painéis Grafana®.](#)

O Node-RED processa e transforma seus fluxos de dados, enquanto o InfluxDB fornece armazenamento de dados em séries temporais. Grafana exibe seus dados operacionais em tempo real. Use essas ferramentas com o SiteWise Edge para sincronizar dados entre seu ambiente local e o Nuvem AWS, fornecendo informações locais imediatas e recursos de análise de longo prazo baseados em nuvem.

Note

Node-RED®, InfluxDB® e Grafana® não são fornecedores ou fornecedores do Edge. SiteWise



Note

Neste guia, estamos usando a versão de código aberto do [Grafana](#) SiteWise for Edge em vez do serviço [Amazon Managed Grafana](#).

Opções de implantação

Você pode implantar essa solução usando uma das duas abordagens. Com uma configuração Microsoft Windows manual, você controla a configuração e a integração dos componentes com sua infraestrutura. Com Linux, você pode usar o Docker para implantar componentes pré-configurados em contêineres.

Escolha o método que atenda aos seus requisitos operacionais.

- [Configurar integrações de código aberto manualmente \(Windows\)](#)— Para configurações personalizadas ou infraestrutura existente
- [Configure integrações de código aberto com o Docker \(Linux\)](#)— Para implantação rápida com componentes pré-configurados

Visão geral do exemplo de parque eólico

Este guia usa um exemplo de parque eólico para demonstrar como você pode monitorar a velocidade do vento de uma turbina em um parque eólico. Esse cenário prático ilustra as necessidades comuns de monitoramento industrial em que a visibilidade local e baseada na nuvem são valiosas para a eficiência operacional.

Com essa integração, você pode:

- Colete dados de equipamentos industriais usando um gateway AWS IoT SiteWise Edge
- Processe dados localmente com Node-RED, InfluxDB e Grafana
- Armazene dados localmente usando o InfluxDB
- Monitore dados em tempo real usando os painéis da Grafana

Ao longo deste guia, usamos o exemplo de um parque eólico. Usamos o Node-RED para simular uma turbina que gera dados de velocidade do vento. O Node-RED traduz a carga útil de dados, publica os dados no corretor SiteWise Edge MQTT, se inscreve para receber dados do corretor e armazena os dados localmente no InfluxDB. Essa abordagem garante que todos os dados operacionais estejam disponíveis localmente para acesso imediato e na nuvem para análises adicionais. Ao implementar esse padrão, você ganha resiliência contra interrupções na rede e, ao mesmo tempo, mantém a capacidade de realizar análises avançadas no. Nuvem AWS Grafana se conecta ao InfluxDB para monitoramento local, fornecendo aos operadores visibilidade em tempo real das métricas sem dependências na nuvem. Um gateway habilitado para SiteWise Edge MQTT

se conecta ao mesmo broker MQTT para o qual enviar dados AWS IoT SiteWise, criando uma ponte entre suas operações de borda e serviços baseados em nuvem.

Você pode usar seus próprios dados e configurações para criar um fluxo de trabalho semelhante, adaptado às suas necessidades industriais específicas, seja monitorando equipamentos de fabricação, infraestrutura de serviços públicos ou outros ativos industriais.

Requisitos para integrações de código aberto

Antes de implementar integrações de código aberto com o SiteWise Edge, certifique-se de que seu ambiente atenda aos requisitos necessários.

- Requisitos de hardware - O hardware do gateway deve atender aos requisitos dos gateways SiteWise Edge. Para obter mais informações, consulte [AWS IoT SiteWise Requisitos de gateway auto-hospedado do Edge](#) para gateways V3 habilitados para MQTT e [Requisitos para o aplicativo AWS IoT SiteWise Edge](#)

Important

[Ao implantar componentes adicionais de código aberto, certifique-se de que seu hardware atenda aos requisitos do InfluxDB, Node-RED e Grafana.](#)

- Sua configuração de rede deve suportar tanto a comunicação local entre os componentes quanto a conectividade em nuvem para o SiteWise Edge.
- Todos os serviços devem ser executados no mesmo host.

Considerações sobre segurança

Recomendamos que você criptografe todas as comunicações entre componentes, especialmente ao acessar interfaces de redes não locais. Implemente controles de acesso adequados para cada componente e siga as AWS melhores práticas para configuração do gateway AWS IoT SiteWise Edge e segurança AWS da conta.

Ambiente de desenvolvimento

Este guia demonstra o Node-RED, o InfluxDB e o Grafana em execução e acessados localmente em um host de gateway. Para implantações de produção que exigem acesso externo, implemente medidas de segurança, incluindo criptografia, autenticação e autorização TLS. Siga as melhores práticas de segurança de cada aplicativo.

Software de terceiros

Esta solução usa software de terceiros não mantido por AWS, incluindo InfluxDB, Node-RED, Grafana e o plug-in. `node-red-contrib-influxdb` Antes da implantação, garanta que esses componentes estejam em conformidade com os requisitos de segurança, os padrões de conformidade e as políticas de governança da sua organização.

Important

Este guia faz referência e usa software de terceiros que não pertence nem é mantido pela AWS. Antes da implementação, garanta que todos os componentes atendam aos seus requisitos de segurança, conformidade e governança. Mantenha todo o software atualizado com os patches de segurança mais recentes e siga as melhores práticas para proteger sua implantação periférica.

InfluxDB, Node-RED, Grafana não são vendedores ou fornecedores do Edge. SiteWise

Outras considerações

Considere esses fatores adicionais ao implementar integrações de código aberto com SiteWise o Edge.

- Use as versões mais recentes de todos os serviços, ferramentas e componentes.
- Filtre e agregue dados localmente antes da transmissão na nuvem para reduzir AWS IoT SiteWise os custos de ingestão de dados. Configure os períodos de retenção de dados apropriados no InfluxDB e dimensione adequadamente o hardware do gateway. Para obter mais informações, consulte [Preços do AWS IoT SiteWise](#).
- Implemente procedimentos regulares de backup para todos os dados.
- Monitore o uso de recursos em seu gateway e configure os limites de recursos apropriados para cada componente. Implemente políticas de retenção de dados no InfluxDB para gerenciar o uso do disco.

Configurar integrações de código aberto manualmente (Windows)

Use este guia para criar manualmente um intervalo de séries temporais para dados de velocidade do vento que se conectam ao Grafana® e ao Node-RED®.

Instale e configure manualmente o Node-RED, o InfluxDB® e o Grafana para controlar sua configuração de implantação. Microsoft Windows Você pode armazenar e gerenciar dados de séries temporais de seus dispositivos usando o InfluxDB.

Pré-requisitos de configuração manual

Antes de começar, preencha estes requisitos:

Note

Execute todos os serviços (SiteWise Edge, InfluxDB, Node-RED e Grafana) no mesmo host.

- Instale um gateway V3 habilitado para MQTT. Para obter mais informações, consulte [Gateways V3 habilitados para MQTT para Edge AWS IoT SiteWise](#).
- Instale e execute esses serviços localmente:
 - InfluxDB OSS v2. Para as etapas de instalação, consulte [Instalar o InfluxDB](#).
 - Node-red. Para ver as etapas de instalação, consulte [Instalar o Node-RED localmente](#).
 - Grafana. Para as etapas de instalação, consulte [Instalar o Grafana](#).

Configure o armazenamento local com o InfluxDB

Com o InfluxDB®, você pode armazenar dados de séries temporais de seus dispositivos localmente. O objetivo da capacidade de armazenamento local é manter a visibilidade operacional durante interrupções na rede e reduzir a latência para aplicativos urgentes. Você pode realizar análises e visualizações na borda e ainda ter a opção de encaminhar dados seletivamente para a nuvem.

Nesta seção, você cria um intervalo de séries temporais para dados de velocidade do vento da turbina e gera um token de API para conectividade Grafana® e Node-RED®. O bucket do InfluxDB serve como um contêiner de armazenamento dedicado para seus dados de séries temporais, semelhante a um banco de dados em sistemas tradicionais. O token da API permite acesso programático seguro aos seus dados.

Para configurar o InfluxDB

1. [Depois de concluir as etapas de pré-requisito e garantir que todas as ferramentas estejam sendo executadas no mesmo host, abra seu navegador e acesse `http://127.0.0.1:8086`.](#)

2. (Opcional) Ative a criptografia TLS para aumentar a segurança. Para obter mais informações, consulte [Habilitar a criptografia TLS](#) no InfluxData Documentation.
3. Crie um bucket InfluxDB de série temporal para armazenar dados do Node-RED. O bucket servirá como um contêiner dedicado para os dados do seu parque eólico, permitindo que você organize e gerencie políticas de retenção específicas para esse conjunto de dados. Para obter mais informações, consulte [Gerenciar buckets](#) no InfluxData Documentation.
4. (Opcional) Configure o período de retenção de dados para seu ponto de presença. Definir períodos de retenção adequados ajuda a gerenciar os recursos de armazenamento de forma eficiente, removendo automaticamente dados antigos que não são mais necessários para as operações locais.

Para obter informações sobre retenção de dados, consulte [Retenção de dados no InfluxDB](#) no InfluxData Documentation

5. Gere um token de API para o bucket. Esse token permitirá a comunicação segura entre o InfluxDB e outros componentes, como Node-RED e Grafana. Dessa forma, somente serviços autorizados podem ler ou gravar em seu armazenamento de dados. Para obter mais informações, consulte [Criar um token](#) no InfluxData Documentation.

Depois de concluir essas etapas, você pode armazenar dados de séries temporais em sua instância do InfluxDB, fornecendo uma base para persistência e análise de dados locais em seu ambiente de borda.

Configurar fluxos Node-RED para AWS IoT SiteWise integração de dados

Com o Node-RED®, você pode implementar dois fluxos para gerenciar dados entre seus dispositivos e AWS IoT SiteWise. Esses fluxos trabalham juntos para criar uma solução abrangente de gerenciamento de dados que aborda o fluxo de dados local e na nuvem.

- Fluxo de publicação de dados — publica na nuvem. O fluxo de publicação de dados envia dados para AWS IoT SiteWise. Esse fluxo simula um dispositivo de turbina gerando dados do sensor, traduzindo-os para o AWS IoT SiteWise formato e publicando-os no corretor SiteWise Edge MQTT. Isso permite que você aproveite os recursos AWS IoT SiteWise de nuvem para armazenamento, análise e integração com outros AWS serviços.

Para obter mais informações, consulte [Configurar o fluxo de publicação de dados](#).

- Fluxo de retenção de dados — armazena dados na borda. O fluxo de retenção de dados se inscreve no corretor SiteWise Edge MQTT para receber dados, traduzi-los para o formato

InfluxDB® e armazená-los localmente para monitoramento. Esse armazenamento local fornece acesso imediato aos dados operacionais, reduz a latência para aplicativos urgentes e garante a continuidade durante interrupções na rede.

Para obter mais informações, consulte [Configurar o fluxo de retenção de dados](#).

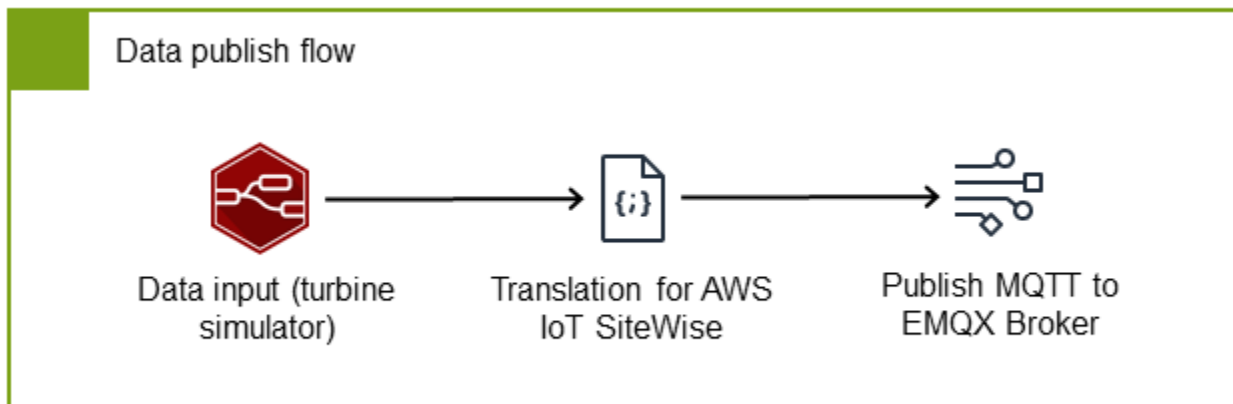
Esses dois fluxos trabalham juntos para garantir que os dados sejam enviados AWS IoT SiteWise e armazenados localmente para acesso imediato.

[Para acessar seu console Node-RED, acesse `http://127.0.0.1:1880`](#). Para obter informações sobre como habilitar o TLS, consulte [Habilitar a criptografia TLS](#).

Configurar o fluxo de publicação de dados

O fluxo de publicação de dados usa três nós para criar um pipeline que envia seus dados industriais para a nuvem. Esse fluxo é essencial para permitir análises baseadas em nuvem, armazenamento de longo prazo e integração com outros AWS serviços. Primeiro, os dados simulados do dispositivo são enviados para o corretor SiteWise Edge MQTT. O gateway coleta os dados do corretor, o que permite a transmissão para a AWS IoT SiteWise nuvem, onde você pode aproveitar os poderosos recursos de análise e visualização.

- Entrada de dados - Recebe dados do dispositivo de seus equipamentos industriais ou simuladores
- Tradutor de dados para AWS IoT SiteWise - Traduz dados em AWS IoT SiteWise formato para garantir a compatibilidade com o SiteWise gateway Edge
- Editor MQTT - publica dados no corretor SiteWise Edge MQTT, disponibilizando-os para consumidores locais e na nuvem



Configurar o nó de entrada de dados

Neste exemplo, o nó de entrada de dados usa um dispositivo simulado de turbina eólica que gera dados de velocidade do vento. Esse nó serve como ponto de entrada para seus dados industriais, sejam eles provenientes de fontes simuladas (como em nosso exemplo) ou de equipamentos industriais reais em ambientes de produção.

Usamos um formato JSON personalizado para a carga de dados a fim de fornecer uma estrutura padronizada que funciona de forma eficiente com as ferramentas de processamento locais e com o AWS IoT SiteWise serviço em nuvem. Esse formato inclui metadados essenciais, como registros de data e hora e indicadores de qualidade, juntamente com os valores reais de medição, permitindo gerenciamento abrangente de dados e rastreamento de qualidade em todo o pipeline. Importe o nó de injeção para receber dados simulados nesse formato JSON padronizado com registros de data e hora, indicadores de qualidade e valores.

Para obter mais informações sobre o nó de injeção Node-RED, consulte a seção [Injetar](#) na documentação. Node-RED

O simulador de turbina gera dados de velocidade do vento a cada segundo nesse formato JSON padronizado:

Example : Carga útil de dados da turbina

```
{
  name: string,          // Property name/identifier
  timestamp: number,     // Epoch time in nanoseconds
  quality: "GOOD" | "UNCERTAIN" | "BAD",
  value: number | string | boolean
}
```

Esse formato oferece vários benefícios:

- O `name` campo identifica a propriedade ou medida específica, permitindo que você rastreie vários pontos de dados do mesmo dispositivo
- O `timestamp` em nanossegundos garante um rastreamento preciso do tempo para uma análise histórica precisa
- O `quality` indicador ajuda você a filtrar e gerenciar dados com base em sua confiabilidade
- O `value` campo flexível suporta diferentes tipos de dados para acomodar várias saídas de sensores

Example : Nodo de injeção de um simulador de turbina

```
[
  {
    "id": "string",
    "type": "inject",
    "z": "string",
    "name": "Turbine Simulator",
    "props": [
      {
        "p": "payload.timestamp",
        "v": "",
        "vt": "date"
      },
      {
        "p": "payload.quality",
        "v": "GOOD",
        "vt": "str"
      },
      {
        "p": "payload.value",
        "v": "$random()",
        "vt": "jsonata"
      },
      {
        "p": "payload.name",
        "v": "/Renton/WindFarm/Turbine/WindSpeed",
        "vt": "str"
      }
    ],
    "repeat": "1",
    "crontab": "",
    "once": false,
    "onceDelay": "",
    "topic": "",
    "x": 270,
    "y": 200,
    "wires": [
      [
        "string"
      ]
    ]
  }
]
```

]

Configurar um nó para tradução de dados

O gateway SiteWise Edge requer dados em um formato específico para garantir a compatibilidade com a AWS IoT SiteWise nuvem. O nó tradutor é um componente importante que converte seus dados de entrada no formato de AWS IoT SiteWise carga útil necessário. Essa etapa de tradução garante que seus dados industriais possam ser processados, armazenados e posteriormente analisados adequadamente no ambiente de AWS IoT SiteWise nuvem.

Ao padronizar o formato dos dados nesse estágio, você permite a integração entre seus dispositivos de ponta e o serviço de nuvem, onde você pode usar recursos de modelagem, análise e visualização de ativos. Use essa estrutura:

Example : Estrutura de carga útil para análise de dados SiteWise do Edge

```
{
  "propertyAlias": "string",
  "propertyValues": [
    {
      "value": {
        "booleanValue": boolean,
        "doubleValue": number,
        "integerValue": number,
        "stringValue": "string"
      },
      "timestamp": {
        "timeInSeconds": number,
        "offsetInNanos": number
      },
      "quality": "GOOD" | "UNCERTAIN" | "BAD",
    }
  ]
}
```

Note

Combine `propertyAlias` o com sua hierarquia de tópicos do MQTT (por exemplo, `/Renton/WindFarm/Turbine/WindSpeed`). Isso garante que seus dados estejam associados adequadamente à propriedade correta do ativo em AWS IoT SiteWise. Para obter

mais informações, consulte o conceito de “alias de fluxo de dados” em [AWS IoT SiteWise conceitos](#).

1. Importe o nó de função de exemplo para tradução AWS IoT SiteWise de carga útil. Essa função gerencia a conversão do seu formato de entrada padronizado para o formato AWS IoT SiteWise compatível, garantindo a formatação adequada do carimbo de data/hora, indicadores de qualidade e digitação de valores.

```
[
  {
    "id": "string",
    "type": "function",
    "z": "string",
    "name": "Translate to SiteWise payload",
    "func": "let input = msg.payload;\nlet output = {};\n\noutput[\"propertyAlias\"] = input.name;\n\nlet propertyVal = {};\n\nlet timeInSeconds = Math.floor(input.timestamp / 1000);\nlet offsetInNanos = (input.timestamp % 1000) * 1000000;\n\npropertyVal[\"timestamp\"] = {\n  \"timeInSeconds\": timeInSeconds,\n  \"offsetInNanos\": offsetInNanos,\n};\n\npropertyVal[\"quality\"] = input.quality;\n\nlet typeNameConverter = {\n  \"number\": (x) => Number.isInteger(x) ? \"integerValue\" : \"doubleValue\",\n  \"boolean\": (x) => \"booleanValue\",\n  \"string\": (x) => \"stringValue\",\n};\nlet typeName = typeNameConverter[typeof input.value]\n(propertyVal[\"value\"] = {};\npropertyVal[\"value\"][typeName] = input.value;\n\noutput[\"propertyValues\"] = [propertyVal];\n\nreturn {\n  payload: JSON.stringify(output)\n};",
    "outputs": 1,
    "timeout": "",
    "noerr": 0,
    "initialize": "",
    "finalize": "",
    "libs": [],
    "x": 530,
    "y": 200,
    "wires": [
      [
        "string"
      ]
    ]
  }
]
```

2. Verifique se o JavaScript código traduz os dados da velocidade do vento corretamente. A função executa várias tarefas importantes:
 - Extrai o nome da propriedade da entrada e a define como PropertyAlias
 - Converte o timestamp de milissegundos para o formato necessário de segundos e nanossegundos
 - Preserva o indicador de qualidade para rastreamento da confiabilidade dos dados
 - Detecta automaticamente o tipo de valor e o formata de acordo AWS IoT SiteWise com os requisitos
3. Conecte o nó ao seu fluxo, vinculando-o entre o nó de entrada de dados e o editor do MQTT.

Para obter orientação sobre como escrever uma função específica para suas necessidades de negócios, consulte [Funções de escrita](#) na Node-RED documentação

Configurar o editor MQTT

Após a tradução, os dados estão prontos para publicação no corretor SiteWise Edge MQTT.

Configure o editor do MQTT com estas configurações para enviar dados ao agente SiteWise Edge MQTT:

Para importar o nó de saída do MQTT

1. Importe um nó de configuração de saída do MQTT usando o. "type": "mqtt out" Os nós de saída do MQTT permitem que você compartilhe a configuração de um broker.
2. Insira pares de valores-chave para obter informações relevantes sobre a conexão do agente MQTT e o roteamento de mensagens.

Importe o mqtt out nó de exemplo.

Example

```
[
  {
    "id": "string",
    "type": "mqtt out",
    "z": "string",
    "name": "Publish to MQTT broker",
```

```

    "topic": "/Renton/WindFarm/Turbine/WindSpeed",
    "qos": "1",
    "retain": "",
    "respTopic": "",
    "contentType": "",
    "userProps": "",
    "correl": "",
    "expiry": "",
    "broker": "string",
    "x": 830,
    "y": 200,
    "wires": []
  },
  {
    "id": "string",
    "type": "mqtt-broker",
    "name": "emqx",
    "broker": "127.0.0.1",
    "port": "1883",
    "clientId": "",
    "autoConnect": true,
    "usetls": false,
    "protocolVersion": "5",
    "keepalive": 15,
    "cleansession": true,
    "autoUnsubscribe": true,
    "birthTopic": "",
    "birthQos": "0",
    "birthPayload": "",
    "birthMsg": {},
    "closeTopic": "",
    "closePayload": "",
    "closeMsg": {},
    "willTopic": "",
    "willQos": "0",
    "willPayload": "",
    "willMsg": {},
    "userProps": "",
    "sessionExpiry": ""
  }
]

```

O exemplo de nó de saída do MQTT cria a conexão MQTT com as seguintes informações:

- Servidor: 127.0.0.1
- Porto: 1883
- Protocolo: MQTT V5

Em seguida, o nó de saída do MQTT configura o roteamento de mensagens com as seguintes informações:

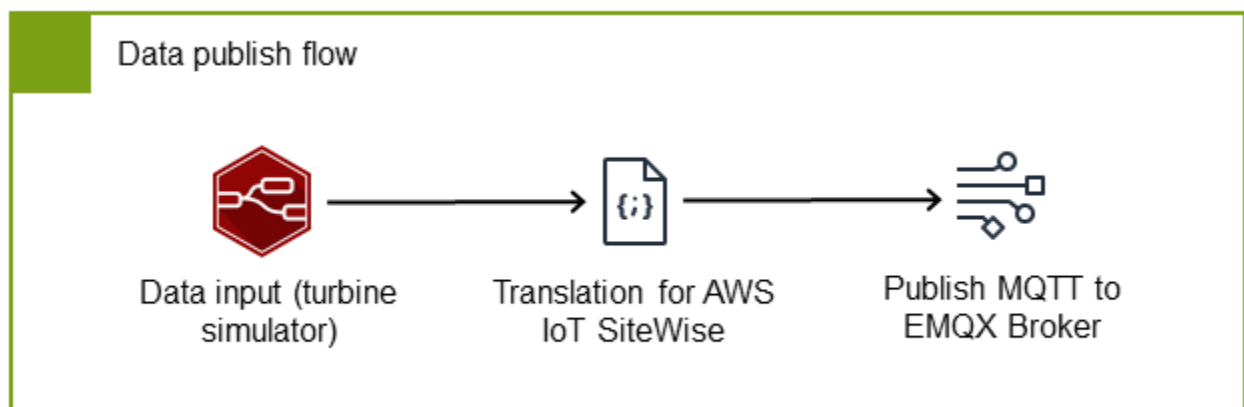
- Tópico: /Renton/WindFarm/Turbine/WindSpeed
- QoS: 1

Implante e verifique os nós

Depois de configurar os três nós de fluxo de publicação de dados, siga estas etapas para implantar o fluxo e verificar se os dados estão sendo transmitidos corretamente para AWS IoT SiteWise

Para implantar e verificar conexões

1. Conecte os três nós conforme mostrado no fluxo de publicação de dados.



2. Escolha Implantar para aplicar todas as alterações de conexão do nó.
3. Navegue até o [AWS IoT SiteWise console](#) e escolha Fluxos de dados.
4. Verifique se o prefixo Alias está selecionado no menu suspenso. Em seguida, pesquise o /Renton/WindFarm/Turbine/WindSpeed alias.

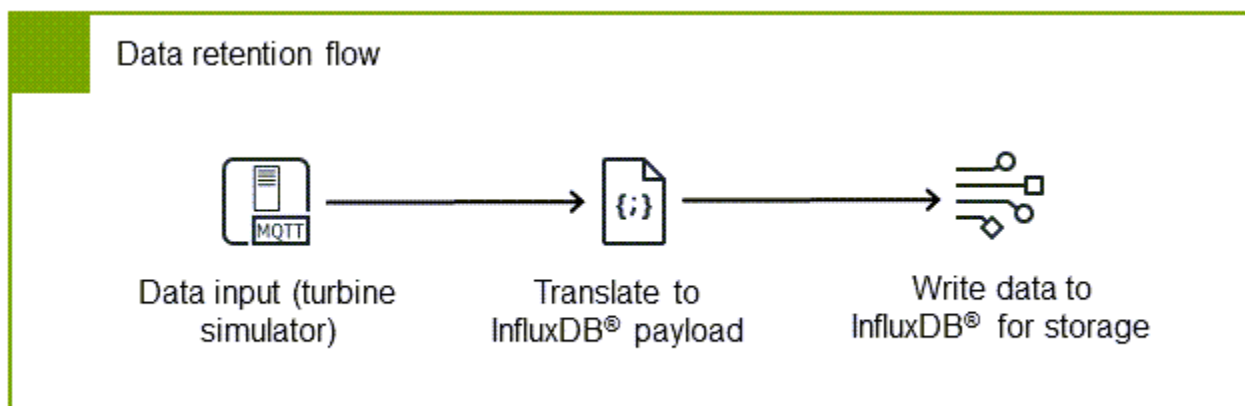
Se você ver o alias correto em sua pesquisa, você implantou o fluxo e verificou a transmissão de dados.

Configurar o fluxo de retenção de dados

O fluxo de retenção de dados pode ser usado para manter a visibilidade operacional na borda. Isso é útil durante interrupções na rede ou quando você precisa de acesso imediato aos seus dados. Esse fluxo se inscreve no corretor MQTT para receber dados do dispositivo, convertê-los no formato InfluxDB® e armazená-los localmente. Ao implementar esse fluxo, você cria um armazenamento de dados local resiliente que os operadores podem acessar sem dependências na nuvem, permitindo o monitoramento em tempo real e a tomada de decisões na borda.

O fluxo consiste em três componentes principais trabalhando juntos para garantir que seus dados sejam capturados e armazenados adequadamente:

- Cliente de assinatura MQTT - Recebe dados da corretora, garantindo a captura de todos os dados industriais relevantes
- Tradutor InfluxDB - Converte a AWS IoT SiteWise carga útil para o formato InfluxDB, preparando os dados para um armazenamento eficiente de séries temporais
- InfluxDB writer - manipula o armazenamento local, garantindo a persistência e a disponibilidade dos dados para aplicativos locais



Configurar o cliente de assinatura MQTT

- Configure o cliente de assinatura MQTT no Node-RED para receber dados do broker MQTT EMQX importando o exemplo abaixo. AWS IoT SiteWise

Example : MQTT no modo

[

```

{
  "id": "string",
  "type": "mqtt in",
  "z": "string",
  "name": "Subscribe to MQTT broker",
  "topic": "/Renton/WindFarm/Turbine/WindSpeed",
  "qos": "1",
  "datatype": "auto-detect",
  "broker": "string",
  "nl": false,
  "rap": true,
  "rh": 0,
  "inputs": 0,
  "x": 290,
  "y": 340,
  "wires": [
    [
      "string"
    ]
  ]
},
{
  "id": "string",
  "type": "mqtt-broker",
  "name": "emqx",
  "broker": "127.0.0.1",
  "port": "1883",
  "clientid": "",
  "autoConnect": true,
  "usetls": false,
  "protocolVersion": "5",
  "keepalive": 15,
  "cleansession": true,
  "autoUnsubscribe": true,
  "birthTopic": "",
  "birthQos": "0",
  "birthPayload": "",
  "birthMsg": {},
  "closeTopic": "",
  "closePayload": "",
  "closeMsg": {},
  "willTopic": "",
  "willQos": "0",
  "willPayload": "",

```



```

    "willMsg": {},
    "userProps": "",
    "sessionExpiry": ""
  }
]

```

Essa assinatura garante que todos os dados relevantes publicados na corretora sejam capturados para armazenamento local, fornecendo um registro completo de suas operações industriais. O nó usa os mesmos parâmetros de conexão MQTT da [Configurar o editor MQTT](#) seção, com as seguintes configurações de assinatura:

- Tópico — /Renton/WindFarm/Turbine/WindSpeed
- QoS — 1

Para obter mais informações, consulte [Connect to an MQTT Broker](#) na Node-RED documentação.

Configurar o tradutor InfluxDB

[O InfluxDB organiza dados usando tags para indexação e campos para valores.](#) Essa organização otimiza o desempenho das consultas e a eficiência do armazenamento para dados de séries temporais. Importe o exemplo de nó de função que contém JavaScript código para converter a AWS IoT SiteWise carga útil para o formato InfluxDB. O tradutor divide as propriedades em dois grupos:

- Etiquetas — Propriedades de qualidade e nome para uma indexação eficiente
- Campos — Registro de data e hora (em milissegundos desde a época) e valor

Example : nó de função de tradução para uma carga útil do InfluxDB

```

[
  {
    "id": "string",
    "type": "function",
    "z": "string",
    "name": "Translate to InfluxDB payload",
    "func": "let data = msg.payload;\n\nlet timeInSeconds =
data.propertyValues[0].timestamp.timeInSeconds;\nlet offsetInNanos =
data.propertyValues[0].timestamp.offsetInNanos;\nlet timestampInMilliseconds =
(timeInSeconds * 1000) + (offsetInNanos / 1000000);\n\nmsg.payload = [\n  {\n    \"timestamp(milliseconds_since_epoch)\": timestampInMilliseconds,\n  }
]

```

```

    \"value\": data.propertyValues[0].value.doubleValue\n    },\n    {\n    \"name\": data.propertyAlias,\n    \"quality\": data.propertyValues[0].quality\n    }\n]\n\nreturn msg",
    "outputs": 1,
    "timeout": "",
    "noerr": 0,
    "initialize": "",
    "finalize": "",
    "libs": [],
    "x": 560,
    "y": 340,
    "wires": [
      [
        "string"
      ]
    ]
  }
]

```

Para obter opções adicionais de configuração, consulte [node-red-contrib-influxdb](#) no repositório Node-RED GitHub .

Configurar o gravador InfluxDB

O nó de gravação do InfluxDB é o componente final em seu fluxo de retenção de dados, responsável por armazenar seus dados industriais no banco de dados local do InfluxDB. Esse armazenamento local é importante para manter a visibilidade operacional durante interrupções na rede e fornecer acesso imediato aos dados para aplicativos urgentes.

1. Instale o `node-red-contrib-influxdb` pacote por meio da opção Gerenciar paleta. Este pacote fornece os nós necessários para conectar o Node-RED ao InfluxDB.
2. Adicione um nó de saída do InfluxDB ao seu fluxo. Esse nó manipulará a gravação real de dados em seu banco de dados InfluxDB.
3. Configure as propriedades do servidor para estabelecer uma conexão segura com sua instância do InfluxDB:
 - a. Defina a versão como 2.0 - Isso especifica que você está se conectando ao InfluxDB v2.x, que usa uma API diferente das versões anteriores
 - b. Defina o URL como `http://127.0.0.1:8086` - Isso aponta para sua instância local do InfluxDB

- c. Insira seu token de autenticação do InfluxDB. Esse token seguro autoriza a conexão com seu banco de dados. Você gerou o token durante o [Configure o armazenamento local com o InfluxDB](#) procedimento.
4. Especifique os parâmetros do local de armazenamento para definir onde e como seus dados serão armazenados:
 - a. Insira o nome da sua organização InfluxDB — A organização é um espaço de trabalho para um grupo de usuários, ao qual pertencem seus buckets e painéis. Para obter mais informações, consulte [Gerenciar organizações](#) no InfluxData Documentation.
 - b. Especifique o InfluxDB Bucket (por exemplo, WindFarmData) — O bucket é equivalente a um banco de dados em sistemas tradicionais, servindo como um contêiner para seus dados de série temporal
 - c. Defina a medição do InfluxDB (por exemplo, TurbineData) — A medição é semelhante a uma tabela em bancos de dados relacionais, organizando pontos de dados relacionados

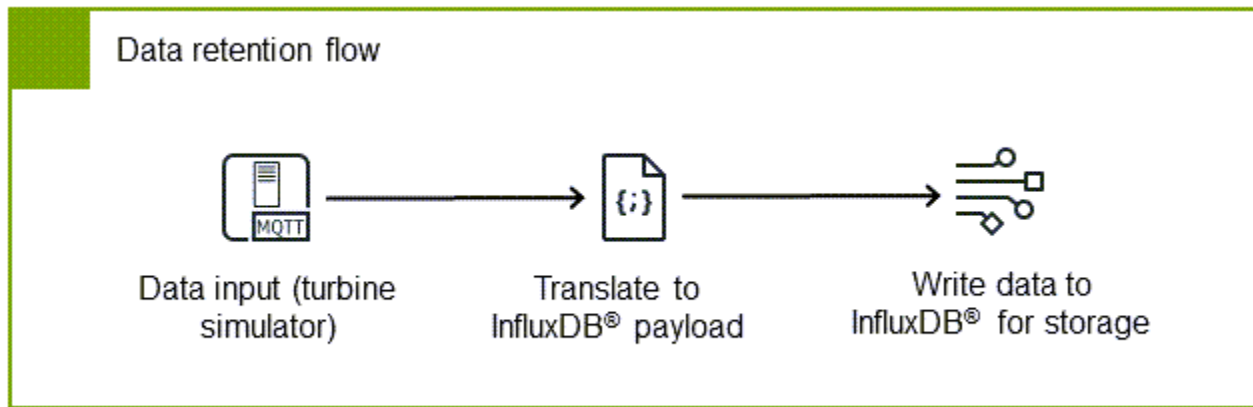
 Note

Encontre o nome da sua organização na barra lateral esquerda da instância do InfluxDB. Os conceitos de organização, bucket e medição são fundamentais para o modelo de organização de dados do InfluxDB. Para obter mais informações, consulte a documentação do [InfluxDB](#).

Implemente e verifique o fluxo de retenção

Depois de configurar todos os componentes do fluxo de retenção de dados, você precisa implantar e verificar se o sistema está funcionando corretamente. Essa verificação garante que seus dados industriais sejam armazenados localmente adequadamente para acesso e análise imediatos.

1. Conecte os três nós conforme mostrado no diagrama de fluxo de retenção de dados. Isso cria um pipeline completo, desde a assinatura de dados até o armazenamento local.



2. Escolha Implantar para aplicar suas alterações e ativar o fluxo. Isso inicia o processo de coleta e armazenamento de dados.
3. Use o InfluxDB Data Explorer para consultar e visualizar seus dados. Essa ferramenta permite verificar se os dados estão sendo armazenados adequadamente e criar visualizações iniciais dos dados da série temporal.

No Data Explorer, você deve ser capaz de ver suas medições de velocidade do vento sendo registradas ao longo do tempo, confirmando que todo o pipeline, desde a geração de dados até o armazenamento local, está funcionando corretamente.

Para obter mais informações, consulte [Consulta no Data Explorer](#) no InfluxData Documentation.

Com o fluxo de publicação de dados e o fluxo de retenção de dados implantados, agora você tem um sistema completo que envia dados para a AWS IoT SiteWise nuvem enquanto mantém uma cópia local para acesso e resiliência imediatos. Essa abordagem de caminho duplo garante que você obtenha os benefícios da análise e do armazenamento baseados em nuvem, mantendo a visibilidade operacional na borda.

Configurar o Grafana para Edge SiteWise

O Grafana® permite criar painéis de monitoramento locais em tempo real para seus dados industriais. Ao visualizar os dados armazenados no InfluxDB®, você pode fornecer aos operadores uma visão imediata sobre o desempenho do equipamento, a eficiência do processo e possíveis problemas. Essa visibilidade na borda é importante para operações urgentes e para manter a continuidade durante interrupções na rede.

Configurar a fonte de dados

Conectar o Grafana ao seu banco de dados InfluxDB cria uma poderosa camada de visualização para seus dados industriais. Essa conexão permite painéis de monitoramento em tempo real que os operadores podem usar para tomar decisões informadas sem dependências na nuvem.

1. Acesse sua instância Grafana localmente navegando até <http://127.0.0.1:3000> em seu navegador. Se for necessário ativar o TLS, você pode consultar [Configurar o HTTPS da Grafana para tráfego seguro na Web](#) na Grafana Labs Documentação.
2. Adicione uma fonte de dados do InfluxDB apontando para o bucket de série temporal do InfluxDB, onde o Node-RED grava dados. Por exemplo, .WindFarmData Essa conexão estabelece o link entre seus dados armazenados e a plataforma de visualização.
3. Para obter instruções detalhadas, consulte [Configurar a fonte de dados do InfluxDB](#) na Grafana Labs documentação.

Crie um painel Grafana para SiteWise dados do Edge

A criação de um painel é a etapa final na criação de sua solução de monitoramento local. Os painéis fornecem representações visuais de seus dados industriais, facilitando a identificação rápida de tendências, anomalias e possíveis problemas.

- Siga o guia para criar um painel. Para obter mais informações, consulte [Criar seu primeiro painel](#) na Grafana Labs Documentação. Este modelo pressupõe que seu bucket tenha um nome WindFarmData e a medição seja TurbineData.

Você também pode usar o guia de início rápido importando o modelo de painel de exemplo fornecido para criar rapidamente um painel com um gráfico de séries temporais para os dados que o Node-RED gera na seção anterior. Esse modelo fornece um ponto de partida que você pode personalizar para atender às suas necessidades específicas de monitoramento.

```
{
  "__inputs": [
    {
      "name": "DS_WINDFARM-DEMO",
      "label": "windfarm-demo",
      "description": "",
      "type": "datasource",
      "pluginId": "influxdb",
      "pluginName": "InfluxDB"
```

```

    }
  ],
  "__elements": {},
  "__requires": [
    {
      "type": "grafana",
      "id": "grafana",
      "name": "Grafana",
      "version": "11.6.0-pre"
    },
    {
      "type": "datasource",
      "id": "influxdb",
      "name": "InfluxDB",
      "version": "1.0.0"
    },
    {
      "type": "panel",
      "id": "timeseries",
      "name": "Time series",
      "version": ""
    }
  ],
  "annotations": {
    "list": [
      {
        "builtIn": 1,
        "datasource": {
          "type": "grafana",
          "uid": "-- Grafana --"
        },
        "enable": true,
        "hide": true,
        "iconColor": "rgba(0, 211, 255, 1)",
        "name": "Annotations & Alerts",
        "type": "dashboard"
      }
    ]
  },
  "editable": true,
  "fiscalYearStartMonth": 0,
  "graphTooltip": 0,
  "id": null,
  "links": [],

```

```
"panels": [  
  {  
    "datasource": {  
      "type": "influxdb",  
      "uid": "${DS_WINDFARM-DEMO}"  
    },  
    "fieldConfig": {  
      "defaults": {  
        "color": {  
          "mode": "palette-classic"  
        },  
        "custom": {  
          "axisBorderShow": false,  
          "axisCenteredZero": false,  
          "axisColorMode": "text",  
          "axisLabel": "",  
          "axisPlacement": "auto",  
          "barAlignment": 0,  
          "barWidthFactor": 0.6,  
          "drawStyle": "line",  
          "fillOpacity": 0,  
          "gradientMode": "none",  
          "hideFrom": {  
            "legend": false,  
            "tooltip": false,  
            "viz": false  
          },  
          "insertNulls": false,  
          "lineInterpolation": "linear",  
          "lineWidth": 1,  
          "pointSize": 5,  
          "scaleDistribution": {  
            "type": "linear"  
          },  
          "showPoints": "auto",  
          "spanNulls": false,  
          "stacking": {  
            "group": "A",  
            "mode": "none"  
          },  
          "thresholdsStyle": {  
            "mode": "off"  
          }  
        },  
      },  
    },  
  ],  
],
```

```
    "mappings": [],
    "thresholds": {
      "mode": "absolute",
      "steps": [
        {
          "color": "green"
        },
        {
          "color": "red",
          "value": 80
        }
      ]
    },
    "overrides": []
  },
  "gridPos": {
    "h": 8,
    "w": 12,
    "x": 0,
    "y": 0
  },
  "id": 1,
  "options": {
    "legend": {
      "calcs": [],
      "displayMode": "list",
      "placement": "bottom",
      "showLegend": true
    },
    "tooltip": {
      "hideZeros": false,
      "mode": "single",
      "sort": "none"
    }
  },
  "pluginVersion": "11.6.0-pre",
  "targets": [
    {
      "datasource": {
        "type": "influxdb",
        "uid": "${DS_WINDFARM-DEMO}"
      },

```



```

      "query": "from(bucket: \"WindFarmData\")\n  |> range(start:
v.timeRangeStart, stop: v.timeRangeStop)\n  |> filter(fn: (r) => r[\"_measurement
\"] == \"TurbineData\")\n  |> filter(fn: (r) => r[\"_field\"] == \"value\")\n
  |> filter(fn: (r) => r[\"name\"] == \"/Renton/WindFarm/Turbine/WindSpeed\")\n
  |> filter(fn: (r) => r[\"quality\"] == \"GOOD\")\n  |> aggregateWindow(every:
v.windowPeriod, fn: mean, createEmpty: false)\n  |> yield(name: \"mean\")",
      "refId": "A"
    }
  ],
  "title": "Panel Title",
  "type": "timeseries"
}
],
"schemaVersion": 41,
"tags": [],
"templating": {
  "list": []
},
"time": {
  "from": "now-6h",
  "to": "now"
},
"timepicker": {},
"timezone": "browser",
"title": "demo dashboard",
"uid": "fejc0t08o6d4wb",
"version": 1,
"weekStart": ""
}

```

Configure integrações de código aberto com o Docker (Linux)

Para um processo de implantação simplificado, você pode usar o Docker para configurar o Node-RED®, o InfluxDB® e o Grafana® em um ambiente Linux. Esse método usa contêineres pré-configurados, permitindo uma implantação rápida e um gerenciamento mais fácil dos componentes.

Pré-requisitos de configuração do Docker

Antes de começar, verifique se tem o seguinte:

- Um gateway V3 habilitado para MQTT. Para obter mais informações, consulte [Gateways V3 habilitados para MQTT para Edge AWS IoT SiteWise](#).

- O plug-in Docker Compose. Para as etapas de instalação, consulte [Instalar o Docker Compose plug-in](#) na documentação dos manuais do Docker.

Implemente os serviços

Essa implantação executa SiteWise Edge, InfluxDB, Node-RED e Grafana no mesmo host.

Configurar o ambiente

1. Obtenha acesso root:

```
sudo -i
```

2. Crie um arquivo.env ou exporte essas variáveis de ambiente:

```
export INFLUXDB_PASSWORD=your-secure-influxdb-password
export INFLUXDB_TOKEN=your-secure-influxdb-token
export GRAFANA_PASSWORD=your-secure-grafana-password
```

Configurar a rede Docker

- Crie uma rede de pontes usando o nome SiteWiseEdgeNodeRedDemoNetwork.

```
docker network create --driver=bridge SiteWiseEdgeNodeRedDemoNetwork
```

Atualize a implantação do SiteWise Edge

1. Navegue até o [console do AWS IoT](#).
2. Escolha dispositivos Greengrass no menu de navegação à esquerda, na seção Gerenciar, e depois Dispositivos principais.
3. Selecione o dispositivo principal conectado ao seu SiteWise Edge Gateway.
4. Escolha a guia Implantações e, em seguida, selecione o valor da ID de implantação.
5. Escolha Ações e, em seguida, selecione Revisar.
6. Leia a mensagem pop-up e escolha Revise Deployment.
7. Na Etapa 2 - Selecionar componentes, selecione os componentes a seguir e escolha Avançar.
 - `aws.greengrass.clientdevices.mqtt.EMQX`

- `aws.iot.SiteWiseEdgePublisher`

8. Na Etapa 3 - Configurar componentes, selecione o valor do `aws.greengrass.clientdevices.mqtt.EMQX` componente e adicione a seguinte configuração de rede:

```
{
  "emqxConfig": {
    "authorization": {
      "no_match": "allow"
    },
    "listeners": {
      "tcp": {
        "default": {
          "enabled": true,
          "enable_authn": false
        }
      }
    }
  },
  "authMode": "bypass",
  "dockerOptions": "-p 127.0.0.1:1883:1883 --network=SiteWiseEdgeNodeRedDemoNetwork",
  "requiresPrivilege": "true"
}
```

9. Escolha Próximo.
10. Na Etapa 4 - Definir configurações avançadas, escolha Avançar.
11. Escolha Implantar

Inicie os serviços

1. Inicie os serviços usando o arquivo Docker Compose. Execute o comando a seguir no diretório que contém o `compose.yaml` arquivo.

```
docker compose up -d
```

2. Crie um túnel SSH para acessar os serviços:

```
ssh -i path_to_your_ssh_key -L 1880:127.0.0.1:1880 -L 3000:127.0.0.1:3000 -L  
8086:127.0.0.1:8086 username@gateway_ip_address
```

Essa implantação cria os seguintes serviços no `SiteWiseEdgeNodeRedDemoNetwork` network:

InfluxDB v2 (porta 8086)

Inclui organização pré-configurada (`iot-sitewise-edge`), bucket do `WindFarmData` InfluxDB e credenciais de administrador

Node-RED (porta 1880)

Inclui nós InfluxDB e fluxos pré-configurados para integração AWS IoT SiteWise

Grafana (porta 3000)

Inclui usuário administrador, fonte de dados InfluxDB e painel de monitoramento

Acesse os serviços

Após a implantação, acesse os serviços usando o seguinte URLs e as credenciais:

Note

Você pode acessar cada serviço do seu host ou da máquina gateway.

Detalhes de acesso ao serviço

Serviço	URL	Credenciais
Node-red	http://127.0.0.1:1880	Não são necessárias credenciais
InfluxDB	http://127.0.0.1:8086	Nome de usuário: admin Senha: \$INFLUXDB_PASSWORD
Grafana	http://127.0.0.1:3000	Nome de usuário: admin

Serviço	URL	Credenciais
		Senha: \$GRAFANA_ PASSWORD

Verificar a implantação

Para garantir que sua implantação seja bem-sucedida, execute as seguintes verificações:

1. Para o Node-RED, verifique a presença de dois fluxos pré-carregados:
 - Fluxo de publicação de dados
 - Fluxo de retenção de dados
2. Pois AWS IoT SiteWise, no AWS IoT SiteWise console, confirme a presença de um fluxo de dados com o alias/Renton/WindFarm/Turbine/WindSpeed.
3. Para o InfluxDB, use o Data Explorer para verificar o armazenamento de dados na TurbineData medição dentro do WindFarmData bucket.
4. Para Grafana, visualize o painel para confirmar a exibição dos dados da série temporal gerados a partir do Node-RED.

Processar dados para integrações de código aberto

Os dados podem ser processados (como transformação ou agregação), em diferentes estágios usando várias ferramentas, cada uma atendendo a diferentes requisitos de monitoramento.

Processe dados com nós Node-RED

Transforme seus dados em tempo real usando os nós de processamento integrados do Node-RED®. Configure esses nós por meio do console do Node-RED para criar seu pipeline de dados.

Nós de transformação de dados

Transforme pontos de dados individuais, semelhantes ao Transforms in AWS IoT SiteWise, usando estes nós:

- change node - Executa modificações de valor simples em seus dados.
- node de função - Permite JavaScript transformações personalizadas para processamento complexo de dados.

Nós de cálculo de métricas

Combine vários pontos de dados em uma única saída, semelhante às métricas em AWS IoT SiteWise, usando esses nós:

- batch node - agrupa várias mensagens para processamento em lote.
- join node - combina vários fluxos de dados em uma única saída.
- nó agregador - calcula métricas agregadas de vários pontos de dados.

Para obter mais opções de nós, consulte a Biblioteca [Node-RED](#).

Crie tarefas do InfluxDB

Embora o Node-RED seja excelente no processamento básico de dados com configuração rápida, cálculos métricos complexos podem se tornar um desafio na programação baseada em fluxo. As tarefas do InfluxDB® fornecem uma alternativa por meio de scripts de fluxo programados para necessidades avançadas de processamento.

Use tarefas do InfluxDB para:

- Agregações estatísticas em grandes conjuntos de dados
- Operações matemáticas em várias propriedades
- Medições derivadas de várias fontes

Características da tarefa

- Execução agendada - Execute tarefas com base em expressões cron
- Processamento em lote - Otimize as operações para dados de séries temporais
- Recuperação de erros - repita automaticamente as operações com falha
- Monitoramento - Acompanhe a execução por meio de registros detalhados

Gerencie tarefas por meio da interface de usuário, API ou CLI do InfluxDB. Para obter mais informações, consulte [Processar dados com tarefas do InfluxDB](#).

Use as transformações do Grafana

Transforme a visualização de dados no Grafana® sem modificar os dados de origem no InfluxDB. As transformações do Grafana se aplicam somente à camada de visualização.

- Visual Builder - Crie transformações sem escrever código
- Visualização ao vivo - Visualize os resultados da transformação em tempo real
- Várias fontes - Processe dados de várias fontes de banco de dados
- Armazenamento eficiente — transforme dados no momento da visualização sem armazenar resultados intermediários

Para obter mais informações, consulte [Transformar dados](#).

Solução de problemas de integrações de código aberto

Para obter mais informações sobre tópicos de solução de problemas relacionados às integrações de código aberto para gateways SiteWise Edge, consulte. [Solução de problemas de integrações de código aberto no Edge](#)

Streams clássicos, gateways V2 para Edge AWS IoT SiteWise

Entenda os recursos e as limitações dos streams clássicos, gateways V2 para Edge. AWS IoT SiteWise

O gateway Classic Streams V2 mantém a funcionalidade tradicional familiar de AWS IoT SiteWise implantações anteriores antes da introdução dos gateways V3 habilitados para MQTT. Esses gateways SiteWise Edge são considerados fluxos clássicos, gateways V2. Eles mantêm a compatibilidade com versões anteriores e funcionam com o pacote de processamento de dados. Embora o Classic Streams, o gateway V2 ofereça desempenho confiável para configurações existentes, ele tem limitações em comparação com as opções de gateway mais recentes. Especificamente, esse tipo de gateway não é totalmente compatível com os recursos avançados disponíveis no destino do gateway V3 habilitado para MQTT. Para usar o protocolo de mensagens MQTT, você pode criar um novo gateway V3 habilitado para MQTT. Para obter mais informações, consulte [Gateways V3 habilitados para MQTT para Edge AWS IoT SiteWise](#).

Tópicos

- [Use pacotes para coletar e processar dados no SiteWise Edge](#)
- [Configurar o componente AWS IoT SiteWise do editor](#)
- [Gerenciador de destinos e AWS IoT Greengrass streams](#)
- [Configure os recursos de borda no AWS IoT SiteWise Edge](#)
- [Configure o processamento de dados AWS IoT SiteWise periféricos para modelos e ativos](#)

Use pacotes para coletar e processar dados no SiteWise Edge

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 “Configurar 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. Na navegação à esquerda, escolha Gateways Edge na seção Edge.
3. Na lista de 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 Editar versões do software, escolha Atualizações.

 Note

Você só pode atualizar pacotes que estejam habilitados. Para encontrar a lista de pacotes habilitados para esse gateway SiteWise Edge, escolha Visão geral e, em seguida, consulte a seção Recursos do Edge.

6. Na página de edição das versões de software, na seção Atualizações de componentes do gateway, faça o seguinte:
 - Para atualizar o Coletor OPC-UA, escolha uma versão e selecione Implantar.
 - Para atualizar o Publicador, escolha uma versão e selecione Implantar.
 - Para atualizar o Pacote de processamento de dados, escolha uma versão e selecione Implantar.
7. Quando terminar de implantar as novas versões, escolha Concluído.

Se você estiver tendo problemas para atualizar os pacotes, consulte [Não é possível implantar pacotes nos gateways SiteWise Edge](#).

Configurar o componente AWS IoT SiteWise do editor

Depois de criar um gateway AWS IoT SiteWise Edge e instalar o software, você pode configurar o componente editor para que seu gateway SiteWise Edge possa exportar dados para a AWS nuvem. Use o componente publicador para habilitar recursos adicionais ou definir configurações padrão. Para ter mais informações, consulte [AWS IoT SiteWise publisher](#) no Guia do desenvolvedor do AWS IoT Greengrass Version 2 .

 Note

A configuração do editor é diferente com base no tipo de gateway que você está usando. Para stream clássico, gateways V2, use o `iotsitewise:publisher:2` namespace. Para gateways V3 habilitados para MQTT, use o namespace. `iotsitewise:publisher:3`

Console

1. Navegue até o [console do AWS IoT SiteWise](#).
2. No painel de navegação, escolha Gateways de borda.

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 de corte, insira um valor e escolha uma unidade. O período limite deve ser entre cinco minutos e sete dias. Por exemplo, se o período de corte for de três dias, os dados mais antigos que três dias não serão publicados na nuvem.
8. (Opcional) Para definir configurações personalizadas sobre como os dados são processados no 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 alternância 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. Para gateways auto-hospedados por meio de AWS IoT Greengrass V2, 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

Use a [UpdateGatewayCapabilityConfiguration](#) API para configurar o editor.

Defina o parâmetro `capabilityNamespace` como `iotsitewise:publisher:2`.

Example : Configuração do editor para gateways Classic Stream, V2

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

```
{
  "SiteWisePublisherConfiguration": {
    "publishingOrder": "TIME_ORDER",
    "enableCompression": true,
    "dropPolicy": {
      "cutoffAge": "7d",
      "exportPolicy": {
        "retentionPeriod": "7d",
        "rotationPeriod": "6h",
        "exportSizeLimitGB": 10
      }
    }
  },
  "SiteWiseS3PublisherConfiguration": {
    "accessRoleArn": "arn:aws:iam:123456789012:role/roleName",
    "streamToS3ConfigMapping": [
      {
        "streamName": "S3_OPC-UA_Data_Collector",
        "targetBucketArn": "arn:aws:s3:::amzn-s3-demo-bucket/dataCollector",
        "publishPolicy": {
          "publishFrequency": "10m",
          "localSizeLimitGB": 10
        },
        "siteWiseImportPolicy": {
          "enableSiteWiseStorageImport": true,
          "enableDeleteAfterImport": true
        }
      }
    ]
  }
}
```

O publicador oferece 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.

enableCompression

Defina isso para `true` compactar os dados antes da publicação. A compactação de dados pode reduzir o uso da largura de banda.

dropPolicy

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

cutoffAge

A idade máxima dos dados a serem publicados é especificada em dias, horas e minutos. Por exemplo, 7d ou 1d7h16m. Dados mais antigos do que os especificados não são enviados para AWS IoT SiteWise.

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.

`SiteWiseS3PublisherConfiguration`

`accessRoleArn`

A função de acesso que dá AWS IoT SiteWise permissão para gerenciar o bucket do Amazon S3 no qual você está publicando.

`streamToS3ConfigMapping`

Uma matriz de configurações que mapeia um fluxo para uma configuração do Amazon S3.

`streamName`

O fluxo de leitura e publicação na configuração do Amazon S3.

`targetBucketArn`

O ARN do bucket de publicação.

`publishPolicy`

`publishFrequency`

A frequência com que o gateway SiteWise Edge publica no bucket do Amazon S3.

localSizeLimitGB

O tamanho máximo dos arquivos gravados no disco local. Se esse limite for violado, o publicador publicará todos os dados armazenados em buffer no destino.

siteWiseImportPolicy

enableSiteWiseStorageImport

Defina isso true para importar dados de um bucket do Amazon S3 para AWS IoT SiteWise armazenamento.

enableDeleteAfterImport

Defina isso como true para excluir o arquivo no bucket do Amazon S3 após a ingestão no armazenamento do AWS IoT SiteWise .

Gerenciador de destinos e AWS IoT Greengrass streams

AWS IoT Greengrass O gerenciador de streams permite que você envie dados para os seguintes Nuvem AWS destinos: canais de AWS IoT Analytics entrada, fluxos 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 desenvolvedor do AWS IoT Greengrass Version 2 .

Example : Estrutura da mensagem do fluxo de dados

O exemplo a seguir mostra a estrutura de mensagens de fluxo de dados necessária transmitida pelo gerenciador de AWS IoT Greengrass fluxo.

```
{
  "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 de fluxo de dados deve incluir `assetId` e `propertyId`, ou incluir `propertyAlias`, na 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 [Gerenciar fluxos de dados](#) no Guia do AWS IoT SiteWise usuário.

`propertyId`

(Opcional) O ID da propriedade de ativo dessa entrada.

`propertyValues`

(Obrigatório) A lista dos valores de propriedade a serem carregados. Você pode especificar até 10 elementos de matriz `propertyValues`.

`quality`

(Opcional) A qualidade do valor da propriedade do ativo.

`timestamp`

(Obrigatório) O carimbo de data/hora do valor da propriedade de ativo.

`offsetInNanos`

(Opcional) A diferença, em nanossegundos, em relação a `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 de ativo.

 Note

Somente um dos valores a seguir pode existir no campo `value`.

`booleanValue`

(Opcional) Dados da propriedade de ativo do tipo booleano (`true` ou `false`).

`doubleValue`

(Opcional) Dados da propriedade de ativo do tipo duplo (número de ponto flutuante).

`integerValue`

(Opcional) Dados da propriedade de ativo do tipo inteiro (número inteiro).

`stringValue`

(Opcional) Dados da propriedade de ativo do tipo string (sequência de caracteres).

Configure os recursos de borda no AWS IoT SiteWise Edge

Você pode usar o AWS IoT SiteWise Edge para coletar e armazenar temporariamente dados para poder organizar e processar dados do dispositivo localmente. Ao ativar o processamento de borda, você pode 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. Usando AWS IoT SiteWise componentes com AWS IoT Greengrass, você pode coletar e processar dados na borda antes de enviá-los para o Nuvem AWS, ou gerenciá-los localmente usando o SiteWise Edge APIs.

A coleta de dados ocorre por meio de pacotes de dados e AWS IoT SiteWise componentes que são executados em AWS IoT Greengrass.

 Note

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

Tópicos

- [Configurar a capacidade de borda no SiteWise Edge](#)

Configurar a capacidade de borda no SiteWise Edge

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 pacote de coleta de dados permite que seu gateway SiteWise Edge colete dados de vários servidores OPC UA e, em seguida, exporte os dados da borda para a AWS nuvem. 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 [Modelar ativos industriais](#).

 Note

- O pacote de processamento de dados só está disponível em plataformas x86.

Como configurar recursos de borda

1. Navegue até o [console do AWS IoT SiteWise](#).
2. No painel de navegação, escolha Gateways de borda.
3. Selecione o gateway SiteWise Edge para o qual você deseja ativar os recursos de borda.

4. Na seção Recursos de borda, escolha Editar
5. Na seção Recursos de borda, selecione Habilitar 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 obter mais informações, consulte [Gerencie gateways SiteWise Edge](#).

 Note

Você também pode usar o Linux ou Microsoft Windows as credenciais para acessar o gateway SiteWise Edge. Para obter mais informações, consulte [Acesse 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 o endereço IP do 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. Entre as propriedades do modelo de ativo estão [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 a AWS nuvem e seu gateway SiteWise Edge a cada 10 minutos. Você também pode sincronizar manualmente a partir do aplicativo SiteWise Edge Gateway local.

Configure o processamento de dados AWS IoT SiteWise periféricos para modelos e ativos

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 a AWS nuvem 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 a AWS nuvem 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 dos dados depende do espaço em disco disponível do dispositivo.
- Se o seu gateway SiteWise Edge estiver desconectado da AWS nuvem por 30 dias, ele será automaticamente desativado. [Configurar uma fonte OPC UA no SiteWise Edge](#)

Configurar um modelo de ativo para processamento de dados no SiteWise Edge

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 computar todas as propriedades na borda e enviar os resultados para a Nuvem AWS ou personalizar onde computar separadamente cada propriedade de ativo. Para obter mais informações, consulte [Configure o processamento de dados AWS IoT SiteWise periféricos para modelos e ativos](#).

Entre as propriedades de ativo estão 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 calcular na borda, o AWS IoT SiteWise também calculará sua transformação associada na borda.
- As medições são formatadas como dados brutos que seu dispositivo coleta e envia para a AWS nuvem por padrão. 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 pelo [Gerencie gateways SiteWise Edge](#).

Você pode usar o AWS IoT SiteWise REST APIs e o AWS Command Line Interface (AWS CLI) para consultar seu gateway 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 o REST APIs. Para obter mais informações sobre como configurar credenciais, consulte [the section called “Gerenciar gateways”](#).
- 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, consulte [Consultar dados de AWS IoT SiteWise](#).

Adicione fontes de dados ao seu gateway AWS IoT SiteWise Edge

Depois de configurar um gateway AWS IoT SiteWise Edge, você pode adicionar e configurar fontes de dados para ingerir dados de equipamentos industriais locais para o. AWS IoT SiteWise SiteWise O Edge oferece suporte a vários protocolos, incluindo OPC UA e muitos outros protocolos disponíveis por meio de fontes de dados de parceiros. Essas fontes permitem que seu gateway se conecte a servidores locais e recupere seus dados industriais. Ao configurar as fontes de dados, você pode ingerir dados de uma variedade de fontes de dados e, em seguida, associar os fluxos de dados às propriedades dos ativos, permitindo uma modelagem abrangente de ativos industriais e o mapeamento de dados. AWS IoT SiteWise

Tópicos

- [Fontes de dados OPC UA para gateways AWS IoT SiteWise Edge](#)
- [Fontes de dados de parceiros nos gateways SiteWise Edge](#)

Fontes de dados OPC UA para gateways AWS IoT 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, consulte [Crie um gateway SiteWise Edge auto-hospedado](#).

O tipo de gateway, habilitado para MQTT, gateways V3 versus stream clássico, gateways V2, influencia a forma como os dados do OPC UA são tratados. No fluxo clássico, gateways V2 e fontes de dados OPC UA são adicionadas diretamente à configuração do editor de IoT do gateway. SiteWise Cada fonte de dados é acoplada ao gateway e o roteamento de dados é configurado individualmente para cada fonte. Por outro lado, usando gateways V3 habilitados para MQTT, as fontes de dados OPC UA são convertidas em tópicos de MQTT e gerenciadas por meio de destinos centralizados. Para obter mais informações sobre cada tipo, consulte [Gateways V3 habilitados para MQTT para Edge AWS IoT SiteWise](#) [Streams clássicos, gateways V2 para Edge AWS IoT SiteWise](#) e.

 Note

AWS IoT SiteWise reinicia seu gateway SiteWise Edge sempre que você adiciona ou edita uma fonte. Seu gateway SiteWise Edge não ingere dados enquanto estiver atualizando a configuração da fonte. 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 [Modelar ativos industriais](#).

Você pode visualizar CloudWatch métricas para verificar se uma fonte de dados está conectada AWS IoT SiteWise a. Para obter 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.

Support para protocolos industriais adicionais

SiteWise O Edge oferece suporte a uma ampla variedade de protocolos industriais por meio da integração com parceiros de fonte de dados. Essas parcerias permitem a conectividade com mais de 200 protocolos diferentes, acomodando vários sistemas e dispositivos industriais.

Para obter uma lista dos parceiros de fonte de dados disponíveis, consulte [SiteWise Opções de fonte de dados do parceiro Edge Gateway](#).

Configurar uma fonte OPC UA no SiteWise Edge

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 fonte OPC UA \(console\)](#)
- [Configurar uma fonte OPC UA \(\)AWS CLI](#)

Configurar uma fonte OPC UA (console)

Você pode usar o console para configurar a fonte OPC UA com o procedimento a seguir.

Note

Aviso: a duplicação TQVs pode resultar em carregamento duplo.

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

1. Navegue até o [console do AWS IoT SiteWise](#).
2. Na navegação à esquerda, escolha Gateways Edge na seção Edge.
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, o endpoint local pode ser semelhante ao seguinte:

opc.tcp://203.0.113.0:49320.

7. (Opcional) Para ID de nó para seleção, adicione filtros de nó para limitar quais fluxos de dados são ingeridos na 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 obter mais informações, consulte [Use filtros de nó OPC UA no SiteWise Edge](#).
8. Os destinos variam entre gateways V3 habilitados para MQTT e streams clássicos e gateways V2.
 - Steam clássico, destinos de gateway V2 têm uma relação 1:1 com a fonte. Cada fonte envia dados para um destino específico.
 - Os destinos de gateway V3 habilitados para MQTT são configurados separadamente porque o modelo hub and spoke permite centralizar a configuração e o gerenciamento de várias fontes de dados em diferentes gateways. Para configurar destinos em um gateway V3, consulte [AWS IoT SiteWise Entenda os destinos Edge](#).

Classic streams, V2 gateway destinations

- AWS IoT SiteWise em tempo real — escolha essa opção para enviar dados diretamente para o AWS IoT SiteWise armazenamento. Ingrida e monitore dados em tempo real na borda.
- AWS IoT SiteWise Armazenado em buffer usando o Amazon S3 — Envie dados no 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 a localização preferida para o bucket do Amazon S3 e a frequência com que deseja fazer upload dos dados no Amazon S3. Também é possível 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 AWS IoT SiteWise e no Amazon S3 ou pode optar por excluí-los automaticamente do Amazon S3 depois de serem importados. AWS IoT SiteWise
 - 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 o armazenamento do AWS IoT SiteWise , os dados serão armazenados somente no Amazon S3. Ele não é importado para o SiteWise armazenamento.

Visite [Gerenciar armazenamento de dados](#) para conferir detalhes sobre as várias opções de armazenamento oferecidas pelo AWS IoT SiteWise . Para saber mais sobre opções de preço, consulte [Preço do AWS IoT SiteWise](#).

- AWS IoT Greengrass gerenciador de streams — Use AWS IoT Greengrass o gerenciador de streams para enviar dados para os seguintes destinos na AWS nuvem: 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.

MQTT-enabled, V3 gateway destinations

1. Consulte [Gateways V3 habilitados para MQTT para Edge AWS IoT SiteWise](#) para obter informações sobre como adicionar seus destinos relevantes.
 2. Retorne a esse procedimento depois de adicionar seus destinos de origem.
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 o servidor OPC UA.

- b. Se a origem exigir autenticação, escolha um segredo do AWS Secrets Manager da lista 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 obter 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) Você pode ativar um prefixo de fluxo de dados selecionando Ativar prefixo de streaming de dados - opcional.
- Insira um Prefixo de stream 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) Escolha uma opção de Conversão de tipo de dados para converter tipos de dados OPC UA não compatíveis em strings antes de fazer a ingestão deles no AWS IoT SiteWise. Converta valores de matriz com tipos de dados simples em cadeias de caracteres JSON e tipos de DateTime dados em cadeias de caracteres ISO 8601. Para obter mais informações, consulte [Converter tipos de dados incompatíveis](#).
- e. (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 no AWS IoT SiteWise. O formato é semelhante ao de ID de Nó 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 Configuração do Modo de verificação, configure as propriedades de assinatura padrão usando o Modo de verificação. Você pode selecionar Assinar ou Sondar. Para mais informações sobre o modo de verificação, consulte [the section called “Filtrar intervalos de ingestão de dados”](#).

Subscribe

Como enviar todos os pontos de dados

- i. Escolha Assinar e defina o seguinte:
 - A. [Acionador de alteração de dados](#): a condição que inicia um alerta de alteração de dados.
 - B. [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.
 - C. [Intervalo de publicação de assinatura](#): o intervalo (em milissegundos) do ciclo de publicação determinado quando a assinatura é criada.
 - D. Intervalo do instantâneo - Opcional — A configuração do tempo limite da frequência do instantâneo para garantir que o AWS IoT SiteWise Edge ingira um fluxo constante de dados.
 - E. 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.
 - F. Carimbo de data/hora: o carimbo de data/hora a ser incluído com os pontos de dados OPC UA. Você pode usar o carimbo de data/hora do servidor ou o carimbo de data/hora do dispositivo.



Note

Use a versão 2.5.0 ou posterior do componente coletor SiteWise IOT OPC UA. Se você usar o recurso de carimbo de data/hora com versões anteriores, as atualizações de configuração falharão. Para obter mais informações, consulte [Atualizar a versão de um AWS IoT SiteWise componente](#).

- ii. Em Configurações de deadband, configure um Tipo de deadband. O tipo de banda morta 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”](#).
 - Nenhum: o servidor associado envia todos os pontos de dados desse grupo de propriedades.
 - Porcentagem: o servidor associado só envia dados que estejam fora de uma porcentagem especificada do intervalo de dados. Esse intervalo é calculado pelo servidor com base nos valores mínimo e máximo de unidades de engenharia definidos para cada nó. Se o servidor não oferecer suporte a deadbands de porcentagem ou não tiver unidades de engenharia definidas, o gateway calculará o intervalo usando os valores mínimo e máximo fornecidos abaixo.
 - Absoluto: o servidor associado só envia dados que estejam fora de um intervalo específico.
- A. Defina Valor da deadband como a porcentagem do intervalo de dados em relação à deadband.
- B. (Opcional) Especifique um mínimo e um máximo para o intervalo de deadband usando Intervalo mínimo - opcional e Intervalo máximo - opcional.

Poll

Como enviar pontos de dados em um intervalo específico

- Escolha Sondar e defina o seguinte:
 - A. 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.
 - B. Carimbo de data/hora: o carimbo de data/hora a ser incluído com os pontos de dados OPC UA. Você pode usar o carimbo de data/hora do servidor ou o carimbo de data/hora do dispositivo.

**Note**

Use a versão 2.5.0 ou posterior do componente coletor SiteWise IOT OPC UA. Se você usar o recurso de carimbo de data/hora com versões anteriores, as atualizações de configuração falharão. Para obter mais informações, consulte [Atualizar a versão de um AWS IoT SiteWise componente](#).

**Note**

As Configuração de deadband serão aplicáveis quando você tiver selecionado Assinar nas Configuração do modo de verificação.

10. Escolha Salvar.

Configurar uma fonte OPC UA ()AWS 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-configuration](#) comando para atualizar a configuração do gateway SiteWise Edge. Você deve definir todas as fontes OPC UA em uma única configuração do recurso.

MQTT-enabled, V3 gateway

Esse recurso tem o namespace a seguir.

- `iotsitewise:opcuacollector:3`

```
{
  "sources": [
    {
      "name": "string",
      "endpoint": {
        "certificateTrust": {
          "type": "TrustAny" | "X509",
          "certificateBody": "string",
          "certificateChain": "string",
```

```

    },
    "endpointUri": "string",
    "securityPolicy": "NONE" | "BASIC128_RSA15" | "BASIC256" | "BASIC256_SHA256"
    | "AES128_SHA256_RSA0AEP" | "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",
    "typeConversions": {
        "array": "JsonArray",
        "datetime": "ISO8601String"
    },
    "destination": {
        {
            "type": "MQTT"
        }
    },
    "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,
      "timestampToReturn": "SOURCE_TIME" | "SERVER_TIME"
    },
    "dataQuality": {
      "allowGoodQuality": true | false,
      "allowBadQuality": true | false,
      "allowUncertainQuality": true | false
    },
    "subscription": {
      "dataChangeTrigger": "STATUS" | "STATUS_VALUE" |
"STATUS_VALUE_TIMESTAMP",
      "queueSize": integer,
      "publishingIntervalMilliseconds": integer,
      "snapshotFrequencyMilliseconds": integer
    }
  }
]
}
}

```

Classic streams, V2 gateway

Esse recurso tem o namespace a seguir.

- `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_RSA0AEP" | "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",
    "typeConversions": {
        "array": "JsonArray",
        "datetime": "ISO8601String"
    },
    "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,
        "timestampToReturn": "SOURCE_TIME" | "SERVER_TIME"
    },
    "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

sources

Uma lista das estruturas de definição de fontes OPC UA que contenham as seguintes informações:

name

Um nome exclusivo e amigável para a origem.

endpoint

Uma estrutura de endpoint que contém as seguintes informações:

certificateTrust

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

type

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`.

`certificateBody`

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

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

`certificateChain`

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

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

`endpointUri`

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

`securityPolicy`

A política de segurança a ser usada para que você possa proteger mensagens lidas da fonte 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_RSA0AEP** – A política de segurança de `Aes128_Sha256_Rsa0aep`.
- **AES256_SHA256_RSAPSS** – A política de segurança de `Aes256_Sha256_RsaPss`.
- **BASIC128_RSA15**: (descontinuado) a política de segurança `Basic128Rsa15` foi descontinuada na especificação OPC UA porque não é mais considerada segura. Recomendamos que você escolha uma política de segurança diferente. Para obter mais informações, consulte [Perfil SecurityPolicy — Basic128Rsa15](#).

- BASIC256: (descontinuado) a política de segurança Basic256 foi descontinuada na especificação OPC UA porque não é mais considerada segura. Recomendamos que você escolha uma política de segurança diferente. Para obter mais informações, consulte [SecurityPolicy — 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 obter mais informações, consulte [Configurar servidores OPC UA para confiar no gateway do AWS IoT SiteWise Edge](#).

`messageSecurityMode`

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: dados em trânsito entre o gateway e a fonte 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 obter mais informações, consulte [Configurar servidores OPC UA para confiar no gateway do AWS IoT SiteWise Edge](#).

`identityProvider`

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

type

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`.

usernameSecretArn

(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 obter mais informações, consulte [Configurar a autenticação da fonte de dados para o SiteWise Edge](#).

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

nodeFilterRules

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 obter mais informações, consulte [Use filtros de nó OPC UA no SiteWise Edge](#).

Cada estrutura na lista deve conter as seguintes informações:

action

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.

definition

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

type

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 do OPC UA.

rootPath

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

measurementDataStreamPrefix

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.

typeConversions

Os tipos de conversões disponíveis para tipos de dados OPC UA não compatíveis. Cada tipo de dados é convertido em strings. Para obter mais informações, consulte [Converter tipos de dados incompatíveis](#).

array

O tipo de dados de matriz simples que é convertido em strings. Você pode escolher a seguinte opção:

- `JsonArray`: indica que você optou por converter os tipos de dados de matriz simples em strings.

datetime

O tipo `DateTime` de dados que é convertido em cadeias de caracteres. Você pode escolher a seguinte opção:

- `ISO8601String`: indica que você optou por converter tipos de dados ISO 8601 em strings.

destination

Configuração para o destino das etiquetas OPC UA. Os gateways V3 de stream clássico, habilitados para v2 e MQTT, têm configurações diferentes para destinos.

type

O tipo do destino.

`streamName`— somente para streams clássicos, gateways V2

O nome do stream do . O nome do fluxo deve ser exclusivo.

`streamBufferSize`— somente para streams clássicos, gateways V2

O tamanho de buffer do fluxo. Isso é importante para gerenciar o fluxo de dados das fontes OPC UA.

propertyGroups

(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.

deadband

O valor deadband define a alteração mínima no valor de um ponto de dados que deve ocorrer para que os dados sejam enviados à nuvem. Ela contém as seguintes informações:

type

Os tipos de deadband compatíveis. Você pode escolher as seguintes opções:

- **ABSOLUTE**: um valor fixo que especifica a alteração absoluta mínima necessária para considerar um ponto de dados significativo o suficiente para ser enviado à nuvem.
- **PERCENT**: um valor dinâmico que especifica a alteração mínima necessária como uma porcentagem do valor do último ponto de dados enviado. Esse tipo de deadband é útil quando os valores de dados variam muito ao longo do tempo.

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.

eguMin

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

timeoutMilliseconds

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

scanMode

A estrutura de scanMode contém as seguintes informações:

type

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

rate

O intervalo de amostragem para o modo de verificação.

timestampToReturn

A fonte do carimbo de data/hora. Você pode escolher as seguintes opções:

- SOURCE_TIME: usa o carimbo de data/hora do dispositivo.
- SERVER_TIME: usa o carimbo de data/hora do servidor.

Note

Use TimestampToReturn com a versão 2.5.0 ou posterior do componente coletor SiteWise IOT OPC UA. Se você usar esse recurso com versões anteriores, as atualizações de configuração falharão. Para obter mais informações, consulte [Atualizar a versão de um AWS IoT SiteWise componente](#).

nodeFilterRuleDefinitions

(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:

type

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

rootPath

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

Exemplos adicionais de configuração de recursos para fluxos clássicos, gateways V2 ()AWS CLI

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 fonte OPC UA

O arquivo `opc-ua-configuration.json` a seguir define uma configuração de fonte OPC UA básica e sem proteção.

```
{
  "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 fonte OPC UA com grupos de propriedades definidos

O arquivo `opc-ua-configuration.json` a seguir define uma configuração de fonte OPC UA básica e sem proteção, 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 fonte OPC UA com propriedades

O exemplo de JSON a seguir 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:greenrass-windfarm2-auth-1ABCDE"
        },
        "nodeFilterRules": [
          {
            "action": "INCLUDE",
            "definition": {
              "type": "OpcUaRootPath",
              "rootPath": "/WindFarm/2/WindTurbine/"
            }
          }
        ]
      }
    }
  ],
}
```

```

    "measurementDataStreamPrefix": "/Washington"
  }
]
}

```

Example : configuração da fonte OPC UA com confiança por certificado

O exemplo de JSON a seguir 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-----
MIICiTCCAFICCD6m7oRw0uX0jANBgkqhkiG9w
0BAQUFADCBIDELMAKGA1UEBhMCVVMxCzAJBgNVBAGTAldBMRAwDgYDVQQHEwdTZ
WF0dGx1MQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBA5TC0lBTSBDb25zb2x1MRIw
EAYDVQQDEw1UZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFTYXpvi5
jb20wHhcNMTEwNDI1MjA0NTIxWhcNMTEwNDI0MjA0NTIxWjCBiDELMAKGA1UEBh
MCVVMxCzAJBgNVBAGTAldBMRAwDgYDVQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBb
WF6b24xFDASBgNVBA5TC0lBTSBDb25zb2x1MRIwEAYDVQQDEw1UZXN0Q2lsYWMx
HzAdBgkqhkiG9w0BCQEWEG5vb25lQGFTYXpvi5jb20wgZ8wDQYJKoZIhvcNAQE
BBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ21uUSfwfEvySWtC2XADZ4nB+BLyGVI
k60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9TrDHudUZg3qX4waLG5M43q7Wgc/MbQ
ITx0USQv7c7ugFFDzQGBzZswY6786m86gpEIbb30hjZnzcvcQAaRHhd1QWIMm2nr
AgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4nUhVVxYUntneD9+h8Mg9q6q+auN
KyExzyLwax1Aoo7TJHidbtS4J5iNmZgXL0FkbFFBjvSfpJlI00zbhNYS5f6Guo
EDmFJl0ZxBHjJnyp3780D8uTs7fLvJx79LjSTbNYiytVbZPQUQ5Yaxu2jXnimvw
3rrszlaEXAMPLE=
-----END CERTIFICATE-----",
          "certificateChain": "-----BEGIN CERTIFICATE-----
MIICiTCCAFICCD6m7oRw0uX0jANBgkqhkiG9w
0BAQUFADCBIDELMAKGA1UEBhMCVVMxCzAJBgNVBAGTAldBMRAwDgYDVQQHEwdTZ
WF0dGx1MQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBA5TC0lBTSBDb25zb2x1MRIw
EAYDVQQDEw1UZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFTYXpvi5
jb20wHhcNMTEwNDI1MjA0NTIxWhcNMTEwNDI0MjA0NTIxWjCBiDELMAKGA1UEBh
MCVVMxCzAJBgNVBAGTAldBMRAwDgYDVQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBb
WF6b24xFDASBgNVBA5TC0lBTSBDb25zb2x1MRIwEAYDVQQDEw1UZXN0Q2lsYWMx
HzAdBgkqhkiG9w0BCQEWEG5vb25lQGFTYXpvi5jb20wgZ8wDQYJKoZIhvcNAQE
BBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ21uUSfwfEvySWtC2XADZ4nB+BLyGVI
k60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9TrDHudUZg3qX4waLG5M43q7Wgc/MbQ
ITx0USQv7c7ugFFDzQGBzZswY6786m86gpEIbb30hjZnzcvcQAaRHhd1QWIMm2nr
AgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4nUhVVxYUntneD9+h8Mg9q6q+auN
KyExzyLwax1Aoo7TJHidbtS4J5iNmZgXL0FkbFFBjvSfpJlI00zbhNYS5f6Guo
EDmFJl0ZxBHjJnyp3780D8uTs7fLvJx79LjSTbNYiytVbZPQUQ5Yaxu2jXnimvw
3rrszlaEXAMPLE=
-----END CERTIFICATE-----"
```

```

WF0dGx1MQ8wDQYDVQKKEwZBbWF6b24xFDASBgNVBAwTC01BTsBDb25zb2x1MRIw
EAYDVQQDEw1UZXN0Q21sYWxhZAdBgqhkiG9w0BCQEWEG5vb25lQGFTYXpvi5
jb20wHhcNMTEwNDI1MjA0NTIxWhcNMTEwNDI1MjA0NTIxWjCBiDELMAkGA1UEBh
MCVVMxMzA0BjBBAgTALDQWZWF0dGx1MQ8wDQYDVQKKEwZBbWF6b24xFDASBgNVBAwTC01BTsBDb25zb2x1MRIwEAYDVQQDEw1UZXN0Q21sYWxhZAdBgqhkiG9w0BCQEWEG5vb25lQGFTYXpvi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ21uUSfwfEvySWtC2XADZ4nB+BLyGVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9TrDHudUZg3qX4waLG5M43q7Wgc/MbQITx0USQv7c7ugFFDzQGBzZswY6786m86gpEIbb30hjZnzcVQAaRHhd1QWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEATCu4nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwax1Aoo7TJHidbtS4J5iNmZgXL0FkbFFBjvSfpJI1J00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp3780D8uTs7fLvJx79LjSTbNYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
-----END CERTIFICATE-----"
    },
    "endpointUri": "opc.tcp://203.0.113.2:49320",
    "securityPolicy": "BASIC256",
    "messageSecurityMode": "SIGN_AND_ENCRYPT",
    "identityProvider": {
        "type": "Anonymous"
    },
    "nodeFilterRules": []
  },
  "measurementDataStreamPrefix": ""
}
]
}

```

Configurar servidores OPC UA para confiar no gateway do AWS IoT SiteWise 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 gateway AWS IoT SiteWise Edge. O gateway SiteWise Edge gera um certificado que seu servidor de origem pode exigir. O processo varia de acordo com os servidores de fonte. Para ter mais informações, consulte a documentação dos servidores.

O procedimento a seguir descreve as etapas básicas.

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

1. Abra a interface para configurar o 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 SiteWise Edge. 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 SiteWise Edge. Depois, você poderá importar o certificado no servidor OPC UA.

Como exportar o arquivo do certificado de cliente OPC UA para uma fonte

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

Por padrão, a pasta de trabalho do Greengrass está */greengrass/v2/work/ aws.iot.SiteWiseEdgeCollectorOpcua* no Linux e *C:/greengrass/v2/work/ aws.iot.SiteWiseEdgeCollectorOpcua* está ativada. Microsoft 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 [Conecte-se à sua instância Linux usando SSH](#) no Guia do EC2 usuário da Amazon.

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 maneira como os dados são ingeridos com uma fonte 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.

Coletar ou filtrar dados com base na qualidade

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

- Good
- Bad
- Uncertain

Manipule valores NaN ou nulos

SiteWise O Edge suporta a coleta e o tratamento de valores NaN e nulos.

- NaN (Não é um número): representa resultados numéricos indefinidos ou irrepresentáveis.
- Nulo: indica dados ausentes.

O coletor IoT SiteWise OPC UA captura valores NaN e Null com qualidade RUIM ou INCERTA. Esses valores especiais são gravados no fluxo local, permitindo uma coleta de dados mais abrangente.

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

Você pode configurar o modo de verificação OPC UA para controlar a maneira como coleta dados da fonte 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 OPC UA com intervalos de deadband

Você pode aplicar uma deadband aos grupos de propriedades da fonte 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 da fonte 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 [Fontes de dados OPC UA para gateways AWS IoT SiteWise Edge](#).

 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. Elas permitem que você escolha quantos dados são enviados para a Nuvem AWS 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 assumirá como padrão o intervalo total do tipo de dados da medição.

- **Absoluto** — Você especifica uma janela usando unidades exatas. Por exemplo, especificar um valor de banda morta de 2 em um sensor faz com que o servidor envie dados para a AWS nuvem 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. Depois desse tempo limite, o servidor OPC UA enviará o valor da medição atual, mesmo se estiver 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.

Use filtros de nó OPC UA no SiteWise Edge

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 [Fontes de dados OPC UA para gateways AWS IoT 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 enquanto estiver atualizando a configuração da fonte. 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 : Cenário usando filtros de nós

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, você pode definir filtros de nó para limitar quais dados da fonte OPC UA serão incluídos.

- 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*.

Converter tipos de dados incompatíveis

Opcionalmente, habilite a conversão de tipos de dados AWS IoT SiteWise para matrizes e tipos de DateTime dados simples. AWS IoT SiteWise não suporta todos os tipos de dados OPC UA. Quando você envia dados não compatíveis para o seu fluxo AWS IoT Greengrass de dados, esses dados são perdidos. No entanto, ao converter os tipos de dados nativos não compatíveis em cadeias de caracteres, você pode ingerir os dados em AWS IoT SiteWise vez de descartá-los. AWS IoT SiteWise serializa seus dados convertidos para que você possa usar posteriormente suas próprias funções para converter as cadeias de caracteres de volta ao tipo de dados original a jusante, se necessário.

Você pode atualizar as configurações de conversão de tipos de dados para uma fonte de dados a qualquer momento, e cada fonte de dados pode ter as próprias configurações.

Quando você adiciona fontes de dados no Console do AWS IoT SiteWise, há duas caixas de seleção em Conversão de tipo de dados na Configuração avançada. Você pode indicar quais tipos de dados converter em strings.

Além disso, o coletor IoT SiteWise OPC UA pode aceitar valores NaN ou nulos na borda.

- Converter valores de matriz com tipos de dados simples em strings JSON
- Converta DateTime valores em cadeias de caracteres ISO 8601

Pré-requisito

- Use a versão 2.5.0 ou posterior do coletor [SiteWise IoT OPC UA](#).

Limitações

Essas são as limitações da conversão de tipos de dados OPC UA em strings no AWS IoT SiteWise.

- A conversão de tipos de dados complexos não é compatível.
- Os limites de string depois da conversão são de 1.024 bytes. Se a string tiver mais de 1024 bytes, ela será rejeitada por AWS IoT SiteWise.

Configurar a autenticação da fonte de dados para o SiteWise Edge

Se o 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 gateway SiteWise 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, consulte [Gerenciador secreto](#) no Guia do AWS IoT Greengrass Version 2 desenvolvedor.

Para obter informações sobre como gerenciar o acesso aos segredos do Secrets Manager, consulte:

- [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, insira **username** e, na segunda caixa de entrada, insira o nome de usuário.
 2. Escolha Adicionar linha.
 3. Na primeira caixa de entrada, insira **password** e, na segunda caixa de entrada, insira a senha.
5. Em Chave de criptografia, selecione aws/secretsmanager e escolha Próximo.
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.

Exemplo política

secret-arn Substitua pelo nome de recurso da Amazon (ARN) do segredo que você criou na etapa anterior. Para obter mais informações sobre como obter o ARN de um segredo, consulte [Encontrar segredos AWS Secrets Manager no Guia](#) do AWS Secrets Manager usuário.

```
{
```

```
"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

secret-arn Substitua pelo ARN do segredo que você criou na etapa anterior. Para obter mais informações sobre como obter o ARN de um segredo, consulte [Encontrar segredos AWS Secrets Manager no Guia](#) do AWS Secrets Manager usuário.

```
{
  "cloudSecrets": [
    {
      "arn": "secret-arn"
    }
  ]
}
```

12. Escolha Confirmar.
13. Escolha 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.

Fontes de dados de parceiros nos 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 AWS IoT Greengrass componentes 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.

Note

Você pode adicionar uma fonte de dados para cada parceiro em cada gateway.

Para adicionar uma fonte de dados de parceiro, faça o seguinte:

1. [Adicionar uma fonte de dados de parceiro no SiteWise Edge](#)
2. Acesse o portal web do parceiro, quando aplicável, e configure a fonte de dados do parceiro para que ela se conecte ao gateway SiteWise Edge.

Tópicos

- [Segurança](#)
- [Configure Docker em seu gateway SiteWise Edge](#)
- [Adicionar uma fonte de dados de parceiro no SiteWise Edge](#)
- [SiteWise Opções de fonte de dados do parceiro Edge Gateway](#)

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.
- Monitoramento do uso razoável dos recursos da máquina do gateway SiteWise Edge (CPU, memória e sistema de arquivos).

AWS responsabilidade

- Isolar o parceiro dos recursos de AWS nuvem 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 e memória).

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.

Configure Docker em seu gateway SiteWise Edge

AWS IoT SiteWise fornece uma Docker imagem que permite executar o aplicativo SiteWise Edge em várias plataformas e ambientes. Essa Docker imagem encapsula todos os componentes e dependências necessários para coletar, processar e enviar dados do seu equipamento industrial para a nuvem. AWS Usando a imagem do Docker, você pode implantar e executar o aplicativo SiteWise Edge em hosts compatíveis com o Docker, como servidores, dispositivos de borda ou serviços de contêiner baseados em nuvem.

Para adicionar uma fonte de dados de parceiro, o [Docker Engine](#) 1.9.1 ou posterior deve estar instalado no dispositivo local.

Note

A versão 20.10 é a versão mais recente verificada para funcionar com o software SiteWise Edge Gateway.

Verifique se Docker está instalado

Para verificar se Docker está instalado, execute o seguinte comando em um terminal conectado ao seu gateway SiteWise Edge:

```
docker info
```

Se o comando retornar um `docker is not recognized` resultado ou se uma versão mais antiga do Docker estiver instalada, [instale o Docker Engine](#) antes de continuar.

Configurar o Docker

O usuário do sistema que executa um componente de Docker contêiner deve ter permissões de root ou administrador, ou você deve configurar Docker para executá-lo como usuário não root ou não administrador.

Em dispositivos Linux, você deve adicionar um `ggc_user` usuário ao `docker` grupo para chamar Docker comandos `sudo`.

Para adicionar `ggc_user` ou o usuário não root que você usa para executar componentes de Docker contêiner ao `docker` grupo, execute o seguinte comando:

```
sudo usermod -aG docker ggc_user
```

Para obter mais informações, consulte as [etapas de pós-instalação do Linux para o Docker Engine](#).

Adicionar uma fonte de dados de parceiro no SiteWise Edge

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, você deve fazer o seguinte:

- Para EasyEdge e CloudRail, crie uma conta com o parceiro, depois vincule as contas.
- [Configure Docker em seu gateway SiteWise Edge](#)

Crie um gateway SiteWise Edge com uma fonte de dados parceira

Se você quiser criar um novo gateway SiteWise Edge, conclua as etapas em [Crie um gateway SiteWise Edge auto-hospedado](#). Depois de criar o SiteWise Edge Gateway, siga as etapas [Adicionar uma fonte de dados de parceiro a um gateway SiteWise Edge existente](#) para adicionar uma fonte de dados de parceiro.

Adicionar uma fonte de dados de parceiro a um gateway SiteWise Edge existente

1. Navegue até o [console do AWS IoT SiteWise](#).
2. Na navegação à esquerda, escolha Gateways Edge na seção Edge.
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. Na tela Adicionar fonte de dados, escolha um tipo de fonte para selecionar o parceiro que conecta seu gateway SiteWise Edge. Cada fonte de dados tem as próprias opções de configuração. Existem duas categorias de fontes de dados: fontes da AWS e fontes de parceiros.

Usando uma fonte de dados de parceiro, você pode selecionar uma fonte por gateway. Para conferir uma lista das opções de integração de parceiros de fonte de dados, consulte [SiteWise Opções de fonte de dados do parceiro Edge Gateway](#). Observe que você pode adicionar até 100 fontes de dados OPC UA (AWS fontes). Para começar a usar fontes de dados OPC UA, consulte [Fontes de dados OPC UA para gateways AWS IoT SiteWise Edge](#).

6. Insira um nome para a origem.
7. Selecione a guia da fonte de dados abaixo e siga o procedimento de configuração.

CloudRail

Grande parte da CloudRail configuração é feita no CloudRail portal depois de salvar a fonte de dados do seu gateway SiteWise Edge. No entanto, é necessário autorizar a conexão.

Note

A conexão com o CloudRail só está disponível no Linux.

1. [Crie uma conta do CloudRail](#) para começar a conexão com o AWS IoT SiteWise.
2. Verifique se o Docker está instalado no gateway. Para obter mais informações, consulte [Configure Docker em seu gateway SiteWise Edge](#).
3. Leia o contrato disponível em Autorize o acesso e a implantação e escolha Autorizar. Marcar a caixa concede ao AWS parceiro acesso à sua fonte de dados e permite AWS a implantação no componente do parceiro.

 Note

O Prefixo de medição - opcional é definido no portal do CloudRail.

 Note

O software do parceiro é desenvolvido, mantido e suportado pelo AWS parceiro. AWS não é responsável pela interface, configuração ou software.

Para obter mais informações, consulte [CloudRail](#).

EasyEdge

Grande parte da EasyEdge configuração é feita no EasyEdge portal depois de salvar a fonte de dados do seu gateway SiteWise Edge. No entanto, é necessário autorizar a conexão.

 Note

A conexão com o EasyEdge só está disponível no Linux.

1. [Crie uma conta do EasyEdge](#) para começar a conexão com o AWS IoT SiteWise.
2. Verifique se o Docker está instalado no gateway. Para obter mais informações, consulte [Configure Docker em seu gateway SiteWise Edge](#).
3. Leia o contrato disponível em Autorize o acesso e a implantação e escolha Autorizar. Marcar a caixa concede ao AWS parceiro acesso à sua fonte de dados e permite AWS a implantação no componente do parceiro.

 Note

O Prefixo de medição - opcional é definido no portal do EasyEdge.

 Note

O software do parceiro é desenvolvido, mantido e suportado pelo AWS parceiro. AWS não é responsável pela interface, configuração ou software.

Para obter mais informações, consulte [EasyEdge](#).

Litmus Edge

Você pode ativar a configuração do Litmus de duas maneiras. Ative o Litmus Edge diretamente pelo AWS IoT SiteWise usando as informações do portal Litmus Edge Manager. Ou você pode ativar manualmente o Litmus Edge para AWS IoT SiteWise por meio do Litmus Edge Manager.

 Note

A conexão com o Litmus Edge só está disponível no Linux.

Para ativar usando um código Litmus Edge de ativação em AWS IoT SiteWise

Use esse procedimento ao adicionar uma fonte de dados do Litmus Edge com um código de ativação do Litmus Edge no Console do AWS IoT SiteWise.

1. Selecione Ative agora usando um código. São exibidas opções de configuração adicionais.
2. Insira o Litmus Edge Manager para se conectar Litmus Edge ao seu gateway SiteWise Edge. Para ter mais informações, consulte [Step 3a: Set Data and Device Management Endpoint](#) na documentação do Litmus Edge Manager.
3. Forneça o código de Litmus Edge Manager ativação para ativar Litmus Edge em AWS IoT SiteWise
4. Opcionalmente, AWS IoT SiteWise forneça o certificado Litmus Edge Manager CA. O certificado impede a ativação do Litmus Edge em um Litmus Edge Manager não autorizado.

5. Verifique se o Docker está instalado no gateway. Para obter mais informações, consulte [Configure Docker em seu gateway SiteWise Edge](#).

 Note

AWS IoT SiteWise implanta o aplicativo parceiro como um contêiner Docker. A aplicação é implantada com o recurso NET_ADMIN, de maneira que o contêiner do Docker do Litmus Edge possa ser gerenciado por meio do Litmus Edge Manager. O Litmus Edge requer esse acesso privilegiado para ser executado nos dispositivos. Para obter mais informações sobre os requisitos do Litmus Edge Docker, consulte [Instalação do Docker](#) no QuickStart Guia da documentação do Litmus Edge.

6. Leia o contrato disponível em Autorize o acesso e a implantação e escolha Autorizar. Marcar a caixa concede ao AWS parceiro acesso à sua fonte de dados e permite AWS a implantação no componente do parceiro.

Como ativar manualmente por meio do Litmus Edge

1. Selecione Ative mais tarde no Litmus Edge.
2. Verifique se o Docker está instalado no gateway. Para obter mais informações, consulte [Configure Docker em seu gateway SiteWise Edge](#).

 Note

AWS IoT SiteWise implanta o aplicativo parceiro como um contêiner Docker. A aplicação é implantada com o recurso NET_ADMIN, de maneira que o contêiner do Docker do Litmus Edge possa ser gerenciado por meio do Litmus Edge Manager. O Litmus Edge requer esse acesso privilegiado para ser executado nos dispositivos. Para obter mais informações sobre os requisitos do Litmus Edge Docker, consulte [Instalação do Docker](#) no QuickStart Guia da documentação do Litmus Edge.

3. Leia o contrato disponível em Autorize o acesso e a implantação e escolha Autorizar. Marcar a caixa concede ao AWS parceiro acesso à sua fonte de dados e permite AWS a implantação no componente do parceiro.
4. Depois que a implantação for concluída, siga as instruções em [Access the Litmus Edge Web UI](#) no QuickStart Guide da documentação do Litmus Edge.

 Note

O software do parceiro é desenvolvido, mantido e suportado pelo AWS parceiro. AWS não é responsável pela interface, configuração ou software.

Para obter mais informações, consulte [Litmus Edge](#).

8. Escolha Salvar.

SiteWise Opções de fonte de dados do parceiro Edge Gateway

AWS IoT SiteWise permite conectar e ingerir dados de várias fontes de dados de parceiros, como equipamentos industriais, sensores e outros sistemas de terceiros. Para conectar uma fonte de dados de um parceiro, você precisa seguir algumas etapas, incluindo configurar a fonte de dados para a qual enviar dados AWS IoT SiteWise, configurar as permissões e a autenticação necessárias e mapear os dados para seus modelos de ativos. Esse processo garante que os dados do parceiro sejam perfeitamente integrados ao ambiente do AWS IoT SiteWise, permitindo que você os monitore e analise com as outras fontes de dados.

Esta seção lista os parceiros disponíveis para integração de fontes de dados de terceiros nos gateways SiteWise Edge. Use as informações abaixo para configurar uma fonte de dados do parceiro.

 Note

Você pode adicionar uma fonte de dados para cada parceiro em cada gateway

CloudRail

Portal:

<https://devices.cloudrail.com/>

Requisitos

Para ter mais informações sobre os requisitos do CloudRail, consulte [FAQS](#) no site do CloudRail.

Documentação do CloudRail:

[Computação de SiteWise ponta: borda](#)

EasyEdge

Portal:

<https://studio.easyedge.io/>

Requisitos

[Requisitos da EasyEdge](#): informações sobre os requisitos do EasyEdge, inclusive endpoints e portas necessários para configurar o firewall. Observação: você precisará de uma conta da EasyEdge para ter acesso a essa documentação.

Documentação da EasyEdge:

[EasyEdgepara AWS](#)

Litmus Edge

Acesso ao Litmus Edge Manager:

Para acessar o Litmus Edge, configure uma conta do [Litmus Edge Manager](#).

Requisitos

[Requisitos do Litmus Edge](#): recomendação de configurações e requisitos do sistema para implantar o Litmus Edge.

Documentação do Litmus:

- [Integração com AWS IoT SiteWise](#)

- [Documentação do Litmus Edge](#)

AWS IoT Greengrass componentes para AWS IoT SiteWise Edge

SiteWise O Edge usa AWS IoT Greengrass componentes para coletar, processar e transmitir dados industriais na borda. Esses componentes trabalham juntos para permitir o processamento local de dados e a integração perfeita com o serviço de AWS IoT SiteWise nuvem.

Editora de IoT SiteWise

O componente SiteWise editor de IoT (`aws.iot.SiteWiseEdgePublisher`) é responsável por:

- Transmitindo com segurança os dados coletados para o serviço de nuvem AWS IoT SiteWise
- Gerenciando o buffer de dados e as novas tentativas durante problemas de conectividade

Para obter mais informações sobre como configurar o editor para o SiteWise Edge, consulte [Configurar o componente AWS IoT SiteWise do editor](#). E, para obter mais informações sobre o componente editor, consulte [SiteWise Editor de IoT](#) no Guia do AWS IoT Greengrass Version 2 desenvolvedor.

Processador de IoT SiteWise

O componente do SiteWise processador de IoT (`aws.iot.SiteWiseEdgeProcessor`) executa as seguintes tarefas:

- Executando transformações de dados e cálculos na borda
- Implementando definições e cálculos de propriedades de ativos localmente
- Reduzir o volume de dados agregando ou filtrando dados antes da transmissão

Para obter mais informações sobre o componente do processador, consulte [SiteWise Processador de IoT](#) no Guia do AWS IoT Greengrass Version 2 desenvolvedor.

Coletor IoT SiteWise OPC UA

O componente coletor (`aws.iot.SiteWiseEdgeCollectorOpcua`) do IoT SiteWise OPC UA foi projetado para:

- Conecte-se aos servidores OPC UA em ambientes industriais
- Colete dados de fontes de dados OPC UA de forma eficiente
- Transforme dados OPC UA em um formato compatível com AWS IoT SiteWise

Para obter mais informações sobre o componente coletor OPC UA, consulte o [coletor IOT SiteWise OPC UA](#) no Guia do desenvolvedor.AWS IoT Greengrass Version 2

Simulador de fonte de SiteWise dados IoT OPC UA

O componente do simulador de fonte de dados IoT SiteWise OPC UA (`aws.iot.SiteWiseEdgeOpcuaDataSourceSimulator`) fornece as seguintes funcionalidades:

- Inicia um servidor OPC UA local que gera dados de amostra
- Simula uma fonte de dados que pode ser lida pelo componente coletor AWS IoT SiteWise OPC UA em um gateway AWS IoT SiteWise
- Permite a exploração de AWS IoT SiteWise recursos usando os dados de amostra gerados

Esse componente é particularmente útil para fins de teste e desenvolvimento, permitindo simular fontes de dados industriais sem a necessidade de equipamento físico.

Para obter mais informações sobre o componente de simulação de fonte de dados, consulte o [simulador de fonte de dados IoT SiteWise OPC UA](#) no Guia do desenvolvedor.AWS IoT Greengrass Version 2

Esses AWS IoT Greengrass componentes funcionam para habilitar a funcionalidade SiteWise do Edge. O SiteWise editor de IoT garante que os dados sejam enviados de forma confiável para a nuvem, o SiteWise processador de IoT lida com cálculos locais e otimização de dados, e o coletor IoT SiteWise OPC UA facilita a integração com protocolos industriais comuns.

Note

Para usar esses componentes, você deve ter AWS IoT Greengrass V2 ou instalá-los posteriormente em seus dispositivos de borda. A configuração adequada de cada componente é importante para o desempenho ideal do SiteWise Edge.

Filtrar 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, `<root-asset-id>` substituindo-a pela 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
```

Configure o suporte de proxy e gerencie repositórios confiáveis para o AWS IoT SiteWise Edge

No AWS IoT SiteWise Edge, configure e gerencie repositórios confiáveis para configurar o suporte de proxy para seus dispositivos de borda. Primeiro, defina a configuração do proxy e, em seguida, configure os repositórios confiáveis. Você pode configurar armazenamentos confiáveis durante a instalação do gateway ou manualmente após o estabelecimento do gateway.

- **Proxies** — Facilite a conectividade entre seus dispositivos e AWS serviços de ponta em vários ambientes de rede.
- **Armazenamentos confiáveis** — garanta conexões seguras gerenciando certificados confiáveis. As configurações adequadas ajudam você a cumprir suas políticas de segurança de rede, permitir a comunicação em ambientes de rede restritos e otimizar a transferência de dados entre dispositivos periféricos e serviços em nuvem.

SiteWise O Edge utiliza vários repositórios confiáveis para diferentes tipos de componentes, garantindo um fluxo de dados seguro e eficiente de seus dispositivos de borda para a nuvem. Você pode configurar repositórios confiáveis e proxies em um gateway existente ou durante o processo de instalação ao criar um novo gateway.

Requisitos para configurações de armazenamento confiável e proxy

Antes de configurar um armazenamento confiável ou instalar o SiteWise Edge com configurações de proxy, certifique-se de atender aos pré-requisitos. Existem vários requisitos de implementação com base nos requisitos de uso e funcionalidade de seus componentes.

Requisitos de suporte de proxy

- O URL do seu servidor proxy. O URL deve incluir as informações do usuário, o número da porta do host. Por exemplo, `.scheme://[userinfo@]host[:port]`
 - **scheme**— Deve ser HTTP ou HTTPS
 - (Opcional) **userinfo** — Informações de nome de usuário e senha
 - **host**— O nome do host ou endereço IP do servidor proxy

- `port`— O número da porta
- Uma lista de endereços para ignorar o proxy.
- (Opcional) O arquivo de certificado de CA do proxy se você estiver usando um proxy HTTPS com um certificado autoassinado.

Requisitos da Trust Store

- Para obter a funcionalidade completa do pacote de processamento de dados com o proxy HTTPS, você deve atualizar todos os três repositórios confiáveis.
- Se você usa somente o coletor IoT SiteWise OPC UA e o editor de SiteWise IoT, atualize os AWS IoT Greengrass certificados Core e Java Trust Stores para a versão mais recente.

Práticas recomendadas para configurações de borda de servidor proxy e armazenamento confiável

Para manutenção contínua e para manter o mais alto nível de segurança em seu ambiente de borda:

- Revise e atualize regularmente as configurações de proxy para se alinhar aos requisitos de segurança da sua rede.
- Monitore a conectividade do gateway e o fluxo de dados para garantir a comunicação adequada por proxy
- Mantenha e atualize os repositórios confiáveis de acordo com as políticas de gerenciamento de certificados da sua organização
- Você pode implementar e seguir nossas melhores práticas recomendadas para comunicação segura em ambientes periféricos, como:
- Documente suas configurações de proxy e armazenamento confiável para obter visibilidade operacional
- Siga as práticas de segurança da sua organização para gerenciamento de credenciais

Essas práticas ajudam a manter operações seguras e confiáveis para seus gateways SiteWise Edge, ao mesmo tempo em que permanecem alinhadas com suas políticas de segurança mais amplas.

Defina as configurações de proxy durante a instalação do AWS IoT SiteWise Edge Gateway

Você pode configurar o AWS IoT SiteWise Edge para trabalhar com um servidor proxy durante a instalação do gateway. O script de instalação suporta proxies HTTP e HTTPS e pode configurar automaticamente armazenamentos confiáveis para conexões de proxy seguras.

Quando você executa o script de instalação com configurações de proxy, ele executa várias tarefas importantes:

- Valida o formato e os parâmetros do URL do proxy para garantir que eles sejam especificados corretamente.
- Faz o download e instala as dependências necessárias por meio do proxy configurado.
- Se um certificado de CA proxy for fornecido, ele será anexado ao certificado CA AWS IoT Greengrass raiz e importado para o Java KeyStore.
- Configura AWS IoT Greengrass (que o SiteWise Edge usa) para usar o proxy em todas as conexões de saída.
- Conclui a instalação do SiteWise Edge com as configurações apropriadas de proxy e armazenamento confiável.

Para definir as configurações de proxy ao instalar o software de gateway

1. Crie um gateway SiteWise Edge. Para obter mais informações, consulte [Crie um gateway SiteWise Edge auto-hospedado](#) e [Instale o software AWS IoT SiteWise Edge Gateway em seu dispositivo local](#).
2. Execute o script de instalação com as configurações de proxy apropriadas para seu ambiente. Substitua os espaços reservados por suas informações específicas de proxy

Substitua cada um dos seguintes itens:

- `-p, --proxy-url` — O URL do servidor proxy. O URL deve ser um `http` ou `https`.
- `-n, --no-proxy` — Uma lista de endereços separados por vírgulas para ignorar o proxy.
- (Opcional) `-c, --proxy-ca-cert` — Caminho para o arquivo de certificado CA do proxy.
- (Opcional) `-j, --javastorepass` — A KeyStore senha Java. A senha padrão é `changeit`.

Linux

Para sistemas Linux, use a seguinte estrutura de comando:

```
sudo ./install.sh -p proxy-url -n no-proxy-addresses [-c proxy-ca-cert-path] [-j javastorepass]
```

Windows

Para Microsoft Windows sistemas que usam PowerShell, use esta estrutura de comando:

```
.\install.ps1 -ProxyUrl proxy-url -NoProxyAddresses no-proxy-addresses [-ProxyCaCertPath proxy-ca-cert-path] [-JavaStorePass javastorepass]
```

Solução de problemas durante a instalação habilitada por proxy

Para obter mais informações sobre como resolver problemas de armazenamento confiável relacionados a um gateway SiteWise Edge, consulte [Problemas de instalação habilitada para proxy](#).

Configure manualmente armazenamentos confiáveis para suporte a proxy HTTPS no AWS IoT SiteWise Edge

Ao configurar os componentes do AWS IoT SiteWise Edge para se conectar por meio de um proxy HTTPS, adicione o certificado do servidor proxy aos repositórios confiáveis apropriados. SiteWise O Edge usa vários repositórios confiáveis para proteger as comunicações. Há três repositórios confiáveis e seu uso deles depende do tipo de componente SiteWise Edge na implementação do gateway.

Os repositórios fiduciários são atualizados automaticamente durante o processo de instalação quando as configurações de proxy são fornecidas.

- [Configurar um repositório confiável de componentes AWS IoT Greengrass principais](#)— O certificado CA AWS IoT Greengrass raiz está incluído nos repositórios confiáveis para verificar a autenticidade dos AWS serviços.

Esse armazenamento confiável ajuda AWS IoT Greengrass os componentes a se comunicarem com segurança com os AWS serviços por meio do proxy, ao mesmo tempo em que verifica a autenticidade desses serviços.

- [Configurar um armazenamento confiável de componentes baseado em Java](#)— O Java KeyStore (JKS) é o principal armazenamento confiável usado por componentes baseados em Java para conexões. SSL/TLS

Os aplicativos Java dependem do JKS para estabelecer conexões seguras. Por exemplo, se você estiver usando o SiteWise editor de IoT ou o coletor IoT SiteWise OPC UA, que são baseados em Java, precisará configurar esse armazenamento confiável. Isso garante que esses componentes possam se comunicar com segurança por meio do proxy HTTPS ao enviar dados para a nuvem ou coletar dados dos servidores OPC UA.

- [Configuração do armazenamento confiável de componentes em nível de sistema](#)— Ao usar proxies HTTPS, seus certificados devem ser adicionados aos repositórios confiáveis apropriados para permitir conexões seguras.

Ao usar proxies HTTPS, seus certificados devem ser adicionados aos repositórios confiáveis apropriados para permitir conexões seguras. Isso é necessário porque os componentes no nível do sistema, geralmente escritos em linguagens como Rust ou Go, dependem do armazenamento confiável do sistema em vez do JKS do Java. Por exemplo, se você estiver usando utilitários do sistema que precisam se comunicar por meio do proxy (como para atualizações de software ou sincronização de horário), você precisará configurar o armazenamento confiável no nível do sistema. Isso garante que esses componentes e utilitários possam estabelecer conexões seguras por meio do proxy.

Configurar um repositório confiável de componentes AWS IoT Greengrass principais

Para funções AWS IoT Greengrass principais que usam a CA raiz da Amazon:

1. Localize o arquivo do certificado em `/greengrass/v2/AmazonRootCA1.pem`
2. Anexe o certificado raiz do proxy HTTPS (autoassinado) a esse arquivo.

```
-----BEGIN CERTIFICATE-----
MIIEFTCCA v2gAwIQWgIVAMHSAzWG/5YVRYtRQ0xXUTEpHuEmApzGCSqGSIb3DQEK
\ nCwUAhuL9MQswCQwJVUzEPMAVUzEYMBYGA1UECgwP1hem9uLmNvbSBjbMuMRww
... content of proxy CA certificate ...
+vHIR1t0e5JAm5\ noTIZGoFbK82A0/ n07f/ t5PSIDAim9V3Gc3pSXxCCAQoFYnui
GaPU1Gk1gCE84a0X\ n7Rp/ 1ND/ PuMZ/ s8Yj1kY2NmYmNjMCAXDTE5MTEyN2cM216
gJMIADggEPADf2/ m45hzEXAMPLE=
-----END CERTIFICATE-----
```



```

-----BEGIN CERTIFICATE-----
MIIDQTCCAimgF6AwIBAgITBmyfz/5mjAo54vB4ikPmljZKyjANJmApzyMZFo6qBg
ADA5MQswCQYDVQQGEwJVUzEPMA0tMVT8Q0tPHRh8jrdkGA1UEChMGMGdV3QQDExBBKW
... content of root CA certificate ...
o/ufQJQWUCyziar1hem9uMRkwFwYVPSHCb2XV4cdFyQzR1KldZwgJcIQ6XUDgHaa
5MsI+yMRQ+hDaXJioblXgUka642M4UwtBV8oK2xJNDd2ZhwLnoQdeXeGADKkpy
rqXRfKoQnoZsG4q5WTP46EXAMPLE
-----END CERTIFICATE-----

```

Configurar o proxy HTTPS em um gateway estabelecido

Você pode adicionar suporte de proxy a um gateway estabelecido conectando-se à porta 443 em vez da porta 8883. Para obter mais informações sobre como usar um servidor proxy, consulte [Conectar na porta 443 ou por meio de um proxy de rede](#) no Guia do AWS IoT Greengrass Version 2 desenvolvedor. Se você criar um novo gateway, poderá definir a configuração do proxy durante a instalação do gateway. Para obter mais informações, consulte [Defina as configurações de proxy durante a instalação do AWS IoT SiteWise Edge Gateway](#).

Quando você usa um proxy HTTPS com o AWS IoT Greengrass on SiteWise Edge, o software escolhe automaticamente entre HTTP e HTTPS para conexões de proxy com base na URL fornecida.

Important

Atualize todos os repositórios confiáveis necessários antes de tentar se conectar por meio de um proxy HTTPS.

Configurar um armazenamento confiável de componentes baseado em Java

Para o SiteWise editor de IoT, o coletor IoT SiteWise OPC UA e serviços Java no pacote de processamento de dados, o local padrão do armazenamento confiável de Java é `$JAVA_HOME/jre/lib/security/cacerts`

Para adicionar um certificado

1. Crie um arquivo para armazenar o certificado do servidor proxy, como `comoproxy.crt`.

Note

Crie o arquivo com antecedência usando o certificado do servidor proxy.

2. Adicione o arquivo ao armazenamento confiável do Java usando o seguinte comando:

```
sudo keytool -import -alias proxyCert -keystore /usr/lib/jvm/java-11-openjdk-amd64/lib/security/cacerts -file proxy.crt
```

3. Quando solicitado, use a senha padrão: `changeit`

Configuração do armazenamento confiável de componentes em nível de sistema

Para componentes escritos em Rust, Go e outras linguagens que usam o armazenamento confiável do sistema:

Linux

Sistemas Linux: adicione certificados a `/etc/ssl/certs/ca-certificates.crt`

Windows

Microsoft Windows sistemas: Para configurar o armazenamento confiável, siga o procedimento do [Armazenamento de Certificados](#) na documentação do Microsoft Ignite.

O Windows oferece vários repositórios de certificados, incluindo repositórios separados para os escopos do Usuário e do Computador, cada um com vários subrepositórios. Para a maioria das configurações do SiteWise Edge, recomendamos adicionar certificados à `COMPUTER | Trusted Root Certification Authorities` loja. No entanto, dependendo da configuração específica e dos requisitos de segurança, talvez seja necessário usar uma loja diferente.

Solução de problemas do Trust Store

Para obter mais informações sobre como resolver problemas de armazenamento confiável relacionados a um gateway SiteWise Edge, consulte [Problemas com a Trust Store](#).

Use AWS IoT SiteWise APIs na borda

AWS IoT SiteWise fornece um subconjunto do ITS APIs, juntamente com o específico da borda APIs, permitindo uma interação perfeita com os modelos de ativos e seus ativos associados implantados

na borda. Esses modelos de ativo devem ser configurados para serem executados na borda. Para ter mais informações e conferir instruções detalhadas sobre esse processo de configuração, consulte [Configurar um modelo de ativo para processamento de dados no SiteWise Edge](#).

Depois de configurá-los APIs, você pode recuperar dados abrangentes sobre seus modelos de ativos e ativos individuais. A recuperação de informações sobre modelos de ativo, ativos, painéis, portais e projetos pode ajudar você a monitorar portais e painéis implantados, além de acessar dados de ativo coletados ao nível da borda. Isso fornece um host central em sua rede para interações AWS IoT SiteWise sem exigir uma chamada de API da web.

Tópicos

- [Todos os dispositivos AWS IoT SiteWise Edge disponíveis APIs](#)
- [Somente Edge APIs para uso com AWS IoT SiteWise dispositivos Edge](#)
- [Habilite o CORS on AWS IoT SiteWise Edge APIs](#)
- [Configurar tempos limite de sessão para AWS IoT SiteWise o Edge](#)
- [Tutorial: Listar modelos de ativos em um gateway AWS IoT SiteWise Edge](#)

Todos os dispositivos AWS IoT SiteWise Edge disponíveis APIs

AWS IoT SiteWise fornece uma variedade de dispositivos de ponta APIs para que você possa concluir tarefas localmente no dispositivo. Algumas das vantagens disponíveis APIs incluem a recuperação de modelos de ativos, a criação e atualização de propriedades de ativos e o envio de fluxos de dados para a nuvem. Ao aproveitá-las APIs, você pode criar soluções que possam operar em ambientes com conectividade de rede intermitente ou limitada.

Disponível AWS IoT SiteWise APIs

Os itens a seguir AWS IoT SiteWise APIs estão disponíveis em dispositivos Edge:

- [ListAssetModels](#)
- [DescribeAssetModel](#)
- [ListAssets](#)
- [DescribeAsset](#)
- [DescribeAssetProperty](#)
- [ListAssociatedAssets](#)

- [GetAssetPropertyAggregates](#)
- [GetAssetPropertyValue](#)
- [GetAssetPropertyValueHistory](#)
- [ListDashboards](#)
- [ListPortals](#)
- [ListProjectAssets](#)
- [ListProjects](#)
- [DescribeDashboard](#)
- [DescribePortal](#)
- [DescribeProject](#)

Disponível somente para borda APIs

Os itens a seguir APIs são usados localmente em dispositivos na borda:

- [Authenticate](#) — Use essa API para obter as credenciais temporárias do SigV4 que você usará para fazer chamadas de API.

Somente Edge APIs para uso com AWS IoT SiteWise dispositivos Edge

Além dos AWS IoT SiteWise APIs que estão disponíveis na borda, existem outros específicos para a borda. Essas bordas específicas APIs 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: string

Obrigatório: Sim

password

A senha do usuário solicitando as credenciais.

Tipo: string

Obrigatório: Sim

authMechanism

O método de autenticação para validar esse usuário no host.

Tipo: String

Valores válidos: ldap, linux, winnt

Exigido: 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. O tamanho máximo é 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 malformatado. 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

Habilite o CORS on AWS IoT SiteWise Edge APIs

A ativação do CORS (Cross-Origin Resource Sharing) no AWS IoT SiteWise Edge APIs permite que os aplicativos da web se comuniquem diretamente com eles APIs em diferentes domínios. Isso permite integração perfeita, troca de dados em tempo real e acesso a dados entre domínios sem servidores intermediários ou soluções alternativas. As configurações do CORS podem ser definidas para especificar origens permitidas, garantindo acesso controlado entre origens.

Note

O CORS está disponível para a versão 3.3.1 e posterior do Este recurso está disponível para a versão 3.3.1 e posterior do componente. `aws.iot.SiteWiseEdgeProcessor` Para obter mais informações, consulte o [AWS IoT SiteWise processador](#) no Guia do AWS IoT Greengrass Version 2 desenvolvedor.

Para habilitar o CORS no SiteWise Edge APIs

1. Navegue até o [console do AWS IoT SiteWise](#).
2. No painel de navegação, escolha Gateways de borda.
3. Selecione o gateway SiteWise Edge para o qual você deseja habilitar o CORS. Você pode habilitar o CORS no tipo AWS IoT Greengrass V2 de implantação.
4. Na seção Configuração do gateway, escolha o dispositivo principal do Greengrass associado.

5. Na guia Implantações, em Dispositivos Greengrass, selecione o link de implantação apropriado.
6. Em Ações, escolha Revisar e, em seguida, Revisar implantação.

 Important

A criação de uma configuração revisada habilitada para CORS substitui a configuração atual do dispositivo.

7. Na Etapa 1, Especifique o destino, forneça um Nome opcional para identificar a implantação.
8. Na Etapa 2, Selecionar componentes - opcional, você pode deixar todas as seleções atuais como estão e escolher Avançar.
9. Na Etapa 3, Configurar componentes - opcional, selecione aws.iot. SiteWiseEdgeProcessore escolha Configurar componente.
10. Na seção Atualização de configuração, em Configuração para mesclar, insira o seguinte JSON:

```
{
  "AWS_SITEWISE_EDGE_ACCESS_CONTROL_ALLOW_ORIGIN": "*"
}
```

 Note

Usar * como valor para AWS_SITEWISE_EDGE_ACCESS_CONTROL_ALLOW_ORIGIN permite todas as origens. Para ambientes de produção, é recomendável especificar a origem exata URLs para melhorar a segurança.

11. Escolha Confirmar.
12. Escolha Avançar para prosseguir com as etapas restantes até chegar à Etapa 5, Revisão.
13. Revise suas alterações de configuração e escolha Implantar para aplicar as alterações ao seu gateway SiteWise Edge.

 Note

Como alternativa, você pode habilitar o CORS definindo globalmente AWS_SITEWISE_EDGE_ACCESS_CONTROL_ALLOW_ORIGIN a variável ambiental como * em seu AWS IoT SiteWise gateway.

 Note

Para proxy autenticado, `userinfo` deve ser incluído no `url` campo na configuração do proxy `username` e não como `password` campos separados.

Depois que a implantação for concluída, o CORS será ativado em sua API do SiteWise Edge, permitindo que origens especificadas façam solicitações de origem cruzada para a API.

Configurar tempos limite de sessão para AWS IoT SiteWise o Edge

SiteWise O Edge permite que você configure o tempo limite de sessão para a API do SiteWise Edge. Esse recurso aumenta a segurança ao encerrar automaticamente as sessões inativas após um período de tempo especificado. Esta seção orienta você pelo processo de configuração do tempo limite da sessão usando o Console do AWS IoT SiteWise

 Note

A configuração do tempo limite da sessão está disponível para a versão 3.4.0 e posterior do `aws.iot.SiteWiseEdgeProcessor` componente. Para obter mais informações, consulte o [AWS IoT SiteWise processador](#) no Guia do AWS IoT Greengrass Version 2 desenvolvedor.

Para configurar um tempo limite de sessão para um gateway SiteWise Edge

1. Navegue até o [console do AWS IoT SiteWise](#).
2. No painel de navegação, escolha Gateways de borda.
3. Escolha o gateway SiteWise Edge em que você deseja configurar o tempo limite da sessão.

 Note

Você pode configurar o tempo limite da sessão no tipo AWS IoT Greengrass V2 de implantação.

4. Na seção Configuração do gateway, escolha o dispositivo principal do Greengrass associado.
5. Na guia Implantações, em Dispositivos Greengrass, selecione o link de implantação apropriado.
6. Em Ações, escolha Revisar. Leia o aviso e escolha Revisar implantação.

 Important

A criação de uma configuração de tempo limite de sessão revisada substitui a configuração atual do dispositivo.

7. Na Etapa 1, Especifique o destino, forneça um Nome opcional para identificar a implantação revisada e escolha Avançar.
8. Na Etapa 2, Selecionar componentes - opcional, você pode deixar todas as seleções atuais como estão e escolher Avançar.
9. Na Etapa 3, Configurar componentes - opcional, selecione aws.iot. SiteWiseEdgeProcessore escolha Configurar componente.
10. Na seção Atualização de configuração, em Configuração para mesclar, insira o seguinte JSON:

```
{  
  "AWS_SITEWISE_EDGE_SESSION_TIMEOUT_MINUTES": "240"  
}
```

11. Defina o valor AWS_SITEWISE_EDGE_SESSION_TIMEOUT_MINUTES em minutos. Os valores de tempo limite da sessão podem ser de 1 minuto a 10080 minutos (7 dias). O valor padrão é 240 minutos (4 horas).
12. Escolha Confirmar.
13. Escolha Avançar para prosseguir com as etapas restantes até chegar à Etapa 5, Revisão.
14. Revise suas alterações de configuração e escolha Implantar para aplicar as alterações ao seu gateway SiteWise Edge.

 Note

Como alternativa, você pode configurar o tempo limite da sessão definindo a variável ambiental global AWS_SITEWISE_EDGE_SESSION_TIMEOUT_MINUTES para o valor desejado (em minutos) no gateway do Edge. SiteWise

Depois que a implantação for concluída, a nova configuração de tempo limite da sessão será aplicada à sua API do SiteWise Edge.

Tutorial: Listar modelos de ativos em um gateway AWS IoT SiteWise Edge

Você pode usar um subconjunto do disponível AWS IoT SiteWise APIs junto com o específico da borda APIs para interagir com os modelos de ativos 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 [AWS IoT SiteWise Requisitos de gateway auto-hospedado do Edge](#) implantado e em execução
- Acesso ao seu gateway SiteWise Edge na mesma rede pela porta 443.
- [OpenSSL](#) instalado
- (AWS OpsHub para AWS IoT SiteWise) O [AWS IoT SiteWise aplicativo 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 a APIs disponível 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 obter mais informações, consulte [Gerencie 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>'
```

Etapas 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 de 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 usá-las APIs em seu SiteWise gateway Edge. 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 IoT SiteWise aplicativo AWS OpsHub for](#) instalado.

Para usar o AWS IoT SiteWise aplicativo AWS OpsHub para obter suas credenciais temporárias, faça o seguinte:

1. Faça login no aplicativo.
2. Escolha Settings.
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 o. 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  
}
```

Hospede um gateway SiteWise Edge em Siemens Industrial Edge

Hospede seu gateway no Siemens Industrial Edge usando o aplicativo AWS IoT SiteWise Edge. Assim como com AWS IoT Greengrass V2, você pode otimizar os processos de fabricação ou melhorar os fluxos de trabalho operacionais usando o SiteWise Edge on Siemens Industrial Edge.

Você pode ingerir dados do seu dispositivo Siemens Industrial Edge para sua AWS conta executando um gateway SiteWise Edge no dispositivo. Para fazer isso, solicite acesso ao aplicativo AWS IoT SiteWise Edge da equipe de suporte do SiteWise Edge. Em seguida, crie um recurso de gateway SiteWise Edge com uma meta de implantação do dispositivo Siemens Industrial Edge - novo. Em seguida, faça download do arquivo de configuração e faça upload dele na aplicação por meio do portal Siemens Industrial Edge Management. Para ter mais informações sobre a execução de aplicações no Siemens Industrial Edge, inclusive como configurar os recursos necessários da Siemens, consulte [What is Industrial Edge?](#) na documentação da Siemens.

Note

A Siemens não é fornecedora nem fornecedora do Edge. SiteWise O Siemens Industrial Edge Marketplace é um mercado independente.

Tópicos

- [Segurança](#)
- [Siemens Secure Storage e o aplicativo AWS IoT SiteWise Edge](#)

- [Destinos para Siemens Industrial Edge dispositivos](#)
- [Migrar da aplicação de pré-visualização](#)
- [Solução de problemas](#)
- [AWS IoT SiteWise Registro de alterações do aplicativo Edge](#)
- [Requisitos para o aplicativo AWS IoT SiteWise Edge](#)
- [Criar um gateway para o Siemens Industrial Edge](#)
- [Criar um Siemens Databus user para a aplicação](#)
- [Acesse o aplicativo AWS IoT SiteWise Edge](#)
- [Instale o aplicativo em um Siemens dispositivo](#)
- [Atualizar a configuração do aplicativo AWS IoT SiteWise Edge](#)

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 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.
- Verificar outras aplicações disponíveis no marketplace do parceiro.

Siemens Secure Storage e o aplicativo AWS IoT SiteWise Edge

Para proteger as credenciais e os segredos necessários para executar o aplicativo AWS IoT SiteWise Edge, Siemens Industrial Edge fornece mecanismos para armazenar com segurança as

credenciais no dispositivo. A aplicação do AWS IoT SiteWise Edge não será executada em um dispositivo se não tiver suporte para armazenar essas credenciais em segurança. As falhas de execução causadas pela falta de suporte ao Secure Storage são registradas em arquivos de log.

As seguintes versões mínimas do sistema operacional são necessárias para instalar e executar o aplicativo AWS IoT SiteWise Edge. Atualize os dispositivos para as versões mais recentes a fim de instalar a aplicação.

- Para dispositivos virtuais: IEVD versão 1.19 ou posterior
- Para dispositivos físicos: IED-OS versão 2.2 ou posterior

O aplicativo AWS IoT SiteWise Edge ativado não Siemens Industrial Edge será executado até que você atualize seu dispositivo.

Destinos para Siemens Industrial Edge dispositivos

Ao usar o aplicativo AWS IoT SiteWise Edge ativado Siemens Industrial Edge, os destinos ajudam a preparar os dados antes de enviá-los AWS IoT SiteWise para análise e distribuição adicionais. Você pode definir as configurações de destino de dados para ingestão de dados em buffer usando o Amazon S3 ou usar a ingestão de dados em tempo real. Ambos permitem que você assine tópicos do MQTT usando filtros de caminho no destino de implantação do Siemens Industrial Edge dispositivo.

O destino Siemens Industrial Edge de implantação em seu gateway oferece suporte a dois métodos principais de tratamento de dados:

- AWS IoT SiteWise configurações em tempo real - Os dados são enviados diretamente à AWS IoT SiteWise medida que são coletados
- AWS IoT SiteWise armazenados em buffer usando as configurações do Amazon S3 - Os dados são coletados e armazenados temporariamente em lotes antes de serem enviados para o Amazon S3

Para obter mais informações sobre como configurar essas opções, consulte [Adicione um destino em AWS IoT SiteWise buffer usando o Amazon S3](#) e [Adicione um destino em tempo real do AWS IoT SiteWise Edge](#)

Prefixos para filtros de caminho

Os filtros de caminho para gateways que usam destinos de Siemens Industrial Edge implantação combinam o tópico e o nome do fluxo de dados para criar um identificador exclusivo para seus dados. O tópico combinado com o nome do fluxo de dados é chamado de prefixo nos Siemens Industrial Edge gateways. Isso difere dos gateways auto-hospedados, nos quais os filtros de caminho são baseados exclusivamente nos tópicos do MQTT.

Exemplo Estrutura de filtro de caminho para fluxos de dados da Siemens

Um filtro de caminho típico para um fluxo de dados da Siemens inclui o caminho do tópico e o nome do fluxo de dados:

```
ie/d/device1/application1/datastream1
```

Em que:

- `ie/d/` é o prefixo necessário para fluxos de dados da Siemens
- `device1/application1` representa o caminho hierárquico
- `datastream1` é o nome específico do fluxo de dados

Note

Ao trabalhar com fluxos de Siemens Industrial Edge dados, certifique-se de incluir os tópicos metadados (`ie/m/`) e dados (`ie/d/`) em seus filtros de caminho para receber informações completas sobre seus fluxos de dados.

Destinos e filtros de caminho

Veja os tópicos a seguir para saber mais sobre destinos e filtros de caminho em gateways habilitados para MQTT:

- [AWS IoT SiteWise Entenda os destinos Edge](#)
- [Adicione um destino em tempo real do AWS IoT SiteWise Edge](#)
- [Adicione um destino em AWS IoT SiteWise buffer usando o Amazon S3](#)
- [Entenda os filtros de caminho para destinos AWS IoT SiteWise do Edge](#)

- [Adicione filtros de caminho aos destinos AWS IoT SiteWise do Edge](#)
- [Gerenciar destinos AWS IoT SiteWise do Edge](#)

Migrar da aplicação de pré-visualização

Se você executou o SiteWise Edge Siemens Industrial Edge durante a fase de pré-visualização, precisará atualizar da versão prévia, versão 1.0.1, para a versão mais recente. Faça o seguinte para migrar:

1. Crie novos gateways SiteWise Edge. Para obter mais informações, consulte [Criar um gateway para o Siemens Industrial Edge](#).
2. Crie um Siemens Databus user para cada novo gateway. Para obter mais informações, consulte [Criar um Siemens Databus user para a aplicação](#).
3. Desinstale o aplicativo AWS IoT SiteWise Edge Gateway versão 1.0.1 em seu IED.

Note

Prepare-se para interrupções no fluxo de dados ao reconfigurar os AWS IoT SiteWise ativos usados anteriormente pela versão prévia do aplicativo AWS IoT SiteWise Edge. Embora o histórico de dados seja preservado, existe a possibilidade de perda de dados ao reinstalar o novo gateway.

4. Exclua os gateways do SiteWise Edge que você criou durante a visualização no [Console do AWS IoT SiteWise](#).
5. Instale o aplicativo AWS IoT SiteWise Edge Gateway no IED usando o novo arquivo de configuração do gateway. Para obter mais informações, consulte [Instale o aplicativo em um Siemens dispositivo](#).

Important

A instalação do novo gateway substitui a versão prévia do aplicativo SiteWise Edge. Não será possível voltar para a versão 1.0.1 depois de instalar a versão 2.0.0.

Depois de configurar o novo gateway e Siemens Databus user, os dados vão fluir para as propriedades.

Você também pode atualizar seu aplicativo SiteWise Edge diretamente da versão. No entanto, uma nova configuração de gateway ainda será necessária.

Solução de problemas

Para solucionar problemas do gateway SiteWise Edge em seu Siemens Industrial Edge dispositivo, consulte [Solução de problemas do aplicativo AWS IoT SiteWise Edge em Siemens Industrial Edge](#).

Você também pode acessar o [AWS re:Post](#) para encontrar respostas para as perguntas.

AWS IoT SiteWise Registro de alterações do aplicativo Edge

A tabela a seguir descreve as alterações em cada versão do aplicativo AWS IoT SiteWise Edge.

Versão	Alterações	
3.0.0	Novos recursos - Adiciona opções de configuração adicionais no AWS IoT SiteWise console para gateways instalados em Siemens Industrial Edge: - Adicione e configure destinos do Amazon S3. - Remova o destino AWS IoT SiteWise em tempo real. - Adicione filtros para cada destino para controlar o roteamento de dados. - Adiciona a opção de uma configuração de prefixo global para enviar todos os dados do editor de SiteWise IoT no Siemens IE instalador. O prefixo é aplicado após a filtragem. Correções de bugs e melhorias - Adiciona a capacidade de repetir as conexões com o Siemens Industrial Edge Databus se a tentativa inicial do aplicativo AWS IoT SiteWise Edge falhar.	
2.0.1	Correções de bugs e melhorias	

Versão	Alterações	
	Corrige um problema em que o aplicativo entrava em estado de falha e fechava se não conseguisse recuperar AWS as credenciais na inicialização. Adiciona suporte para tentar novamente até a recuperação bem-sucedida da credencial.	
2.0.0	- O aplicativo AWS IoT SiteWise Edge agora está disponível ao público em geral. - A aplicação requer Siemens IEVD versão 1.19 ou Siemens IED-OS versão 2.2. - Melhorias no desempenho: redução do uso de memória e CPU. - Melhorias na depuração: você já pode fazer upload de um arquivo de configuração opcional para habilitar os logs de depuração. - Melhorias na segurança: a aplicação usa a SecureStorage API para armazenar em segurança as credenciais no dispositivo. - Dockervvalor de resumo: sha256:4a960f29234a190ebb5224c1fd0f3e99faafccc4cb3d93ca13fef247b6656d18	
1.0.1	Lançamento inicial	

Requisitos para o aplicativo AWS IoT SiteWise Edge

Para executar o AWS IoT SiteWise Edge onSiemens 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.
 - O IE App Configuration Service. Para saber mais, consulte [Installing the IE App Configuration Service manually](#) na documentação do Siemens Industrial Edge Management.

- Acesso à versão 2.0.1 ou superior do aplicativo AWS IoT SiteWise Edge. Para obter mais informações, consulte [Acesse o aplicativo AWS IoT SiteWise Edge](#).
- Um dispositivo do Siemens Industrial Edge (IED) ou um dispositivo virtual do Siemens Industrial Edge (IEVD).
 - Pelo menos 15 GB de espaço em disco para os requisitos de hardware.
 - 1 GB de RAM com 1 GB adicional de memória swap.
 - Configuração do dispositivo para permitir tráfego de saída nas portas 443 e 8883.
 - Um processador x86 de 64 bits.
 - Siemens Industrial Edge Management versão 1.13.10 ou posterior.
 - Conformidade do dispositivo com os requisitos do Siemens Secure Storage.
 - Em dispositivos virtuais, IEVD versão 1.19 ou posterior.
 - Em dispositivos físicos, IED-OS versão 2.2 ou posterior.
 - A versão mais recente da Docker Compose.
 - Docker Engine versão 18.091 ou posterior.
- Acesso ao domínio necessário. Para obter mais informações, consulte [AWS IoT SiteWise endpoints](#).

Criar um gateway para o Siemens Industrial Edge

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.

Note

Não se esqueça de atender a todos os requisitos para executar um dispositivo no Siemens Industrial Edge Management. Para obter mais informações, consulte [Requisitos para o aplicativo AWS IoT SiteWise Edge](#).

Como criar o arquivo de configuração

1. Navegue até o [console do AWS IoT SiteWise](#).
2. No painel de navegação, escolha Gateways de borda.
3. Escolha Criar gateway.

4. Para o tipo de implantação, escolha o dispositivo Siemens Industrial Edge.
5. Insira um nome para seu gateway SiteWise Edge ou use o nome gerado por AWS IoT SiteWise.
6. (Opcional) Em 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

Você usa o arquivo de configuração do gateway para fazer backup e restaurar seu aplicativo AWS IoT SiteWise Edge. Salve seu arquivo de configuração do gateway SiteWise Edge [AWS Secrets Manager](#) para armazenar e gerenciar o arquivo com segurança. O Secrets Manager armazena, gerencia e recupera informações confidenciais com segurança.

Criar um Siemens Databus user para a aplicação

AWS IoT SiteWise O Edge on Siemens Industrial Edge ingere dados do Siemens Databus aplicativo. Para conectar o SiteWise Edge ao Siemens Databus, você precisa de um Siemens Databus user que forneça acesso aos dados para os quais você deseja transferir com segurança. AWS IoT SiteWise Para começar, crie um Siemens Databus user e, em seguida, forneça as credenciais para o aplicativo SiteWise Edge.

Para criar um Siemens Databus user

1. Na instância do Siemens Industrial Edge Management, escolha Gerenciamento de borda na seção Aplicações de plataforma.
2. Escolha o ícone Conexões de dados.
3. Selecione Databus. Uma lista dos dispositivos conectados é exibida.
4. Selecione o dispositivo para se conectar ao aplicativo AWS IoT SiteWise Edge.
5. Escolha Executar. O Databus Configurator para o dispositivo selecionado é exibido.

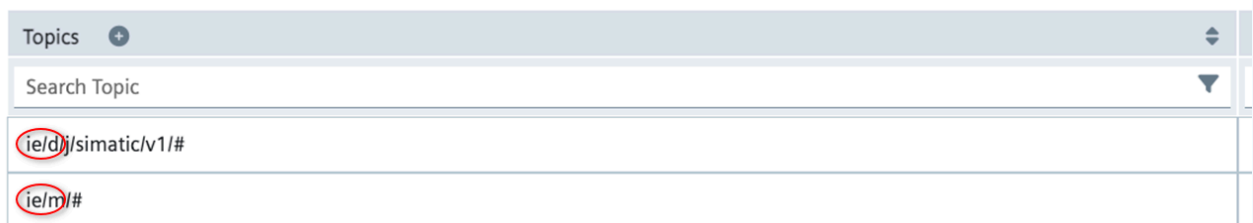
6. Crie um usuário para o dispositivo do Edge em Usuários. Para obter mais informações sobre como criar um usuário, consulte [Usuários](#) na documentação do Siemens Industrial Edge Management.
7. Selecione os tópicos aos quais o Siemens Databus deve ter acesso. Esses tópicos restringem o que o AWS IoT SiteWise Edge pode acessar.

 Important

Todos os tópicos aos quais o Siemens Databus user tem acesso são publicados no AWS IoT SiteWise.

 Note

Um Siemens Databus user precisa acessar os tópicos de dados e de metadados. Os tópicos que começam com `ie/d` são tópicos de dados. Já os tópicos que começam com `ie/m` são tópicos de metadados. Compartilhe tópicos em pares para que o SiteWise Edge tenha acesso aos dados e metadados de cada tópico respectivo.



8. Defina permissões indicadas para a configuração do Siemens Databus.

Depois de criar sua Siemens Databus configuração, você pode instalar o aplicativo AWS IoT SiteWise Edge no seu Siemens Industrial Edge Management. Para obter mais informações, consulte [Instale o aplicativo em um Siemens dispositivo](#).

Opcionalmente, você também pode configurar destinos e filtros de caminho para seu Siemens Industrial Edge gateway. Para obter mais informações, consulte [Destinos e filtros de caminho](#).

Acesse o aplicativo AWS IoT SiteWise Edge

Para obter acesso ao aplicativo AWS IoT SiteWise Edge em Siemens Industrial Edge, [envie um e-mail](#) solicitando acesso à equipe de suporte do SiteWise Edge.

No e-mail, inclua as seguintes informações:

- Seu nome e informações de contato
- Company name (Nome da empresa)
- ID do locatário do Siemens Industrial Edge

Instale o aplicativo em um Siemens dispositivo

Depois de obter acesso ao aplicativo AWS IoT SiteWise Edge enviando um e-mail para a equipe de suporte do SiteWise EdgeSiemens Industrial Edge, atribua o aplicativo a uma instância de. Siemens Industrial Edge Management Em seguida, você pode instalar o aplicativo AWS IoT SiteWise Edge no seu dispositivo.

Para instalar o aplicativo AWS IoT SiteWise Edge

1. Verifique se o Docker resumo fornecido Siemens Industrial Edge Management corresponde à versão mais recente listada no [AWS IoT SiteWise Registro de alterações do aplicativo Edge](#).

Para obter mais informações sobre como localizar o valor Docker resumido da Siemens, consulte [Gerenciando um aplicativo](#) no Siemens Industrial EdgeDispositivo da documentação. Siemens

Siemens Industrial Edge Managementsuporta uma versão do aplicativo AWS IoT SiteWise Edge por vez. Siga esta etapa para garantir que você esteja usando a versão mais recente do aplicativo antes de instalar o aplicativo AWS IoT SiteWise Edge em seu Siemens Industrial Edge dispositivo.

2. Atribua a aplicação do AWS IoT SiteWise Edge ao Siemens Industrial Edge Management. Para ter mais informações, consulte [Managing an app](#) na seção Industrial Edge Management da documentação da Siemens.
3. Em Gerenciamento de borda, navegue pelo catálogo em busca do AWS IoT SiteWise Edge e o escolha.
4. Escolha Instalar.

Note

Se um botão Fale conosco for exibido, escolha-o e siga as etapas para solicitar acesso ao aplicativo AWS IoT SiteWise Edge em Siemens Industrial Edge. Para obter mais informações, consulte [Acesse o aplicativo AWS IoT SiteWise Edge](#).

5. Selecione Databus_Configuration nas opções de configurações do esquema.
6. Insira o Nome do usuário e a Senha para a configuração do Databus. Para ter mais informações sobre como criar um Siemens Databus user, consulte [Criar um Siemens Databus user para a aplicação](#).
7. Escolha o ícone pequeno e redondo de marca de seleção cinza ao lado de Databus_Configuration para deixar o ícone verde.

Note

As configurações de entrada só se aplicarão se o ícone de marca de seleção mudar de cinza para verde. Do contrário, a configuração de entrada será ignorada.

Databus_Configuration Invalid Configuration

Provide Databus user credentials for the AWS IoT SiteWise Edge application to collect data from the Databus application. SiteWise Edge will publish all topics to the cloud that the user has access to. You can manage access using the Databus app

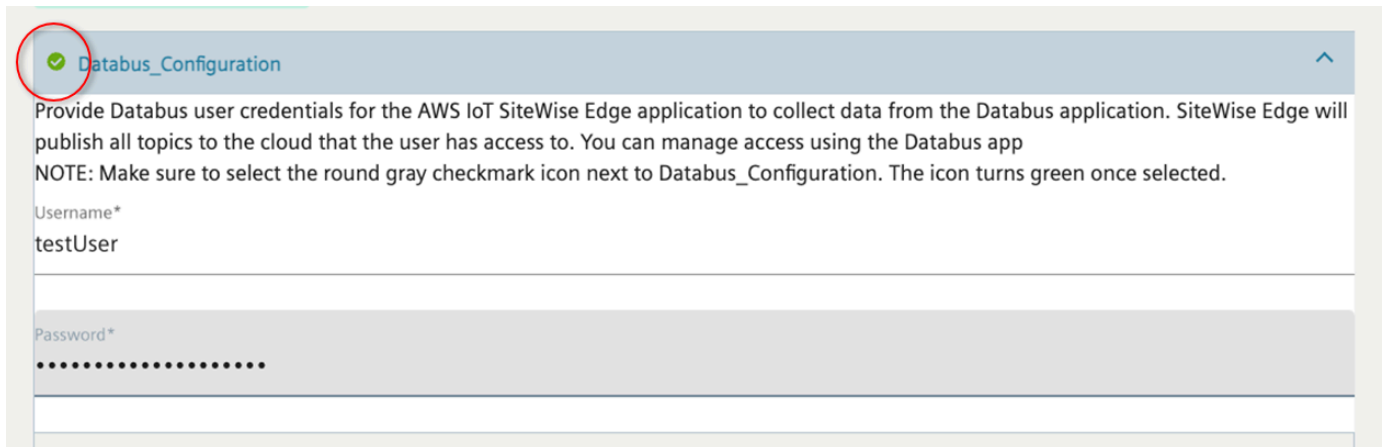
NOTE: Make sure to select the round gray checkmark icon next to Databus_Configuration. The icon turns green once selected.

Username*

is a required property

Password*

is a required property



✓ Databus_Configuration

Provide Databus user credentials for the AWS IoT SiteWise Edge application to collect data from the Databus application. SiteWise Edge will publish all topics to the cloud that the user has access to. You can manage access using the Databus app

NOTE: Make sure to select the round gray checkmark icon next to Databus_Configuration. The icon turns green once selected.

Username*

testUser

Password*

.....

8. Escolha Próximo para ir até Outras configurações, onde você poderá fazer upload do arquivo de configuração do gateway.
9. Escolha SiteWise_Edge_Gateway_Config como o local para carregar o arquivo de configuração do gateway.

 Note

Certifique-se de escolher SiteWise_Edge_Gateway_Config em vez de _Edge_Support_Config_Optional. SiteWise

10. Selecione o dispositivo para instalar a aplicação.
11. Selecione Install now (Instalar agora).

Opcionalmente, você pode configurar o componente editor para exportar dados para a AWS nuvem. Para ter mais informações, consulte [Configure the AWS IoT SiteWise publisher component](#).

Para configurar destinos para seu Siemens Industrial Edge gateway, consulte [Destinos e filtros de caminho](#).

Atualizar a configuração do aplicativo AWS IoT SiteWise Edge

Há algumas coisas a serem consideradas ao atualizar a configuração de um aplicativo AWS IoT SiteWise Edge Siemens Industrial Edge.

 Note

Qualquer alteração na configuração do aplicativo AWS IoT SiteWise Edge requer uma reinicialização do aplicativo.

Razões para reiniciar o aplicativo AWS IoT SiteWise Edge

- Uma novidade Siemens Databus user para o aplicativo AWS IoT SiteWise Edge.
- Uma alteração no arquivo de configuração do gateway (seu arquivo SiteWise_Edge_Gateway_Config).
- Uma atualização na configuração do proxy (que também requer uma reinicialização completa do IEVD).
- Como habilitar logs de depuração para problemas de depuração

Reiniciar a aplicação

1. Na instância do Siemens Industrial Edge Management, escolha Gerenciamento de borda na seção Aplicações de plataforma.
2. Escolha Minhas aplicações instaladas.
3. Selecione o aplicativo AWS IoT SiteWise Edge.
4. Selecione Reiniciar.

Destinos e filtros de caminho

Os destinos no AWS IoT SiteWise Edge fornecem uma maneira flexível e eficiente de gerenciar como seus dados industriais fluem dos dispositivos de borda para a nuvem. Esta seção explica como configurar destinos, usar filtros de caminho para rotear fluxos de dados específicos e escolher o tipo de destino certo para seu caso de uso.

Você pode usar destinos e filtros de caminho em gateways V3 auto-hospedados habilitados para MQTT e gateways usados em conjunto com o aplicativo Edge hospedado em. AWS IoT SiteWise Siemens Industrial Edge Destinos e filtros de caminho não funcionam com o Classic Streams, gateways V2.

Tópicos

- [AWS IoT SiteWise Entenda os destinos Edge](#)
- [Entenda os filtros de caminho para destinos AWS IoT SiteWise do Edge](#)
- [Adicione um destino em tempo real do AWS IoT SiteWise Edge](#)
- [Adicione um destino em AWS IoT SiteWise buffer usando o Amazon S3](#)
- [Adicione filtros de caminho aos destinos AWS IoT SiteWise do Edge](#)
- [Gerenciar destinos AWS IoT SiteWise do Edge](#)

AWS IoT SiteWise Entenda os destinos Edge

Use os destinos do AWS IoT SiteWise Edge para determinar para onde enviar seus dados de origem. Você pode escolher o destino dos dados com base nas características específicas de que precisa, como economia, baixa latência ou requisitos de armazenamento. Integre dados de dispositivos capturados por AWS IoT SiteWise nossos parceiros ou aplicativos personalizados para publicar e assinar filtros de caminho (tópicos) na borda. Em seguida, você pode modelar, transferir e armazenar os dados do seu dispositivo na nuvem.

Note

Para o uso total de todos os recursos de destino em gateways auto-hospedados, atualize para as versões mais recentes do editor de IoT SiteWise e do coletor IoT OPC UA. SiteWise O suporte de streaming continua em streams clássicos, gateways V2, para manter a compatibilidade com as configurações existentes. Para obter mais informações, consulte [Streams clássicos, gateways V2 para Edge AWS IoT SiteWise](#).

Tópicos

- [Como os destinos SiteWise Edge aprimoram o gerenciamento de dados](#)
- [Tipos de destino](#)
- [Compare a funcionalidade de destino entre as versões do gateway](#)
- [Limitações de destino](#)
- [Casos de uso para destinos SiteWise Edge](#)

Como os destinos SiteWise Edge aprimoram o gerenciamento de dados

Exporte dados da borda para AWS IoT SiteWise em tempo real ou em lotes usando o Amazon S3.

Os destinos aprimoram a flexibilidade e a escalabilidade em seu AWS IoT SiteWise ambiente. Os destinos implementam um modelo centralizado de gerenciamento de dados, em que as fontes publicam dados em um sistema central. Os destinos determinam para onde seus dados são enviados usando filtros de caminho. Os destinos podem se inscrever em vários filtros de caminho.

Os gateways habilitados para MQTT, sejam eles auto-hospedados ou em execução em Siemens Industrial Edge, usam o MQTT para comunicação local e vêm com um destino padrão em tempo real com filtros definidos como `#`. Isso significa que, por padrão, todas as mensagens em todos os tópicos são publicadas no destino AWS IoT SiteWise em tempo real. Para obter mais informações, consulte [Entenda os filtros de caminho para destinos AWS IoT SiteWise do Edge](#). Você pode adicionar um destino em tempo real em cada gateway.

Tipos de destino

Ao configurar um destino para seu gateway, você tem duas opções principais: configuração em tempo real usando AWS IoT SiteWise e uma configuração em buffer usando o Amazon S3. Cada tipo de destino tem seu próprio conjunto de configurações e considerações.

AWS IoT SiteWise configurações em tempo real

Escolha essa opção para enviar dados diretamente para o armazenamento AWS IoT SiteWise de camada ativa para facilitar a ingestão e o monitoramento de dados em tempo real. As configurações em tempo real gerenciam o fluxo de dados, principalmente quando um gateway enfrenta problemas de conectividade com a nuvem. Durante a perda da conexão, os dados são temporariamente armazenados localmente no gateway. Depois que a conexão é restabelecida, os dados armazenados são enviados automaticamente para a nuvem.

Você pode ajustar vários aspectos do processo de publicação de dados, como a quantidade máxima de dados a serem armazenados localmente, a taxa na qual os dados são enviados para a nuvem após a reconexão e quando excluí-los após o armazenamento atingir sua capacidade.

Para obter mais informações sobre níveis AWS IoT SiteWise de armazenamento, consulte [Gerencie o armazenamento de dados em AWS IoT SiteWise](#).

AWS IoT SiteWise armazenado em buffer usando as configurações do Amazon S3

Esse tipo de destino permite que você armazene dados localmente no gateway e os envie periodicamente para um bucket do Amazon S3 em lotes. Os dados são armazenados no eficiente formato Parquet, que é otimizado para cargas de trabalho analíticas. Quando os dados estiverem no Amazon S3, você poderá importá-los AWS IoT SiteWise para armazenamento, processamento e análise.

Escolha essa opção para ingerir dados em lotes e armazenar dados históricos de forma econômica. Você pode configurar a localização preferida para o bucket do Amazon S3 e a frequência com que deseja fazer upload dos dados no Amazon S3. Também é possível 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.

Compare a funcionalidade de destino entre as versões do gateway

O recurso de destinos nos gateways habilitados para MQTT simplifica o gerenciamento do fluxo de dados. Os destinos simplificam o gerenciamento de dados por meio da configuração centralizada do roteamento de dados para vários terminais. Essa abordagem elimina a necessidade de configurações de transmissão individuais complexas, tornando o sistema geral mais flexível e fácil de gerenciar.

Em comparação, o Classic streams, V2 gateway e SiteWise Edge transmite dados das fontes de dados para os editores por meio de AWS IoT Greengrass fluxos, configurando destinos de dados individualmente para cada fonte de dados.

Com o recurso de AWS IoT SiteWise destino, a configuração de roteamento do editor é consolidada. A configuração de destino permite gerenciar destinos e filtros de caminho de forma centralizada. Você pode adicionar facilmente um destino, gerenciar filtros de caminho, excluir filtros ou destinos desnecessários, dependendo de suas necessidades.

Além disso, o recurso de destinos utiliza o MQTT (Message Queuing Telemetry Transport), um protocolo padrão do setor amplamente usado em aplicações industriais de IoT. Essa adoção do MQTT ajuda AWS IoT SiteWise a facilitar a integração com vários dispositivos e sistemas.

Limitações de destino

As limitações atuais para destinos nos gateways SiteWise Edge incluem:

- O pacote de processamento de dados não é compatível com gateways habilitados para MQTT.
- O suporte ao tipo de dados é limitado aos tipos de AWS IoT SiteWise dados. Para obter informações sobre como habilitar a conversão de tipo de dados, consulte [Converter tipos de dados incompatíveis](#).

Casos de uso para destinos SiteWise Edge

SiteWise Os destinos periféricos são utilizados em diversas aplicações. Aqui estão alguns exemplos importantes:

Automação industrial, Monitoramento em tempo real e manutenção preditiva

Em ambientes industriais, sensores e dispositivos no chão de fábrica podem publicar dados no SiteWise Edge. Os destinos podem ser configurados para filtrar e rotear dados relevantes, permitindo monitoramento e análise em tempo real do desempenho da máquina. Você pode se inscrever em tópicos relevantes do MQTT usando filtros de caminho, processar os dados e depois publicar os dados processados. Dessa forma, você pode rotear seletivamente os dados processados para serviços analíticos AWS em nuvem ou sistemas locais. Os fabricantes podem então implementar estratégias de manutenção preditiva, otimizar os processos de produção e reduzir o tempo de inatividade.

Edifícios inteligentes, Eficiência energética e otimização da ocupação

Os sistemas de automação predial geram fluxos de dados para monitorar e controlar vários aspectos de um edifício, como sistemas HVAC, iluminação e controle de acesso. Com o SiteWise Edge, esses fluxos de dados podem ser ingeridos, processados e roteados para destinos diferentes. Os gerentes das instalações podem configurar destinos para filtrar e encaminhar dados relevantes, habilitando recursos avançados, como medidas de eficiência energética e otimização de ocupação, garantindo a privacidade e a conformidade dos dados.

Esses casos de uso demonstram como o recurso Destinations no SiteWise Edge pode ser aproveitado em vários setores para ingerir, processar e rotear dados com eficiência. Isso permite recursos avançados, como monitoramento em tempo real, manutenção preditiva, eficiência energética e diagnóstico remoto, garantindo a privacidade e a conformidade dos dados.

Entenda os filtros de caminho para destinos AWS IoT SiteWise do Edge

Tópicos

- [Requisitos de filtro de caminho](#)
- [Melhores práticas para filtros de caminho](#)
- [Filtros de caminho para servidores OPC UA](#)
- [Caracteres especiais nos nomes dos filtros de caminho](#)

Cada destino é configurado para rotear dados para o Amazon S3 AWS IoT SiteWise ou para o Amazon S3. Os filtros de caminho permitem que você selecione dados específicos para filtrar ao receber mensagens MQTT para um destino. Os filtros de caminho representam os nomes lógicos dos seus fluxos de dados, atuando como assinaturas dos tópicos desejados do MQTT.

No MQTT, os dados são organizados em tópicos, que são sequências hierárquicas separadas por barras (/). Por exemplo, um dispositivo pode publicar dados de temperatura no tópico `home/livingroom/sensor1/temperature`. Aqui, `home/livingroom/sensor1` representa o caminho ou o nome lógico do sensor e `temperature` é o tipo de dados que está sendo publicado.

Você pode usar filtros de caminho para se inscrever em tópicos específicos ou em uma variedade de tópicos usando curingas (+e#). O + curinga corresponde a um único nível na hierarquia de tópicos. Por exemplo, `home/+sensor1/temperature` combinaria `home/livingroom/sensor1/temperature` e `home/bedroom/sensor1/temperature`. O # curinga, quando usado no final de um filtro, corresponde a vários níveis.

Você também pode usar uma variedade de caracteres normalmente não permitidos na especificação MQTT em um nome de filtro de caminho. Esses caracteres não funcionam como curingas quando usados em um nome. AWS IoT SiteWise converte esses caracteres usando a codificação para garantir a conformidade com o MQTT e, ao mesmo tempo, preservar sua estrutura de nomenclatura original. Esse recurso é particularmente útil para acomodar as convenções de nomenclatura existentes de outros sistemas. Para obter mais informações, consulte [Caracteres especiais nos nomes dos filtros de caminho](#).

Ao selecionar cuidadosamente os filtros de caminho apropriados, você pode controlar quais dados são enviados para um destino específico. Adapte o fluxo de dados aos requisitos do seu sistema de IoT usando filtros de caminho.

Requisitos de filtro de caminho

Ao inserir filtros de caminho usando o Console do AWS IoT SiteWise, lembre-se do seguinte:

- Os filtros de caminho são delimitados por uma nova linha, com cada linha representando um filtro de caminho separado.
- Os filtros de caminho individuais podem ter entre 1 e 65.535 bytes.
- Um filtro de caminho não pode ficar em branco.
- Valores nulos (U+0000) não são permitidos.
- Você pode inserir até 100 filtros de caminho ou 65.535 caracteres por vez, qualquer que seja o limite atingido primeiro.

- O limite geral é de 20.000 filtros de caminho para todos os destinos em um gateway combinados.
- Você pode usar \$ caracteres%, #, +, e nos nomes dos filtros de caminho, mas os converte AWS IoT SiteWise automaticamente em codificação de URI.

Melhores práticas para filtros de caminho

Ao criar filtros de caminho para seus AWS IoT SiteWise destinos, considere as estratégias a seguir para gerenciar seus dados com eficiência.

- Estruture seus filtros para espelhar sua hierarquia de dispositivos. Por exemplo, em um ambiente de fabricação `factory/+/machine/#`, captura dados de todas as máquinas em diferentes linhas de produção.
- Use níveis específicos para tipos de dispositivos, localizações ou funções. Por exemplo, `.factory/assembly-line/robot/temperature` Ou, na agricultura inteligente `farm/+/crop/+/moisture`, monitorar os níveis de umidade de várias culturas em diferentes campos.
- Use curingas estrategicamente: use + para variações em um único nível e # para capturar todos os níveis subsequentes. Por exemplo `building/+/+/energy-consumption`, monitorea o uso de energia em diferentes zonas e andares de um edifício. Isso pressupõe que o primeiro + capture todos os andares e o segundo + capture todas as zonas.
- Equilibre especificidade e flexibilidade criando filtros específicos o suficiente para capturar dados relevantes, mas flexíveis o suficiente para acomodar futuras mudanças. Por exemplo, `site/+/equipment-type/+/measurement` permite a adição de novos locais ou tipos de equipamentos sem alterar a estrutura do filtro.

Teste seus filtros minuciosamente para garantir que eles capturem os dados pretendidos e estejam alinhados com a arquitetura e os objetivos do seu sistema de IoT.

Filtros de caminho para servidores OPC UA

Para servidores OPC UA, seus filtros de caminho devem corresponder aos nomes das tags OPC UA. O nível final do seu filtro de caminho deve corresponder exatamente ao nome da tag OPC UA. Por exemplo, se sua tag OPC UA for `Device1.Temperature`, seu filtro de caminho pode ser `factory/line1/Device1.Temperature`. Você pode usar curingas nos níveis anteriores, como `factory/+/Device1.Temperature` para capturar a etiqueta em várias linhas de produção. Se você tiver

caracteres especiais nos nomes dos filtros de caminho, consulte [Caracteres especiais nos nomes dos filtros de caminho](#) para obter mais informações.

Caracteres especiais nos nomes dos filtros de caminho

AWS IoT SiteWise acomoda caracteres comumente usados em protocolos industriais como OPC UA, que normalmente não são permitidos em nomes de tópicos padrão do MQTT. Esse recurso facilita a integração mais suave de sistemas industriais com arquiteturas baseadas em MQTT.

Note

Embora nosso tratamento de caracteres especiais seja útil para integração e migração, é recomendável alinhar-se às convenções de nomenclatura padrão do MQTT para novas implementações, quando possível, para garantir uma compatibilidade mais ampla.

Ao receber dados de fontes industriais, AWS IoT SiteWise normaliza os nomes dos tópicos usando a codificação URI para caracteres especiais:

- %torna-se %25 (codificado primeiro como o caractere de escape)
- # se torna %23
- + se torna %2B
- \$torna-se %24 (somente quando está no início de um tópico)

Essa codificação garante que os dados de origem contendo esses caracteres especiais do MQTT possam ser usados com segurança como nomes de tópicos do MQTT, preservando as convenções de nomenclatura industrial originais.

Example : Caracteres especiais nos nomes dos filtros de caminho

Aqui estão alguns exemplos de como os nomes de tópicos industriais podem aparecer nos filtros de AWS IoT SiteWise caminho:

- Factory1/Line#2/Sensor+3 se torna Factory1/Line%232/Sensor%2B3
- Plant%A/Unit\$1/Temp se torna Plant%25A/Unit%241/Temp
- Site1/#Section/+Node se torna Site1/%23Section/%2BNode

Ao criar assinaturas ou visualizar nomes de tópicos em AWS IoT SiteWise, você verá as versões originais não codificadas. A codificação é tratada automaticamente para garantir a conformidade com o MQTT.

Adicione um destino em tempo real do AWS IoT SiteWise Edge

O tipo de destino em tempo real permite que você transmita dados de IoT diretamente de seus dispositivos e gateways para o AWS IoT SiteWise armazenamento em tempo real. Essa opção é ideal para casos de uso que exigem ingestão e processamento imediatos de dados à medida que são gerados, sem a necessidade de lotes ou armazenamento em buffer. Você só pode ter um destino em tempo real configurado em cada gateway, pois ele transmite dados continuamente para AWS IoT SiteWise.

Note

A duplicação TQVs pode resultar em cobrança dupla.

Para adicionar um destino em tempo real

Use o AWS IoT SiteWise console ou AWS CLI adicione um destino em tempo real ao seu gateway SiteWise Edge habilitado para MQTT.

Console

1. Abra o [console de AWS IoT SiteWise](#).
2. No painel de navegação, escolha Gateways de borda.
3. Selecione o gateway ao qual você deseja adicionar um destino.
4. Na seção Destinos, escolha Adicionar destino.
5. Na página Adicionar destino, insira os detalhes do destino:
 - a. Um nome para seu destino no campo Nome do destino.
 - b. Selecione o AWS IoT SiteWise tempo real para o tipo de destino.
6. Configure a ordem de publicação do gateway definindo a Ordem de publicação como Publicar primeiro os dados mais antigos ou Publicar os dados mais recentes primeiro. Por padrão, o gateway publica primeiro os dados mais antigos.

7. Use o Tempo máximo de espera do lote para definir um tempo máximo de espera do editor antes de enviar um lote de dados AWS IoT SiteWise. Essa configuração se aplica a cada alias. Os dados são armazenados localmente até:
 - O tempo definido já passou, ou
 - 10 entradas time-quality-value (TQV) são recebidas para o alias

Qualquer condição atendida primeiro aciona o lote a ser enviado para a nuvem.

8. Para compactar dados carregados, marque a caixa de seleção Ativar compactação ao carregar dados. Deixar o gateway compactar seus dados antes de enviá-los para a nuvem reduz o uso da largura de banda.
9. Para filtrar dados expirados do editor, marque a caixa de seleção Excluir dados expirados. Essa seleção envia somente dados ativos e atuais para AWS IoT SiteWise.
10. No campo Período limite, insira a frequência com que os dados devem ser considerados expirados em seu conjunto de dados. Você pode determinar se os dados são contados em termos de minutos ou dias. O período mínimo de corte é de cinco minutos. O prazo máximo de corte é de sete dias.
11. Opcionalmente, defina as configurações de armazenamento local:
 - a. Defina a frequência do período de retenção — A quantidade de tempo em que o gateway armazena localmente dados anteriores ao período limite. O período mínimo de retenção é de um minuto.

O período máximo de retenção é de 30 dias e maior ou igual ao período de rotação.

- b. Definir o período de rotação — O intervalo de tempo a ser especificado ao salvar dados anteriores ao período limite de um único arquivo. O gateway transfere um lote de dados para o seguinte diretório local no final de cada período de alternância: `/greengrass/v2/work/aws.iot.SiteWiseEdgePublisher/exports`.

A retenção deve ser maior que um minuto e igual ao período de retenção.

- c. Forneça o valor da capacidade de armazenamento (GB) para definir o tamanho máximo dos dados armazenados localmente em GB. Se os dados excederem o tamanho máximo de armazenamento local determinado, o gateway começará a excluir primeiro os dados mais antigos. O gateway continua sendo excluído até que o tamanho dos dados armazenados localmente seja igual ou menor que a cota.

A capacidade de armazenamento deve ser maior ou igual a um GB.

12. Adicione filtros de caminho ao seu destino. Para obter mais informações, consulte, [Adicione filtros de caminho aos destinos AWS IoT SiteWise do Edge](#).

Para obter mais informações, consulte [Tipos de destino](#).

AWS CLI

Example : Crie um novo destino AWS IoT SiteWise em tempo real

Use a [UpdateGatewayCapabilityConfiguration](#)API para configurar o editor.

Defina o parâmetro capabilityNamespace como `iotsitewise:publisher:3`.

```
{
  "sources": [
    {
      "type": "MQTT"
    }
  ],
  "destinations": [
    {
      "type": "SITEWISE_REALTIME",
      "name": "your-destination-name",
      "config": {
        "publishingOrder": "TIME_ORDER",
        "enableCompression": true,
        "maxBatchWaitTime": "10s"
      },
      "filters": [
        {
          "type": "PATH",
          "config": {
            "paths": [
              "#"
            ]
          }
        }
      ]
    }
  ]
}
```

Para atualizar um destino existente AWS IoT SiteWise em tempo real, primeiro use a `DescribeGatewayCapabilityConfiguration` API para encontrar `destinationId` o.

Example : Atualize um destino AWS IoT SiteWise em tempo real

Use a [UpdateGatewayCapabilityConfiguration](#) API para configurar o editor.

Defina o parâmetro `capabilityNamespace` como `iotsitewise:publisher:3`.

```
{
  "sources": [
    {
      "type": "MQTT"
    }
  ],
  "destinations": [
    {
      "id": "your-existing-destination-id",
      "type": "SITEWISE_REALTIME",
      "name": "your-destination-name",
      "config": {
        "publishingOrder": "TIME_ORDER",
        "enableCompression": true,
        "dropPolicy": {
          "cutoffAge": "7d",
          "exportPolicy": {
            "retentionPeriod": "7d",
            "rotationPeriod": "6h",
            "exportSizeLimitGB": 10
          }
        },
        "maxBatchWaitTime": "10s"
      },
      "filters": [
        {
          "type": "PATH",
          "config": {
            "paths": [
              "#"
            ]
          }
        }
      ]
    }
  ]
}
```

```

    }
  ]
}

```

As opções de configuração a seguir são específicas para gateways que usam o `iotsitewise:publisher:3` namespace.

`sources`

Define as fontes de dados para as quais transferir dados de seu equipamento industrial AWS IoT SiteWise. Para gateways habilitados para MQTT, use. MQTT

Tipo: matriz de objetos

Obrigatório: Sim

`destinations`

Define para onde enviar os dados. Os destinos são em tempo real ou armazenados em buffer usando o Amazon S3. É necessário pelo menos um objeto de destino, mas você pode adicionar uma matriz vazia. Você pode ter um destino em tempo real para cada gateway. Para obter mais informações, consulte [AWS IoT SiteWise Entenda os destinos Edge](#).

Tipo: matriz de objetos

Obrigatório: Sim

`id`

O identificador exclusivo do destino. Você pode fornecer uma ID de destino existente ou deixá-la em branco. Se você não especificar um ID, um UUID será gerado por padrão.

Tipo: String

Obrigatório: Não

`type`

Tipo de destino. As opções incluem: `SITewise_REALTIME` `SITewise_BUFFERED` e.

- `SITewise_REALTIME`— Envie dados diretamente para o AWS IoT SiteWise armazenamento em tempo real.

- **SITWISE_BUFFERED**— Envie dados para o Amazon S3 em lotes no formato Parquet e, em seguida, importe para o armazenamento. AWS IoT SiteWise

Tipo: string

Obrigatório: Sim

name

Um nome exclusivo para o destino.

Tipo: string

Obrigatório: Sim

config

Configuração específica para o tipo de destino no formato JSON. A configuração varia entre destinos em tempo real e em buffer.

Tipo: Objeto

Obrigatório: Sim

Ordem de publicação

Determina a ordem na qual os dados são publicados. Os dados são publicados com base em seu registro de data e hora. As opções incluem **TIME_ORDER** **RECENT_DATA** e.

- **TIME_ORDER**(padrão) — Publica primeiro os dados mais antigos.
- **RECENT_DATA**— Publica primeiro os dados mais recentes.

Tipo: String

Obrigatório: Não

Ativar compactação

Quando definido como **true**, ativa a compactação de dados antes de enviar para AWS IoT SiteWise. Deixar o gateway compactar seus dados antes de enviá-los para a nuvem reduz o uso da largura de banda. O valor padrão é **true**.

Tipo: booliano

Obrigatório: não

Política de descarte

Define como lidar com dados antigos.

Tipo: objeto

Obrigatório: Não

- `cutoffAge`

A idade máxima dos dados a serem publicados é especificada em dias, horas e minutos. Por exemplo, 7d ou 1d7h16m. Dados mais antigos do que os especificados não são enviados para AWS IoT SiteWise.

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.

Tipo: string

Obrigatório: Sim

- `exportPolicy`

Define como lidar com dados que excedem a idade limite.

Tipo: Objeto

Obrigatório: Não

- `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.

Tipo: String

Obrigatório: Não

- `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.

Tipo: String

Obrigatório: Não

- `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.

Tipo: inteiro

Obrigatório: não

`maxBatchWaitTime`

Define um tempo máximo para o editor esperar antes de enviar um lote de dados AWS IoT SiteWise. Essa configuração se aplica a cada alias. Os dados são armazenados localmente até:

- O tempo definido já passou, ou
- 10 entradas time-quality-value (TQV) são recebidas para o alias

Use mh, e d para especificar um horário limite. Observe que m representa minutos, h representa horas e d representa dias.

Tipo: String

Obrigatório: Não

filters

Filtros a serem aplicados aos dados. É necessário pelo menos um filtro.

Tipo: string

Obrigatório: Sim

type

Tipo de filtro. Use PATH.

Tipo: string

Obrigatório: Sim

config

Configuração específica para o tipo de filtro no formato JSON. É necessário pelo menos um objeto, mas a matriz pode estar vazia.

Tipo: Objeto

Obrigatório: Sim

- paths

Uma variedade de filtros de caminho. Para obter mais informações, consulte [Entenda os filtros de caminho para destinos AWS IoT SiteWise do Edge](#). O caminho padrão é #.

Tipo: matriz de strings

Obrigatório: Sim

Adicione um destino em AWS IoT SiteWise buffer usando o Amazon S3

O tipo de destino armazenado em buffer permite que você economize nos custos de ingestão AWS IoT SiteWise caso não precise dos dados em tempo real. Ele permite que você armazene temporariamente seus dados de IoT em um bucket do Amazon S3 antes de importá-los. AWS IoT SiteWise Ou você pode simplesmente carregar seus dados no S3 para armazenamento, independentemente de planejar importá-los para AWS IoT SiteWise o S3. Isso é útil para agrupar e armazenar dados em buffer de seus dispositivos e gateways antes de inseri-los. AWS IoT SiteWise Com essa opção, os dados são carregados no bucket S3 especificado no formato Parquet em uma

frequência configurada. Em seguida, você pode importar esses dados para AWS IoT SiteWise armazenamento para análise e processamento adicionais.

Para adicionar um destino armazenado em buffer usando o Amazon S3

Use o AWS IoT SiteWise console ou AWS CLI adicione um destino que armazene dados usando o Amazon S3 em SiteWise seu gateway Edge.

Console

Use o AWS Management Console para adicionar um AWS IoT SiteWise destino armazenado em buffer usando o Amazon S3.

1. Abra o [console de AWS IoT SiteWise](#).
2. No painel de navegação, escolha Gateways de borda.
3. Selecione o gateway ao qual você deseja adicionar um destino.
4. Na seção Destinos, escolha Adicionar destino.
5. Na página Adicionar destino, insira os detalhes do destino:
 - a. Um nome para seu destino no campo Nome do destino.
 - b. Selecione em AWS IoT SiteWise buffer usando o Amazon S3 como tipo de destino. AWS IoT SiteWise armazenado em buffer usando o Amazon S3 envia dados para o Amazon Simple Storage Service em lotes, no formato Parquet, e depois importa os dados para o armazenamento. AWS IoT SiteWise
6. Insira a URL do Amazon S3 para o local onde você deseja armazenar seus dados de gateway. Você pode procurar o caminho escolhendo Browse S3. Depois que um bucket é adicionado, você também pode ver o bucket escolhendo Exibir.
7. Especifique com que frequência seu gateway deve carregar dados para o Amazon S3 inserindo um período de tempo e selecionando um incremento de tempo para a frequência de upload de dados. O valor da frequência deve ser maior que 0 e menor ou igual a 30 dias.
8. Em Configurações de armazenamento de dados, determine o que fazer com os dados do gateway após importá-los para AWS IoT SiteWise. Há duas decisões a serem tomadas em relação ao armazenamento de dados:
 - Se você quiser copiar dados importados para o AWS IoT SiteWise armazenamento, marque a caixa de seleção Copiar dados para armazenamento. Essa opção duplica os dados importados do seu bucket AWS IoT SiteWise Amazon S3 configurado no armazenamento.

- Se você optar por importar seus dados do seu bucket do Amazon S3 para o AWS IoT SiteWise armazenamento, você também pode especificar se os dados importados devem ser excluídos após a conclusão da importação. Marque a caixa de seleção Excluir dados do Amazon S3 para excluir a data importada do bucket do Amazon S3 configurado após importá-la para o armazenamento. AWS IoT SiteWise
9. Adicione filtros de caminho ao seu destino. Para obter mais informações, consulte, [Adicione filtros de caminho aos destinos AWS IoT SiteWise do Edge](#).

AWS CLI

Example : Crie um novo AWS IoT SiteWise destino armazenado em buffer usando o Amazon S3

Use a [UpdateGatewayCapabilityConfiguration](#) API para configurar o editor.

Defina o parâmetro capabilityNamespace como `iotsitewise:publisher:3`.

```
{
  "sources": [
    {
      "type": "MQTT"
    }
  ],
  "destinations": [
    {
      "type": "SITEWISE_BUFFERED",
      "name": "your-s3-destination-name",
      "config": {
        "targetBucketArn": "arn:aws:s3:::amzn-s3-demo-bucket/Optional/SomeFolder",
        "publishPolicy": {
          "publishFrequency": "15m",
          "localSizeLimitGB": 10
        },
        "siteWiseImportPolicy": {
          "enableSiteWiseStorageImport": true,
          "enableDeleteAfterImport": true,
          "bulkImportJobRoleArn": "arn:aws:iam::123456789012:role/your-role-name"
        }
      }
    }
  ],
  "filters": [
    {
      "type": "PATH",
```

```

        "config": {
            "paths": [
                "#"
            ]
        }
    }
]
}
]
}
}

```

Example : Atualize um AWS IoT SiteWise destino armazenado em buffer usando o Amazon S3

Para atualizar um destino existente AWS IoT SiteWise em tempo real, primeiro use a `DescribeGatewayCapabilityConfiguration` API para encontrar `destinationId` o.

O namespace do publicador: `iotsitewise:publisher:3`

```

{
  "sources": [
    {
      "type": "MQTT"
    }
  ],
  "destinations": [
    {
      "id": "your-existing-destination-id",
      "type": "SITEWISE_BUFFERED",
      "name": "your-s3-destination-name",
      "config": {
        "targetBucketArn": "arn:aws:s3:::amzn-s3-demo-bucket/Optional/SomeFolder",
        "publishPolicy": {
          "publishFrequency": "15m",
          "localSizeLimitGB": 10
        },
        "siteWiseImportPolicy": {
          "enableSiteWiseStorageImport": true,
          "enableDeleteAfterImport": true,
          "bulkImportJobRoleArn": "arn:aws:iam::123456789012:role/your-role-name"
        }
      },
    },
  ],
  "filters": [

```

```
{
  "type": "PATH",
  "config": {
    "paths": [
      "#"
    ]
  }
}
```

As opções de configuração a seguir são específicas para gateways habilitados para MQTT usando o namespace. `iotsitewise:publisher:3`

`sources`

Define as fontes de dados para as quais transferir dados de seu equipamento industrial AWS IoT SiteWise. Para gateways habilitados para MQTT, use. MQTT

Tipo: matriz de objetos

Obrigatório: Sim

`destinations`

Define para onde enviar os dados. Os destinos são em tempo real ou armazenados em buffer usando o Amazon S3. É necessário pelo menos um objeto de destino, mas você pode adicionar uma matriz vazia. Você pode ter um destino em tempo real para cada gateway. Para obter mais informações, consulte [AWS IoT SiteWise Entenda os destinos Edge](#).

Tipo: matriz de objetos

Obrigatório: Sim

`id`

O identificador exclusivo do destino. Você pode fornecer uma ID de destino existente ou deixá-la em branco para que uma nova ID seja gerada automaticamente para o destino.

Tipo: String

Obrigatório: Não

type

Tipo de destino. As opções incluem: SITEWISE_REALTIME SITEWISE_BUFFERED e. Selecione SITEWISE_BUFFERED.

- SITEWISE_REALTIME(padão) — Envie dados diretamente para o AWS IoT SiteWise armazenamento em tempo real. Para obter mais informações, consulte [Adicione um destino em tempo real do AWS IoT SiteWise Edge](#).
- SITEWISE_BUFFERED— Envie dados para o Amazon S3 em lotes no formato Parquet e, em seguida, importe para o armazenamento. AWS IoT SiteWise

Tipo: string

Obrigatório: Sim

name

Um nome exclusivo para o destino.

Tipo: string

Obrigatório: Sim

config

Configuração específica para o tipo de destino no formato JSON. A configuração varia entre destinos em tempo real e em buffer.

Tipo: Objeto

Obrigatório: Sim

targetBucketArn

O ARN do bucket de publicação. Escolha o mesmo Região da AWS para ambos AWS IoT SiteWise e para o Amazon S3. Se um prefixo for escolhido, ele deverá ter entre 1 e 255 caracteres.

Note

AWS IoT SiteWise, incluindo o gateway, terá acesso a todo o bucket S3 especificado. Recomendamos usar um bucket dedicado para ingestão de dados em buffer.

Tipo: string

Obrigatório: Sim

`publishPolicy`

Detalhes da política de publicação.

Tipo: Objeto

Obrigatório: Sim

`publishFrequency`

A frequência com que o gateway SiteWise Edge publica no bucket do Amazon S3. A frequência de upload de dados para o Amazon S3 deve ser maior que 0 minutos e menor ou igual a 30 dias. Você pode usar mh, e d ao especificar uma idade de frequência de publicação. Observe que m representa minutos, h representa horas e d representa dias. O valor padrão é 15 minutos.

Tipo: string

Obrigatório: Sim

`localSizeLimitGB`

O tamanho máximo dos arquivos gravados no disco local em GB. Se esse limite for violado, o publicador publicará todos os dados armazenados em buffer no destino.

Tipo: inteiro

Obrigatório: Sim

`siteWiseImportPolicy`

Detalhes da política de importação para importação de dados para o. AWS IoT SiteWise

Tipo: Objeto

Obrigatório: Sim

`enableSiteWiseStorageImport`

Defina isso `true` para importar dados de um bucket do Amazon S3 para AWS IoT SiteWise armazenamento. Inicialmente, ele faz uma cópia dos dados em AWS IoT SiteWise. Em seguida, se você `enableDeleteAfterImport` definir como

verdadeiro, os dados no S3 serão excluídos após a cópia para o. AWS IoT SiteWise
As implicações de preços se aplicam. O valor padrão é `true`.

Tipo: booleano

Obrigatório: Sim

`enableDeleteAfterImport`

Defina isso `true` para excluir o arquivo no bucket do Amazon S3 após a ingestão no armazenamento. AWS IoT SiteWise O valor padrão é `true`.

Tipo: booleano

Obrigatório: Sim

`bulkImportJobRoleArn`

O ARN da função do IAM que AWS IoT SiteWise pressupõe a leitura de dados em buffer do Amazon S3 durante a ingestão de dados. Essa função é usada quando um dispositivo de borda é chamado AWS IoT SiteWise APIs para iniciar o processo de importação em massa.

 Note

Se `enableSiteWiseStorageImport` estiver definido como `true`, esse parâmetro será obrigatório.

Tipo: String

Obrigatório: Não

Adicione filtros de caminho para seu destino. Para obter mais informações, consulte [Adicione filtros de caminho aos destinos AWS IoT SiteWise do Edge](#).

Adicione filtros de caminho aos destinos AWS IoT SiteWise do Edge

Adicione filtros de caminho a um destino. Os filtros de caminho usam a sintaxe de tópico do MQTT, onde `#` é um caractere curinga que corresponde a qualquer número de níveis e `+` é um caractere curinga que corresponde a um único nível. Você pode adicionar vários destinos a um gateway, cada um com seu próprio conjunto de filtros de caminho inscritos na telemetria do seu equipamento.

Siemens Industrial Edgeos gateways usam um prefixo para compatibilidade. Para obter mais informações, consulte [Prefixos para filtros de caminho](#).

Console

Para adicionar filtros de caminho

1. Abra o [console de AWS IoT SiteWise](#).
2. No painel de navegação, escolha Gateways de borda.
3. Selecione o gateway ao qual você deseja adicionar filtros de caminho.
4. Na seção Filtros de caminho, em Adicionar destino, escolha Adicionar filtro de caminho.
5. Insira o filtro de caminho no qual você deseja que esse destino se inscreva. Você pode usar caracteres curinga (#e+) para se inscrever em vários caminhos.
6. Escolha Adicionar filtro de caminho para adicionar o filtro de caminho à lista.
7. Repita as etapas para adicionar filtros de caminho adicionais, se necessário.
8. Depois de adicionar todos os filtros de caminho necessários, escolha Criar.

AWS CLI for self-hosted gateways

Example : Configuração do filtro de caminho

```
{
  "destinations": [
    {
      ...
    }
  ],
  "filters": [
    {
      "type": "PATH",
      "config": {
        "paths": [
          "home/+/sensor1/temperature",
          "home/livingroom/sensor1/temperature",
          "home/livingroom/sensor1/temperature",
          "building/#"
        ]
      }
    }
  ]
}
```

```

    }
  ]
}
```

AWS CLI for Siemens IEGateways

Example : Configuração de prefixo para filtros de caminho

Capture todos os dados usando os prefixos data (ie/d) e metadata (ie/m) para cada filtro de caminho.

```

{
  "destinations": [
    {
      ...
    }
  ],
  "filters": [
    {
      "type": "PATH",
      "config": {
        "paths": [
          "ie/d/home/+/sensor12/temperature",
          "ie/m/home/livingroom/sensor12/temperature",
          "ie/d/home/livingroom/sensor13/temperature2",
          "ie/m/home/livingroom/sensor13/temperature2",
          "ie/d/building/#",
          "ie/m/building/#"
        ]
      }
    }
  ]
}
```

Note

Copie filtros de caminho entre destinos baixando a lista de filtros de caminho. Para obter mais informações, consulte [Baixe todos os filtros de caminho em um destino \(console\)](#).

Carregue filtros de caminho em massa

Para fazer upload de filtros de caminho em massa, use um arquivo CSV ou de texto. AWS IoT SiteWise remove automaticamente as duplicatas exatas quando você carrega arquivos. Por exemplo, `windfarm/site1/` e `windfarm/site1/` são duplicatas exatas que são AWS IoT SiteWise capturadas porque a string é exatamente a mesma. As duplicatas parciais não são removidas e resultam em cobranças adicionais. Por exemplo, `windfarm/#` e `windfarm/site1` são tópicos sobrepostos porque já estão `windfarm/site1` abrangidos por `windfarm/#`.

Note

Evite duplicatas para evitar cobranças adicionais. O arquivo carregado deve estar no formato `.csv` ou `.txt`. Ele não pode conter nenhum cabeçalho e deve consistir em uma única coluna. Na coluna, liste seus filtros de caminho, com cada filtro em uma linha separada. Nenhuma outra informação deve ser incluída no arquivo.

Requisitos de upload de arquivos

Esses são requisitos adicionais de filtro de caminho.

- Você pode carregar um arquivo `.csv` ou `.txt`. Arquivos em outros formatos não são compatíveis.
- Os arquivos CSV (`.csv`) não podem ter cabeçalhos e devem conter apenas uma coluna.
- Você pode ter um filtro de caminho em cada linha.
- Os arquivos enviados não podem estar vazios.
- Ao ser usado `#` como curinga, ele deve ser o último caractere no filtro de tópicos. Por exemplo, `topic/#` ou como um personagem independente em um determinado nível de tópico. No entanto, observe que também `#` pode ser usado como um caractere normal em um nome de nível de tópico, como `factory/machine#1/topic`. Para obter mais informações, consulte [Caracteres especiais nos nomes dos filtros de caminho](#).
- Você também pode usar o `+` personagem. Por exemplo, use `factory/+/temp` para obter todas as temperaturas para fábricas em vez de `factory/machine2/temp` e `factory/machine3/temp` individualmente.

Gerenciar destinos AWS IoT SiteWise do Edge

Depois de adicionar destinos, você pode realizar várias operações para gerenciá-los, como editar configurações de destino, excluir destinos e gerenciar filtros de caminho.

Editar um destino

Selecione o botão de rádio ao lado do destino na tabela e escolha o botão Editar para editar um destino.

Console

Para editar um destino usando o AWS IoT SiteWise console

1. Abra o [console de AWS IoT SiteWise](#).
2. Na navegação à esquerda, escolha Gateways Edge na seção Edge.
3. Selecione o gateway apropriado.
4. Na seção Destinos, escolha o destino que você deseja editar e, em seguida, escolha Editar.
5. Modifique o destino e escolha Salvar.

AWS CLI

Para editar um destino usando AWS CLI

- Você pode editar um destino modificando as informações de configuração do recurso JSON.

```
aws iotsitewise update-gateway-capability-configuration \
--gateway-id your-gateway-id \
--capability-namespace "iotsitewise:publisher:3" \
--capability-configuration '{
  "sources": [
    {
      "type": "MQTT"
    }
  ],
  "destinations": [
    {
      "id": "your-existing-destination-id",
      "type": "SITEWISE_REALTIME",
      "name": "your-updated-destination-name",
```

```

    "config": {
      "publishingOrder": "TIME_ORDER",
      "enableCompression": true,
      "dropPolicy": {
        "cutoffAge": "10d",
        "exportPolicy": {
          "retentionPeriod": "10d",
          "rotationPeriod": "6h",
          "exportSizeLimitGB": 10
        }
      },
      "maxBatchWaitTime": "15s"
    },
    "filters": [
      {
        ...
      }
    ]
  }
]
}'

```

Note

Você não pode atualizar o destino `type` ou `capability-namespace`. Por exemplo, você não pode mudar de um tipo de `SITWISE_REALTIME` para `SITWISE_BUFFERED`. Você pode ter um destino em tempo real para cada gateway habilitado para MQTT.

Excluir um destino

Se você não precisar mais de um destino, poderá excluí-lo do seu gateway SiteWise Edge.

Console

Para excluir um destino usando o AWS IoT SiteWise console

1. Abra o [console de AWS IoT SiteWise](#).
2. Na navegação à esquerda, escolha Gateways Edge na seção Edge.
3. Selecione o gateway apropriado.

4. Na seção Destinos, escolha o destino que você deseja excluir e, em seguida, escolha Excluir. Uma tela de confirmação é exibida.
5. Para confirmar sua escolha de excluir o destino, digite “excluir” na caixa de confirmação.

AWS CLI

Para excluir um destino usando AWS CLI

- Exclua a configuração do recurso do gateway especificando o ID do gateway e modificando a configuração do recurso para remover o destino que você deseja excluir.

```
aws iotsitewise update-gateway-capability-configuration \  
  --gateway-id your-gateway-id \  
  --capability-namespace "iotsitewise:publisher:3" \  
  --capability-configuration '{  
    "sources": [  
      {  
        "type": "MQTT"  
      }  
    ],  
    "destinations": []  
  }'
```

Note

A matriz de destinos pode estar vazia ([]), mas o próprio objeto de destinos deve ser incluído na configuração do recurso.

Baixe todos os filtros de caminho em um destino (console)

Baixe um arquivo CSV contendo todos os seus filtros de caminho no AWS IoT SiteWise console. Você pode usar uma lista baixada de filtros de caminho para compartilhar facilmente listas de filtros de caminho entre destinos de gateway.

Para baixar um arquivo CSV de todos os filtros de caminho usando o console AWS IoT SiteWise

1. Abra o [console de AWS IoT SiteWise](#).

2. Na navegação à esquerda, escolha Gateways Edge na seção Edge.
3. Selecione o gateway que contém seus filtros de caminho.
4. Escolha Adicionar destino ou Editar destino.
5. Navegue até a seção Filtros de caminho e escolha Baixar CSV.

 Note

O arquivo CSV inclui todos os filtros de caminho em um destino específico, independentemente de quais você selecionou na lista de filtros de caminho.

Editar um filtro de caminho

Você pode editar filtros de caminho individuais para refinar quais dados seu destino recebe.

Console

Usando o AWS IoT SiteWise console, você pode editar cada filtro de caminho individual em cada caixa de texto respectiva.

Para editar um filtro de caminho usando o AWS IoT SiteWise console

1. Abra o [console de AWS IoT SiteWise](#).
2. Na navegação à esquerda, escolha Gateways Edge na seção Edge.
3. Selecione o gateway que contém seus filtros de caminho.
4. Selecione o destino apropriado.
5. Escolha Editar.
6. Escolha a caixa de texto para a linha que contém o filtro de caminho que você deseja editar.
7. Atualize o texto do filtro de caminho, garantindo que a caixa de seleção do filtro de caminho editado esteja marcada.
8. Escolha Salvar.

AWS CLI

Para editar filtros de caminho para um destino usando o AWS CLI, primeiro recupere a configuração atual, modifique-a e, em seguida, atualize-a usando o `update-gateway-capability-configuration` comando.

Para editar um filtro de caminho usando AWS CLI

1. Recupere a configuração de capacidade atual:

```
aws iotsitewise describe-gateway-capability-configuration \
  --gateway-id your-gateway-id \
  --capability-namespace "iotsitewise:publisher:3" \
  --query "capabilityConfiguration"
```

2. Edite o JSON para modificar os filtros de caminho conforme necessário.
3. Atualize a configuração do recurso com os filtros de caminho modificados:

```
aws iotsitewise update-gateway-capability-configuration \
  --gateway-id your-gateway-id \
  --capability-namespace "iotsitewise:publisher:3" \
  --capability-configuration json-containing-your-updated-path-filters
```

Excluir um filtro de caminho

Você pode excluir filtros de caminho de um destino para controlar os dados que ele recebe das fontes do MQTT e dos pipelines de processamento de dados.

Console

Para excluir um filtro de caminho usando o AWS IoT SiteWise console

1. Abra o [console de AWS IoT SiteWise](#).
2. Na navegação à esquerda, escolha Gateways Edge na seção Edge.
3. Selecione o gateway que contém seus filtros de caminho.
4. Selecione o destino apropriado.
5. Escolha Editar.
6. Na tela Editar destino, na seção Filtros de caminho, selecione um ou mais filtros de caminho a serem excluídos.

7. Escolha Excluir. Uma mensagem de confirmação de exclusão é exibida. Se quiser continuar com a exclusão dos filtros de caminho, escolha Excluir na tela de confirmação.

AWS CLI

Para excluir um destino usando AWS CLI

- Exclua um filtro de caminho removendo-o da configuração do recurso.

```
aws iotsitewise update-gateway-capability-configuration \
  --gateway-id your-gateway-id \
  --capability-namespace "iotsitewise:publisher:3" \
  --capability-configuration '{
    "sources": [
      {
        "type": "MQTT"
      }
    ],
    "destinations": [
      {
        "id": "your-destination-id",
        "type": "SITEWISE_REALTIME",
        "name": "your-destination-name",
        "config": {
          ...
        },
        "filters": [
          {
            "type": "PATH",
            "config": {
              "paths": [
                "/path1",
                "/path2",
                "/delete-a-path-to-remove-it"
              ]
            }
          }
        ]
      }
    ]
  }
```

 Note

A matriz de filtros pode estar vazia ([]), mas o próprio objeto de filtros deve ser incluído na configuração do recurso.

Gerencie 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 no dispositivo local, o serviço exclui automaticamente um pequeno volume de dados com os carimbos de data/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 Settings.
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: *number*bytes de dados foram excluídos para evitar que o armazenamento do SiteWise Edge Gateway fique sem espaço.

Gerencie 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 Detalhes do gateway de borda de um gateway específico, escolha o nome de um gateway do Edge.

Na guia Visão geral da página Detalhes do gateway de borda, você pode fazer o seguinte:

- Na seção Fontes de dados, atualize a configuração de fontes 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 Detalhes do gateway de borda, você pode ver as versões atuais do componente e do pacote implantadas no gateway do Edge. Também é onde você implanta novas versões quando são disponibilizadas.

Gerencie 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 auto-hospedados. 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, veja os ativos implantados no dispositivo local e o último valor coletado ou calculado para propriedades de 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 habilitado.

Para gerenciar gateways SiteWise Edge usando AWS OpsHub

1. Baixe e instale o aplicativo [AWS OpsHubAWS IoT SiteWise for Windows](#).
2. Abra o aplicativo .
3. Se você não tiver credenciais locais configuradas para o gateway, siga as etapas em [Acesse seu gateway SiteWise Edge usando as 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 o endereço IP do 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 o endereço IP do 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.

Acesse seu gateway SiteWise Edge usando as 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 gateway Edge SiteWise auto-hospedado.

Important

Para acessar seu gateway SiteWise Edge com credenciais Linux, você deve ativar o pacote de processamento de dados para seu gateway SiteWise Edge.

Acesse 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.
password Substitua *user-name* e 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 um SWE_ADMIN_GROUP ou SWE_USER_GROUP, *user-name* substitua 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.

Acesse seu gateway SiteWise Edge usando as 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 PowerShell na 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. *password* Substitua *user-name* e pelo nome de usuário e pela senha que você deseja criar.

```
net user user-name password /add
```

5. Execute o seguinte comando para adicionar um usuário ao grupo de administradores. *user-name* Substitua 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.

Gerenciar 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 Settings.
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.

Alterar 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 Visualizar versões do software.
5. Na página Editar versões do software, para o pacote cuja versão você quer atualizar, selecione a versão desejada e escolha Implantar.
6. Selecione Concluído.

Listar gateways SiteWise Edge

Console

Para listar os gateways SiteWise do Edge

1. Navegue até o [console do AWS IoT SiteWise](#).
2. No painel de navegação, escolha Gateways de borda.
3. Veja a lista de todos os seus gateways SiteWise do Edge.

AWS CLI

Para listar seus gateways usando AWS CLI, siga estas etapas:

- Use o comando `list-gateways` para visualizar todos os seus gateways:

```
aws iotsitewise list-gateways
```

Esse comando retorna uma lista dos seus gateways com seus IDs nomes e outras informações.

Você também pode especificar os parâmetros de paginação:

```
aws iotsitewise list-gateways --max-results 10 --next-token your-token
```

Para obter mais informações, consulte [list-gateways](#) na Referência de Comandos. AWS CLI

Descreva um gateway SiteWise Edge

Console

Para ver os detalhes do gateway

1. Navegue até o [console do AWS IoT SiteWise](#).
2. No painel de navegação, escolha Gateways de borda.
3. Escolha o nome do gateway do qual você deseja ver os detalhes.
4. Veja os detalhes do gateway na página de detalhes do gateway Edge.

AWS CLI

Para obter informações detalhadas sobre o uso de um gateway específico AWS CLI, siga estas etapas:

- Use o comando `describe-gateway` com o ID do gateway:

```
aws iotsitewise describe-gateway --gateway-id a1b2c3d4-5678-90ab-cdef-1a1a1EXAMPLE
```

Esse comando retorna informações detalhadas sobre o gateway.

Para obter mais informações, consulte [describe-gateway](#) na Referência de Comandos. AWS CLI

Crie um gateway SiteWise Edge

Console

Para criar um gateway SiteWise Edge

1. Navegue até o [console do AWS IoT SiteWise](#).
2. No painel de navegação, escolha Gateways de borda.
3. Escolha Criar gateway.
4. Insira um nome para seu gateway.
5. Selecione o grupo Greengrass para seu gateway.

6. Opcionalmente, adicione tags ao seu gateway.
7. Escolha Criar.

AWS CLI

Para criar um novo SiteWise gateway de IoT usando AWS CLI, siga estas etapas:

- Use o comando `create-gateway` para criar um novo gateway:

```
aws iotsitewise create-gateway \
  --gateway-name "NewSiteWiseGateway" \
  --gateway-platform '{
    "greengrass": {
      "groupArn": "arn:aws:greengrass:us-east-1:123456789012:group/
a1b2c3d4-5678-90ab-cdef-1a1a1EXAMPLE"
    }
  }' \
  --tags '{
    "Environment": "Production",
    "Location": "Factory1"
  }'
```

Esse comando retorna o ID e o ARN do novo gateway:

```
{
  "gatewayId": "a1b2c3d4-5678-90ab-cdef-1a1a1EXAMPLE",
  "gatewayArn": "arn:aws:iotsitewise:us-east-1:123456789012:gateway/
a1b2c3d4-5678-90ab-cdef-1a1a1EXAMPLE"
}
```

Para obter mais informações, consulte [create-gateway](#) na Referência de Comandos. AWS CLI

Atualizar um gateway SiteWise Edge

Console

Para atualizar um gateway SiteWise Edge

1. Navegue até o [console do AWS IoT SiteWise](#).

2. No painel de navegação, escolha Gateways de borda.
3. Selecione o gateway que você deseja atualizar.
4. Escolha Editar.
5. Atualize o nome do gateway ou outras configurações conforme necessário.
6. Escolha Salvar.

AWS CLI

Para atualizar um gateway existente usando AWS CLI, siga estas etapas:

- Use o comando `update-gateway` para atualizar o nome de um gateway:

```
aws iotsitewise update-gateway \
  --gateway-id a1b2c3d4-5678-90ab-cdef-1a1a1EXAMPLE \
  --gateway-name "UpdatedGatewayName"
```

Esse comando não gera nenhuma saída quando é bem-sucedido.

Para obter mais informações, consulte [update-gateway na Referência](#) de AWS CLI Comandos.

Atualizar a configuração da capacidade do gateway

Console

Para atualizar a configuração da capacidade do gateway

1. Navegue até o [console do AWS IoT SiteWise](#).
2. No painel de navegação, escolha Gateways de borda.
3. Escolha o nome do gateway que você deseja atualizar.
4. Na seção Fontes de dados, escolha Editar.
5. Atualize a configuração da fonte de dados conforme necessário.
6. Escolha Salvar.

AWS CLI

Para atualizar a configuração de capacidade de um gateway usando AWS CLI, siga estas etapas:

- Use o `update-gateway-capability-configuration` comando para atualizar a configuração do recurso:

```
aws iotsitewise update-gateway-capability-configuration \
  --gateway-id a1b2c3d4-5678-90ab-cdef-1a1a1EXAMPLE \
  --capability-namespace "iotsitewise:opcuacollector:1" \
  --capability-configuration '{
    "sources": [
      {
        "name": "OPC-UA Server",
        "endpoint": {
          "certificateTrust": {
            "type": "TrustAny"
          },
          "endpointUri": "opc.tcp://10.0.0.1:4840",
          "securityPolicy": "NONE",
          "messageSecurityMode": "NONE",
          "identityProvider": {
            "type": "Anonymous"
          }
        },
        "measurementDataStreamPrefix": ""
      }
    ]
  }'
```

Esse comando retorna o namespace da capacidade e o status de sincronização:

```
{
  "capabilityNamespace": "iotsitewise:opcuacollector:1",
  "capabilitySyncStatus": "CONFIGURING"
}
```

Para obter mais informações, consulte [update-gateway-capability-configuration](#) na Referência de AWS CLI Comandos.

Tag: recursos do gateway

Console

Para marcar um recurso de gateway

1. Navegue até o [console do AWS IoT SiteWise](#).
2. No painel de navegação, escolha Gateways de borda.
3. Escolha o nome do gateway que você deseja marcar.
4. Escolha a guia Tags.
5. Selecione Gerenciar tags.
6. Escolha Adicionar nova tag e insira uma chave e um valor para cada tag.
7. Escolha Salvar.

AWS CLI

Para adicionar tags a um gateway usando AWS CLI, siga estas etapas:

- Use o comando `tag-resource` para adicionar tags a um gateway:

```
aws iotsitewise tag-resource \
  --resource-arn "arn:aws:iotsitewise:us-east-1:123456789012:gateway/
a1b2c3d4-5678-90ab-cdef-1a1a1EXAMPLE" \
  --tags '{
    "Department": "Operations",
    "Project": "FactoryAutomation"
  }'
```

Esse comando não gera nenhuma saída quando é bem-sucedido.

Para obter mais informações, consulte [tag-resource na Referência de AWS CLI Comandos](#).

Listar tags para um gateway

Console

Para listar tags para um gateway

1. Navegue até o [console do AWS IoT SiteWise](#).
2. No painel de navegação, escolha Gateways de borda.
3. Escolha o nome do gateway para o qual você deseja visualizar as tags.
4. Escolha a guia Tags.
5. Veja a lista de tags associadas ao gateway.

AWS CLI

Para listar as tags associadas a um gateway usando AWS CLI, siga estas etapas:

- Use o `list-tags-for-resource` comando para listar as tags de um gateway:

```
aws iotsitewise list-tags-for-resource \
  --resource-arn "arn:aws:iotsitewise:us-east-1:123456789012:gateway/
a1b2c3d4-5678-90ab-cdef-1a1a1EXAMPLE"
```

Esse comando retorna as tags associadas ao gateway:

```
{
  "tags": {
    "Environment": "Production",
    "Location": "Factory1",
    "Department": "Operations",
    "Project": "FactoryAutomation"
  }
}
```

Para obter mais informações, consulte [list-tags-for-resource](#) na Referência de AWS CLI Comandos.

Remover tags de um gateway

Console

Para remover tags de um gateway

1. Navegue até o [console do AWS IoT SiteWise](#).
2. No painel de navegação, escolha Gateways de borda.
3. Escolha o nome do gateway do qual você deseja remover as tags.
4. Escolha a guia Tags.
5. Selecione Gerenciar tags.
6. Escolha o ícone de remoção (X) ao lado de cada tag que você deseja remover.
7. Escolha Salvar.

AWS CLI

Para remover tags de um gateway usando AWS CLI, siga estas etapas:

- Use o comando `untag-resource` para remover tags de um gateway:

```
aws iotsitewise untag-resource \
  --resource-arn "arn:aws:iotsitewise:us-east-1:123456789012:gateway/
a1b2c3d4-5678-90ab-cdef-1a1a1EXAMPLE" \
  --tag-keys '["Project", "Department"]'
```

Esse comando não gera nenhuma saída quando é bem-sucedido.

Para obter mais informações, consulte [untag-resource](#) na Referência de Comandos. AWS CLI

Atualizar a versão de um AWS IoT SiteWise componente

Atualize o componente de AWS IoT SiteWise gateway em seu dispositivo AWS IoT Greengrass principal para garantir seu acesso aos recursos mais recentes, melhorias de desempenho e patches de segurança.

Para atualizar um AWS IoT SiteWise componente no AWS IoT Greengrass

1. Navegue até o [console do AWS IoT SiteWise](#).
2. No painel de navegação esquerdo, escolha Edge gateways.
3. Selecione o gateway a ser editado e escolha Editar.
4. Em Capacidades do Edge, em Versões de software, escolha Atualizações de software disponíveis. A página Editar versões do software é exibida.
5. Escolha a versão do componente.

Note

É recomendável selecionar a versão mais recente disponível. Manter os componentes do gateway up-to-date ajuda você a manter a funcionalidade ideal para coleta e processamento de dados industriais.

6. Escolha Implantar. Isso inicia uma AWS IoT Greengrass V2 implantação para atualizar o AWS IoT SiteWise componente no gateway.

Excluir um gateway SiteWise Edge

Console

Para excluir o gateway SiteWise Edge

1. Navegue até o [console do AWS IoT SiteWise](#).
2. No painel de navegação, escolha Gateways de borda.
3. Escolha o gateway que você deseja excluir.
4. Escolha Excluir.
5. Para confirmar que você deseja excluir o gateway, digite “delete” e escolha Delete na janela que aparece.

AWS CLI

Para excluir um gateway usando AWS CLI, siga estas etapas:

1. Liste seus gateways para identificar o ID do gateway que você deseja excluir.

```
aws iotsitewise list-gateways
```

Esse comando retorna uma lista dos seus gateways com seus IDs nomes e outras informações:

```
{
  "gatewaySummaries": [
    {
      "gatewayId": "a1b2c3d4-5678-90ab-cdef-1a1a1EXAMPLE",
      "gatewayName": "ExampleCorpGateway",
      "gatewayCapabilitySummaries": [
        {
          "capabilityNamespace": "iotsitewise:opcuacollector:1",
          "capabilitySyncStatus": "IN_SYNC"
        }
      ],
      "creationDate": 1588369971.457,
      "lastUpdateDate": 1588369971.457
    }
  ]
}
```

2. Exclua o gateway especificando seu ID:

```
aws iotsitewise delete-gateway --gateway-id a1b2c3d4-5678-90ab-cdef-1a1a1EXAMPLE
```

Esse comando não gera nenhuma saída quando é bem-sucedido.

 Note

Quando você exclui um gateway, alguns dos arquivos do gateway permanecem no sistema de arquivos do gateway.

3. Para verificar se o gateway foi excluído, você pode listar seus gateways novamente:

```
aws iotsitewise list-gateways
```

O gateway excluído não deve mais aparecer na lista.

Para obter mais informações, consulte [delete-gateway](#) na Referência de Comandos. AWS CLI

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 [Solucionando 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.

Esta seção se aplica aos gateways que usam o pacote de processamento de dados. Para ter mais informações sobre o pacote de processamento de dados, consulte [Configurar um modelo de ativo para processamento de dados no SiteWise Edge](#).

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

Antes de tentar restaurar um gateway SiteWise Edge, certifique-se de que todos os dispositivos de borda conectados ao gateway estejam parados ou desconectados.

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](#).

Gateways legados (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. Para obter mais informações sobre como executar um AWS IoT SiteWise gateway usando AWS IoT Greengrass V2, consulte [Hospede automaticamente um gateway AWS IoT SiteWise Edge com AWS IoT Greengrass V2](#).

SiteWise Os gateways Edge agora são executados exclusivamente AWS IoT Greengrass V2, fornecendo funcionalidade aprimorada e desempenho aprimorado para seus aplicativos industriais de IoT. Essa versão mais recente AWS IoT Greengrass V2 representa uma evolução arquitetônica, construída em uma estrutura moderna baseada em componentes que permite a implantação modular de software. Ele simplifica a instalação por meio de um instalador unificado, oferecendo aos desenvolvedores maior flexibilidade na implantação de componentes personalizados e na

realização de testes locais. O modelo baseado em componentes permite um gerenciamento de recursos mais eficiente e introduz uma abordagem de configuração simplificada por meio de receitas de componentes. Esse design facilita um melhor tratamento da dependência entre componentes, oferece suporte a práticas de implantação contínua e fornece recursos aprimorados de CLI para desenvolvimento local. Além disso, AWS IoT Greengrass V2 centraliza o gerenciamento de configurações AWS IoT Core e oferece recursos aprimorados de registro e monitoramento, todos protegidos por um modelo de permissões de segurança mais granular.

Para obter mais informações sobre como começar a usar os gateways SiteWise Edge usando AWS IoT Greengrass V2, [AWS IoT SiteWise Requisitos de gateway auto-hospedado do Edge](#). Esses recursos fornecem step-by-step instruções sobre como configurar seus gateways, configurar fontes de dados e gerenciar sua infraestrutura industrial de IoT.

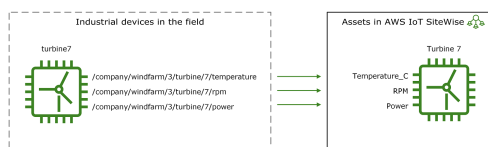
 Note

À medida que AWS continua inovando e aprimorando seus serviços de IoT, é recomendável se manter atualizado com os recursos e aprimoramentos mais recentes. Verifique regularmente a AWS IoT Greengrass documentação AWS IoT SiteWise e veja se há novos recursos que podem otimizar ainda mais suas soluções industriais de IoT.

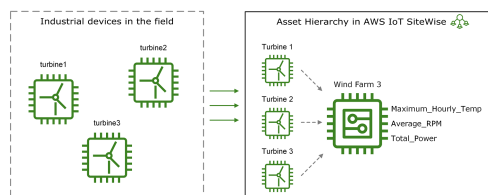
Modelar ativos industriais

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 a AWS nuvem. 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 dentro dos ativos filhos 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 com base em um modelo de ativo. Os modelos de ativos são estruturas declarativas que padronizam o formato de seus ativos. Os modelos de ativo impõem informações consistentes em vários ativos do mesmo tipo, para que você possa processar dados nos ativos que representem 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 componente. Um modelo de componente é um tipo especial de modelo de ativo que você pode incluir em modelos de ativo ou em outros modelos de componente.

Você pode usar os modelos de componente para definir subconjuntos reutilizáveis comuns, como sensores, motores e assim por diante, que compartilha entre vários modelos de ativo.

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.

Também é possível atualizar e excluir ativos, modelos de ativo e modelos de componente 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, a atualização se aplica a cada ativo com base em cada modelo de ativo que faz referência ao modelo de componente.

Os modelos de ativo podem ser muito complexos, por exemplo, ao modelar um equipamento complicado que tenha muitos subcomponentes. Para ajudar a manter esses modelos de ativo organizados e sustentáveis, você pode usar modelos compostos personalizados para agrupar propriedades relacionadas ou reutilizar componentes compartilhados. Para obter mais informações, consulte [Modelos compostos personalizados \(componentes\)](#).

Tópicos

- [Estados de ativos e modelos](#)
- [Versões do modelo de ativo](#)
- [Modelos compostos personalizados \(componentes\)](#)
- [Configurar AWS IoT SiteWise objeto IDs](#)
- [Crie modelos de ativos e componentes para AWS IoT SiteWise](#)
- [Crie ativos para modelos de ativos em AWS IoT SiteWise](#)
- [Pesquise ativos em Console do AWS IoT SiteWise](#)
- [Atualizar valores de atributo](#)
- [Associar e desassociar ativos](#)
- [Atualizar ativos e modelos](#)
- [Exclua ativos e modelos em AWS IoT SiteWise](#)
- [Operações em massa com ativos e modelos](#)

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 quaisquer mensagens 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 ativo e modelos de componente.
- **CREATING:** o recurso está sendo criado.
- **UPDATING:** o recurso está sendo atualizado.
- **DELETING:** o recurso está sendo excluído.
- **PROPAGATING:** (somente modelos de ativo e modelos de componente) as alterações estão se propagando para todos os recursos dependentes (do modelo de ativo para os ativos ou do modelo de componente para os modelos de ativo).
- **FAILED:** houve falha de validação no recurso durante uma operação de criação ou de atualização, possivelmente devido a uma referência circular em uma expressão. Você pode excluir recursos que estão no estado FAILED.

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, aguarde até que o estado seja alterado para ACTIVE. Caso contrário, suas solicitações falharão.

Tópicos

- [Verificar o status de um ativo](#)
- [Verificar o status de um modelo de ativo ou de componente](#)

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 \(console\)](#)
- [Verificar o status de um ativo \(AWS CLI\)](#)

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 .

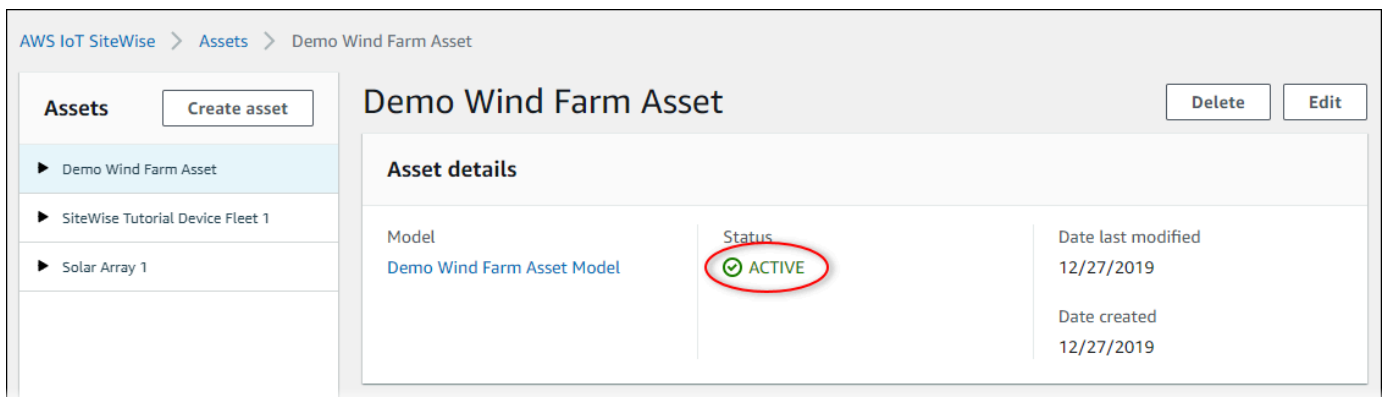
Como verificar o status de um ativo (console)

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 .



Verificar 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 [DescribeAsset](#) operação com o `assetId` parâmetro.

Como verificar o status de um ativo (AWS CLI)

- Execute o comando a seguir para descrever o ativo. *asset-id* Substitua pela ID do ativo ou pela ID externa. O ID externo é um ID definido pelo usuário. Consulte mais informações em [Objetos de referência com objetos externos IDs](#) 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 objeto `assetStatus` com a seguinte estrutura:

```
{
  ...
  "assetStatus": {
    "state": "String",
    "error": {
      "code": "String",
      "message": "String"
    }
  }
}
```

O estado do ativo está em `assetStatus.state` no objeto JSON.

Verificar o status de um modelo de ativo ou 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

- [Verificar o status de um modelo de ativo ou modelo de componente \(console\)](#)
- [Verificar o status de um modelo de ativo ou modelo de componente \(AWS CLI\)](#)

Verificar o status de um modelo de ativo ou modelo de componente (console)

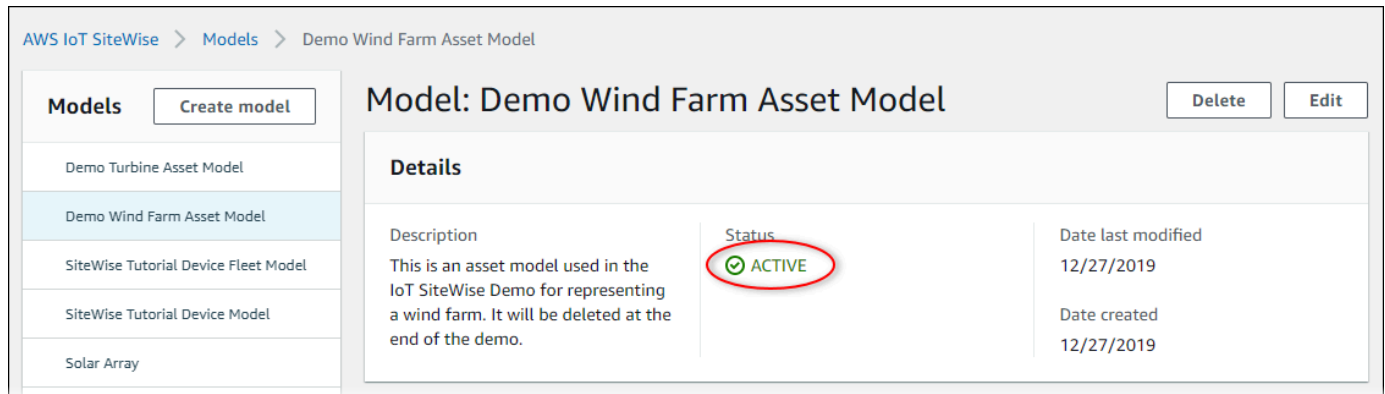
Use o procedimento a seguir para verificar o status de um modelo de ativo ou modelo de componente no AWS IoT SiteWise console.

Tip

Os modelos de ativo e os modelos de componente estão listados em Modelos no painel de navegação. O painel Detalhes do modelo de ativo ou do modelo de componente selecionado indica de que tipo ele é.

Como 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 que deseja verificar.
4. Localize Status no painel Detalhes.



Verificar 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 [DescribeAssetModel](#) operação com o `assetModelId` parâmetro.

Tip

O AWS CLI define modelos de componentes como um tipo de modelo de ativo. Portanto, você usa a mesma [DescribeAssetModel](#) operação para os dois tipos de modelo. O campo `assetModelType` na resposta indica se é um `ASSET_MODEL` ou um `COMPONENT_MODEL`.

Como verificar o status de um modelo de ativo ou modelo de componente (AWS CLI)

- Execute o comando a seguir para descrever o modelo. *asset-model-id* Substitua pela ID ou pela ID externa do modelo do ativo ou do modelo do componente. O ID externo é um ID definido pelo usuário. Consulte mais informações em [Objetos de referência com objetos externos IDs](#) 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 em `assetModelStatus.state` no objeto JSON.

Versões do modelo de ativo

AWS IoT SiteWise suporta o processamento assíncrono de operações de criação e atualização em modelos de ativos e modelos de componentes. Ele também atualiza o status do modelo.

AWS IoT SiteWise propaga as alterações de um modelo válido nas solicitações de criação e atualização para seus recursos dependentes (do modelo do ativo para os ativos ou do modelo do componente para os modelos do ativo). Depois, ele coloca o modelo no estado ACTIVE.

Se a definição do modelo fornecida for inválida, AWS IoT SiteWise coloca o modelo em um FAILED estado. As alterações não serão propagadas para os recursos dependentes. Os recursos dependentes consultam a definição de modelo mais recente propagada quando o modelo estava em um estado ACTIVE.

Com base nas informações acima, as definições de modelo têm dois tipos de versões de modelo:

1. Versão mais recente: a definição mais recente aceita como parte de uma solicitação de criação ou atualização.
2. Versão ativa: a definição mais recente processada com êxito, e o estado do modelo é ACTIVE.

Por padrão, os detalhes da versão mais recente do modelo APIs são retornados quando a descrição é chamada em um modelo de ativo ou modelo de componente. Há cenários em que a versão ativa do modelo de ativo ou do modelo de componente é necessária. Veja alguns exemplos de cenários abaixo:

- Uma operação de atualização com uma definição inválida coloca o modelo de ativo em um estado FAILED. Você deve reverter as alterações, recuperando a versão ativa do modelo de ativo e criando outra solicitação de atualização que faça referência a essa definição válida.
- AWS IoT SiteWise Existe um aplicativo no qual os clientes podem visualizar os ativos e seus modelos de ativos correspondentes. Quando um usuário consulta a definição do modelo de ativo correspondente a um ativo específico e o modelo de ativo está em um estado transitório UPDATING, PROPAGATING ou FAILED, a versão mais recente retorna a definição do modelo de ativo que ainda não foi propagada para os ativos. Nesse caso, você deve recuperar a versão ativa do modelo de ativo para os clientes.

Tópicos

- [Recuperar a versão ativa de um modelo de ativo ou modelo de componente \(console\)](#)
- [Recuperar a versão ativa de um modelo de ativo ou modelo de componente \(AWS CLI\)](#)

Recuperar a versão ativa de um modelo de ativo ou modelo de componente (console)

Siga este procedimento para recuperar a versão ativa de um modelo de ativo ou modelo de componente no AWS IoT SiteWise console.

 Tip

Os modelos de ativo e os modelos de componente estão listados em Modelos no painel de navegação. O painel Detalhes do modelo de ativo ou do modelo de componente selecionado indica de que tipo ele é.

Como recuperar a versão ativa 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 para recuperar a versão ativa dele.
 - a. Se o modelo estiver em um estado ACTIVE, você já estará vendo a versão ativa.
 - b. Se o modelo estiver em um estado transitório UPDATING, PROPAGATING ou FAILED, encontre a opção Ver versão ativa em Status no painel Detalhes.

Recuperar a versão ativa de um modelo de ativo ou modelo de componente (AWS CLI)

Use o AWS CLI para recuperar a versão ativa de um modelo de ativo ou modelo de componente.

Para recuperar a versão ativa de um modelo de ativo ou modelo de componente, use a [DescribeAssetModel](#) operação com o `assetModelVersion` parâmetro.

 Tip

O AWS CLI define modelos de componentes como um tipo de modelo de ativo. Portanto, você usa a mesma [DescribeAssetModel](#) operação para os dois tipos de modelo. O campo `assetModelType` na resposta indica se é um `ASSET_MODEL` ou um `COMPONENT_MODEL`.

Como recuperar a versão ativa de um modelo de ativo ou modelo de componente (AWS CLI)

- Execute o comando a seguir para descrever o modelo. *asset-model-id* Substitua pela ID ou pela ID externa do modelo do ativo ou do modelo do componente. O ID externo é um ID definido

pelo usuário. Consulte mais informações em [Objetos de referência com objetos externos IDs](#) no Guia de Usuário AWS IoT SiteWise .

```
aws iotsitewise describe-asset-model --asset-model-id asset-model-id --asset-model-version ACTIVE
```

A operação retorna uma resposta com os detalhes do modelo. A resposta contém um objeto `assetModelStatus` com a estrutura a seguir.

```
{
  ...
  "assetModelName": "string",
  "assetModelProperties": [ ... ],
  ...,
  "assetModelVersion": "string"
}
```

Modelos compostos personalizados (componentes)

Ao modelar um ativo industrial especialmente complexo, como uma máquina complicada que tenha muitas peças, pode ser um desafio manter os modelos de ativo organizados e sustentáveis.

Nesses casos, você pode adicionar modelos compostos personalizados, ou componentes se estiver usando o console, aos modelos de ativo e modelos de componente existentes. Isso ajuda você a manter a organização ao agrupar propriedades relacionadas e reutilizar definições de subcomponente.

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 modelo de componente ao qual o modelo composto personalizado pertence. Use-os para agrupar propriedades relacionadas. Eles consistem em um nome, uma descrição e um conjunto de propriedades do modelo de ativo. Eles não são reutilizáveis.
- Os modelos compostos `omponent-model-based` personalizados em C fazem referência a um modelo de componente que você deseja incluir em seu modelo de ativo ou modelo de componente. Use-os para incluir subconjuntos padrão no modelo. Eles consistem em um nome, uma descrição e 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 todos os ativos criados.

As seções a seguir ilustram como usar modelos compostos personalizados nos designs.

Tópicos

- [Modelos compostos personalizados em linha](#)
- [Component-model-based modelos compostos personalizados](#)
- [Usar caminhos para fazer referência a propriedades do modelo composto personalizado](#)

Modelos compostos personalizados em linha

Os modelos compostos personalizados em linha oferecem uma maneira de organizar o modelo de ativo ao agrupar propriedades relacionadas.

Por exemplo, vamos supor que você queira modelar um ativo de robô. O robô inclui um servomotor, uma fonte de alimentação e uma bateria. Cada uma dessas partes constituintes tem propriedades próprias que você deseja incluir no modelo. Você pode definir um modelo de ativo chamado `robot_model` que tenha as propriedades mostradas a seguir.

- `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, é possível que haja tantas propriedades que se torne difícil referenciar 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 em linha para agrupar as propriedades. Um modelo composto personalizado em linha é um tipo de modelo

composto personalizado que define as próprias propriedades. Por exemplo, você poderia modelar o robô conforme mostrado a seguir.

- `robot_model`
 - `servo`
 - `status` (inteiro)
 - `position` (duplo)
 - `powersupply`
 - `status` (inteiro)
 - `temperature` (duplo)
 - `battery`
 - `status` (inteiro)
 - `charge` (duplo)

No exemplo anterior, `servo`, `powersupply` e `battery` são os nomes dos modelos compostos personalizados em linha definidos no modelo de ativo `robot_model`. Cada um desses modelos compostos define as próprias propriedades.

Note

Nesse caso, cada modelo composto personalizado define as próprias propriedades, de maneira 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 tivesse criado algum outro modelo de ativo que também tivesse um modelo composto personalizado em linha chamado `servo`, fazer uma alteração em `servo` dentro de `robot_model` não afetaria a definição de `servo` do outro modelo de 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 `component-model-based` compostos que façam referência a ele. Para conferir detalhes, consulte a seção a seguir.

Para ter mais informações sobre como criar modelos compostos personalizados em linha, consulte [Criar modelos compostos personalizados \(componentes\)](#).

Component-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 poderá adicionar referências a ele nos outros modelos de ativo e modelos de componente. Você faz isso adicionando um modelo composto component-model-based personalizado a qualquer modelo em que queira referenciar o componente. É possível adicionar referências ao componente de muitos modelos ou várias vezes no mesmo modelo.

Dessa forma, você pode evitar a duplicação das mesmas definições nos modelos. Isso também simplifica a manutenção dos modelos, porque todas as alterações feitas em um modelo de componente serão refletidas em todos os modelos de ativo que o utilizam.

Por exemplo, vamos supor que a 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 ter que duplicar a definição de `servo` toda vez. Você quer modelá-lo apenas uma vez e usá-lo nos vários modelos de ativo. Se, posteriormente, você fizer uma alteração na definição de `servo`, ele será atualizado em todos os modelos e ativos.

Para modelar o robô do exemplo anterior assim, você pode definir servomotores, fontes de alimentação e baterias como modelos de componente, conforme mostrado a seguir.

- `servo_component_model`
 - `status` (inteiro)
 - `position` (duplo)

- `powersupply_component_model`
 - `status` (inteiro)
 - `temperature` (duplo)

- `battery__component_model`

- `status` (inteiro)
- `charge` (duplo)

Depois, você pode definir modelos de ativo, como `robot_model`, que fazem referência a esses componentes. Vários modelos de ativo podem fazer referência ao mesmo modelo de componente. Você também pode fazer referência ao mesmo modelo de componente várias vezes em um modelo de ativo, por exemplo, se o robô tiver 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 ter informações sobre como criar modelos de componente, consulte [Criar modelos de componente](#).

Para ter informações sobre como fazer referência aos modelos de componente em outros modelos, consulte [Criar modelos compostos personalizados \(componentes\)](#).

Usar caminhos para fazer referência a propriedades do modelo composto personalizado

Ao criar uma propriedade em um modelo de ativo, modelo de componente ou modelo composto personalizado, você pode referenciá-la de outras propriedades que usem o valor dela, 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 fazer referência a ela por caminho.

Um caminho é uma sequência ordenada de segmentos de caminho que especifica uma propriedade em termos da posição entre os modelos compostos aninhados dentro de um modelo de ativo e modelo composto.

Obter caminhos de propriedade

Você pode obter o caminho de uma propriedade a partir do path campo dela [AssetModelProperty](#).

Por exemplo, vamos supor que você tenha um modelo de ativo `robot_model` que contenha um modelo composto personalizado `servo` com uma propriedade `position`. Se você [DescribeAssetModelCompositeModel](#)ligar `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"  
  }  
]
```

Usar caminhos de propriedade

Você pode usar um caminho de propriedade ao definir uma propriedade que faz referência a outras propriedades, como uma transformação ou uma métrica.

Uma propriedade usa uma variável para fazer referência a outra propriedade. Para ter mais informações sobre como trabalhar com variáveis, consulte [Usar variáveis em expressões de fórmula](#).

Ao definir uma variável para fazer referência a uma propriedade, você pode usar o ID ou o caminho da propriedade.

Para definir uma variável que use o caminho da propriedade referenciada, especifique o campo `propertyPath` do 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
                ]
              }
            }
          ]
        }
      },
      ...
    },
    ...
  ],
  ...
}
```

Configurar AWS IoT SiteWise objeto IDs

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 objetos.

Tópicos

- [Trabalhar com objeto UUIDs](#)
- [Use externo IDs](#)

Trabalhar com objeto UUIDs

Cada objeto persistente AWS IoT SiteWise tem um [UUID](#) para identificá-lo. Por exemplo, modelos de ativo têm um ID de modelo de ativo, ativos têm um ID de ativo e assim por diante. Esse ID é atribuído no momento em que você cria o objeto e permanece inalterado 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 o próprio ID no momento da criação no formato UUID.

Note

UUIDs deve ser globalmente exclusivo na AWS região em que foi criado e para o mesmo tipo de objeto. Quando AWS IoT SiteWise gera automaticamente um ID para você, ele é sempre exclusivo. Se você escolher o próprio ID, garanta que ele seja 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, o AWS IoT SiteWise vai gerar um UUID para o novo modelo de ativo.

Use externo IDs

Para definir o próprio ID em algum formato diferente de 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. IDs Os externos têm um formato mais flexível. Você pode usá-los para fazer referência aos objetos em operações de API do AWS IoT SiteWise em que, de outra forma, usaria o UUID.

Assim como a UUIDs, cada ID externa deve ser exclusiva dentro de seu contexto. Por exemplo, não é possível ter dois modelos de ativo com o mesmo ID externo. Além disso, como o UUIDs, um objeto só pode ter uma ID externa em sua vida útil, que não pode ser alterada.

Diferenças entre externo IDs e UUIDs

IDs Os externos UUIDs diferem das seguintes formas:

- Cada objeto tem um UUID, mas os externos IDs são opcionais.
- AWS IoT SiteWise nunca gera algo externo IDs. Você os fornece por conta própria.
- Se o objeto ainda não tiver um, você poderá atribuir um ID externo a qualquer momento.

Formato externo IDs

Um ID externo válido tem as seguintes propriedades:

- Ele tem entre 2 e 128 caracteres.
- O primeiro e o último caracteres devem ser alfanuméricos (A–Z, a–z, 0–9).
- Os demais caracteres devem ser alfanuméricos ou os seguintes: _ - . :

Por exemplo, um ID externo deve estar em conformidade com a seguinte expressão regular:

```
[a-zA-Z0-9][a-zA-Z0-9_\-\. :]*[a-zA-Z0-9]+
```

Objetos de referência com objetos externos IDs

Em muitos locais em que é possível fazer referência a um objeto usando o UUID, você pode usar o ID externo em vez disso, caso ele tenha um. Para isso, acrescente o ID externo à string `externalId:`.

Por exemplo, vamos supor que você tenha um modelo de ativo cujo UUID (ID do modelo de ativo) seja `a1b2c3d4-5678-90ab-cdef-11111EXAMPLE`, que também tem o ID externo `myExternalId`. Ligue [DescribeAssetModel](#) para obter detalhes sobre isso. Você pode usar qualquer uma das seguintes opções como valor de `assetModelId`:

- Com o próprio ID do modelo de ativo (UUID): `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 prefixo `externalId`: não faz, por si só, parte do ID externo. Você só precisa fornecer o prefixo ao fornecer uma ID externa a uma operação de API que aceita uma UUIDs ou uma externa IDs. Por exemplo, forneça o prefixo ao consultar ou atualizar um objeto existente. Ao definir um ID externo para um objeto, como ao criar um modelo de ativo, não inclua o prefixo.

Você pode usar external IDs no lugar de UUIDs dessa forma para muitas operações de API em AWS IoT SiteWise, mas não em todas. Por exemplo, o [GetAssetPropertyValue](#), must use 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 de API](#).

Crie modelos de ativos e componentes para AWS IoT SiteWise

AWS IoT SiteWise modelos de ativos e modelos de componentes impulsionam a padronização de seus dados industriais. Os modelos de ativo e de componente representam a estrutura e as propriedades dos ativos industriais e dos respectivos componentes. Os modelos de ativo definem o ativo de forma geral, como uma turbina eólica ou uma linha de produção. Os modelos de componente representam os componentes individuais que compõem o ativo, como pás, geradores ou sensores. Ao criar esses modelos, você pode organizar e estruturar os dados de ativos de maneira que reflita as relações e as hierarquias reais dos equipamentos industriais, facilitando o monitoramento, a análise e a manutenção.

Um modelo de ativo ou modelo de componente contém nome, descrição, propriedades de ativo e (opcionalmente) modelos compostos personalizados que agrupam propriedades ou que fazem referência a modelos de componente para subconjuntos.

Em AWS IoT SiteWise, você pode criar modelos de ativos e modelos de componentes para representar a estrutura e as propriedades de seus ativos industriais e seus componentes.

- Você pode usar um modelo de ativo para criar ativos. Além dos recursos listados acima, um modelo de ativo também pode conter definições de hierarquia que definem relações entre ativos.
- Um modelo de componente representa um subconjunto dentro de um modelo de ativo ou de outro modelo de componente. Ao criar um modelo de componente, você pode adicionar referências a

ele em modelos de ativo e em outros modelos de componente. No entanto, não é possível criar ativos diretamente nos modelos de componente.

Depois de criar um modelo de ativo ou modelo de componente, você poderá criar modelos compostos personalizados para agrupar propriedades ou fazer referência a modelos de componente existentes.

Para conferir detalhes sobre como criar modelos de ativo e modelos de componente, consulte as seções a seguir.

Tópicos

- [Crie modelos de ativos em AWS IoT SiteWise](#)
- [Criar modelos de componente](#)
- [Definir propriedades de dados](#)
- [Criar modelos compostos personalizados \(componentes\)](#)

Crie modelos de ativos em AWS IoT SiteWise

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 ativo não podem conter outros modelos de ativo. Se você precisar definir um modelo ao qual possa fazer referência como um subconjunto dentro de outro modelo, crie um modelo de componente em vez disso. Para obter mais informações, consulte [Criar modelos de componente](#).

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 \(console\)](#)
- [Criar um modelo de ativo \(AWS CLI\)](#)
- [Exemplos de modelos de ativos](#)
- [Definir hierarquias de modelos de ativo](#)

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 um ID externo para o modelo. É um ID definido pelo usuário. Consulte mais informações em [Objetos de referência com objetos externos IDs](#) 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 obter mais informações, consulte [Definir fluxos de dados de equipamentos \(medições\)](#).
 - d. (Opcional) Adicione Definições de transformação ao modelo. As transformações são fórmulas que mapeiam dados de um formulário para outro. Para obter mais informações, consulte [Transformar 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 obter mais informações, consulte [Agregação de dados de propriedades e outros ativos \(métricas\)](#).

- f. (Opcional) Adicione Definições de hierarquia ao modelo. Hierarquias são relacionamentos entre ativos. Para obter mais informações, consulte [Definir hierarquias de modelos de ativo](#).
- g. (Opcional) Adicione tags ao modelo de ativo. Para obter mais informações, consulte [Marque seus AWS IoT SiteWise recursos](#).
- 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 obter 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, consulte [Configure os recursos de borda no AWS IoT SiteWise Edge](#).
 - 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 [Configurar uma fonte OPC UA no SiteWise Edge](#).
 - 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 [Configurar uma fonte OPC UA no SiteWise Edge](#).

- d. Escolha Salvar. Na página do modelo, sua configuração do Edge agora deve estar Configurada.

Criar 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 [CreateAssetModel](#) 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
}
```

Como 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**. Esse nome deve ser exclusivo entre todos os modelos de ativo e modelos de componente da conta nessa Região da AWS.
 - b. (Opcional) Insira um ID externo (`assetModelExternalId`) para o modelo de ativo. É um ID definido pelo usuário. Consulte mais informações em [Objetos de referência com objetos externos IDs](#) 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 obter mais informações, consulte [Definir propriedades de dados](#).
 - e. (Opcional) Defina hierarquias de ativos (`assetModelHierarchies`) para o modelo. Para obter mais informações, consulte [Definir hierarquias de modelos de ativo](#).
 - 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 [Monitore dados com alarmes em AWS IoT SiteWise](#) e [Defina alarmes em modelos de ativos em AWS IoT SiteWise](#).
 - g. (Opcional) Adicione tags (`tags`) ao modelo de ativo. Para obter mais informações, consulte [Marque seus AWS IoT SiteWise recursos](#).
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 [DescribeAssetModel](#) operação especificando o `assetModelId`. Depois que o status do modelo de ativo for ACTIVE, você poderá usá-lo para criar ativos. Para obter mais informações, consulte [Estados de ativos e modelos](#).

4. (Opcional) Crie modelos compostos personalizados para o modelo de ativo. Com modelos compostos personalizados, você pode agrupar propriedades dentro do modelo ou incluir um subconjunto ao fazer referência a um modelo de componente. Para obter mais informações, consulte [Criar 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 AWS CLI AWS IoT SiteWise SDKs 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 obter mais informações, consulte [Use 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) com base nos dados de todas as turbinas eólicas no parque.

Note

Esse modelo de exemplo se assemelha ao modelo de parque eólico da AWS IoT SiteWise demonstração. Para obter mais informações, consulte [Use 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"
  }
]
}

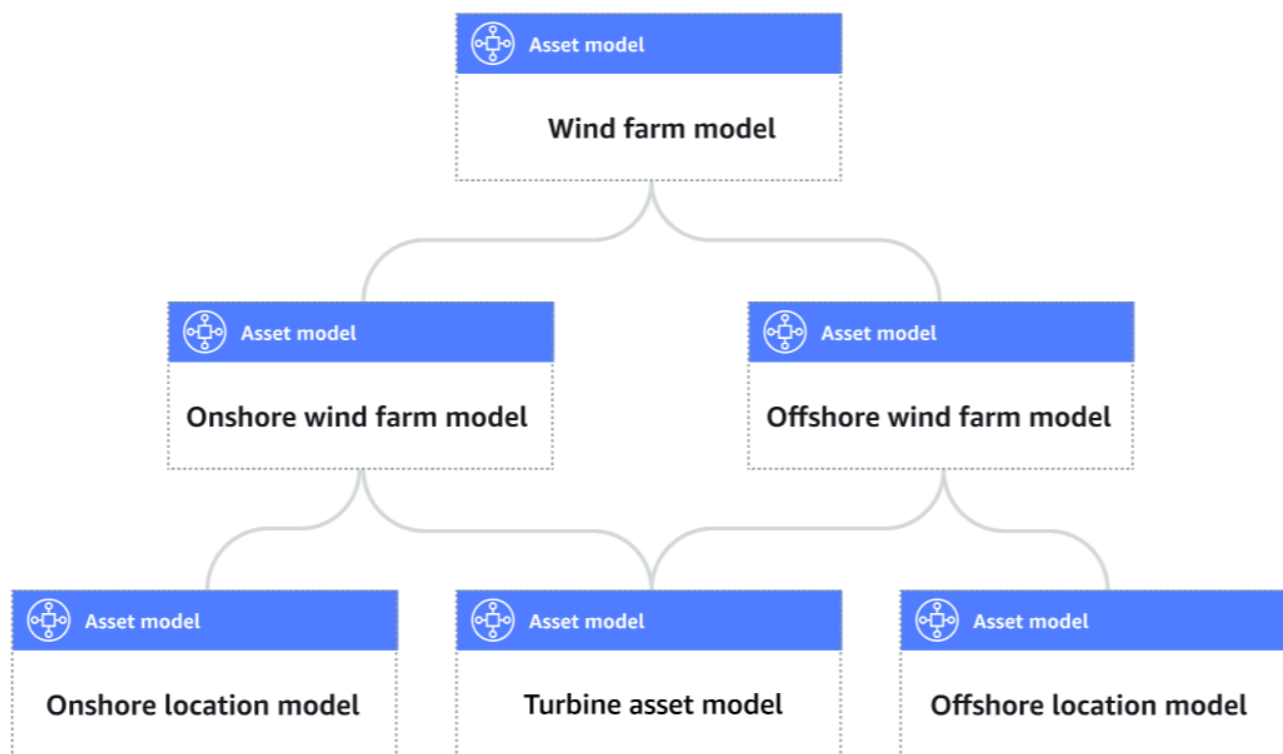
```

Definir hierarquias de modelos de ativo

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.



Asset model hierarchy



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 obter mais informações, consulte [Agregação de 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 obter 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 [Crie ativos para modelos de ativos em AWS IoT SiteWise](#) e [Associar e desassociar ativos](#).

Tópicos

- [Definir hierarquias de modelos de ativo \(console\)](#)
- [Definir hierarquias de ativos \(AWS CLI\)](#)

Definir hierarquias de modelos de ativo (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 externo da hierarquia (opcional): é um ID definido pelo usuário. Consulte mais informações em [Objetos de referência com objetos externos IDs](#) no Guia de Usuário AWS IoT SiteWise .

Para obter mais informações, consulte [Criar um modelo de ativo \(console\)](#).

Definir 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 filho para a hierarquia. Você pode usar a [ListAssetModels](#) operação para encontrar a ID de um modelo de ativo existente.

Exemplo 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 um [AssetModelHierarchy](#). Para obter mais informações, consulte [Criar um modelo de ativo \(AWS CLI\)](#).

```
{
  ...
  "assetModelHierarchies": [
    {
      "name": "Wind Turbines",
      "childAssetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE"
    },
  ]
}
```

Criar modelos de componente

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 dentro do 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 ativo. No entanto, os modelos de componente não podem incluir definições de hierarquia de ativos, pois não é possível usar os modelos de componente em si para criar ativos diretamente. Os modelos de componente 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. Depois, você poderá 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 o componente de servomotor antes de criar o modelo de ativo da máquina CNC. Os modelos de ativo contêm referências aos modelos de componente existentes.
- Não é possível criar um ativo diretamente de um modelo de componente. Para criar um ativo que use o componente, você deve criar um modelo de ativo para o ativo. Depois, crie um modelo composto personalizado para ele que faça referência ao componente. Para ter mais informações sobre a criação de modelos de ativo, consulte [Crie modelos de ativos em AWS IoT SiteWise](#). Para ter mais informações sobre a criação de modelos compostos personalizados, consulte [Criar modelos compostos personalizados \(componentes\)](#).

As seções a seguir descrevem como usar a AWS IoT SiteWise API para criar modelos de componentes.

Tópicos

- [Criar um modelo de componente \(AWS CLI\)](#)
- [Exemplo de modelo de componente](#)

Criar um modelo de componente (AWS CLI)

Você pode usar o AWS Command Line Interface (AWS CLI) para criar um modelo de componente.

Use a [CreateAssetModel](#) operação 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,
}
```

Como criar um modelo de componente (AWS CLI)

1. Crie um arquivo chamado `component-model-payload.json` e 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 de componente, como **Servo Motor** ou **Servo Motor Model**. Esse nome deve ser exclusivo entre todos os modelos de ativo e modelos de componente da conta nessa Região da AWS.
 - b. (Opcional) Insira um ID externo (`assetModelExternalId`) para o modelo de componente. É um ID definido pelo usuário. Consulte mais informações em [Objetos de referência com objetos externos IDs](#) 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 de ativo (`assetModelProperties`) para o modelo de componente. Para obter mais informações, consulte [Definir propriedades de dados](#).
 - e. (Opcional) Adicione tags (`tags`) ao modelo de ativo. Para obter mais informações, consulte [Marque seus AWS IoT SiteWise recursos](#).
3. Execute o comando a seguir para criar um modelo de componente com base na definição no arquivo JSON.

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

A operação retorna uma resposta que contém o `assetModelId` que você referencia ao adicionar uma referência ao 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 de componente é `CREATING` até que as alterações sejam propagadas.

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 [DescribeAssetModel](#) operação especificando o `assetModelId`. Depois que o status do modelo de componente for `ACTIVE`, você poderá adicionar referências ao modelo de componente em modelos de ativo ou outros modelos de componente. Para obter mais informações, consulte [Estados de ativos e modelos](#).

4. (Opcional) Crie modelos compostos personalizados para o modelo de componente. Com modelos compostos personalizados, você pode agrupar propriedades dentro do modelo ou incluir um subconjunto ao fazer referência a outro modelo de componente. Para obter mais informações, consulte [Criar 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 AWS CLI AWS IoT SiteWise SDKs e. Esse modelo de componente representa um servomotor que pode ser usado em outro equipamento, como uma máquina CNC.

Tópicos

- [Modelo de componente do servomotor](#)

Modelo de componente do servomotor

O modelo de componente a seguir representa um servomotor que pode ser usado em equipamentos, como máquinas CNC. O servomotor oferece várias medições, como temperaturas e resistência elétrica. Essas medições estão disponíveis como propriedades em ativos criados com base em modelos de ativo que fazem referência ao modelo de componente 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 obter mais informações, consulte [Definir 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 obter mais informações, consulte [Definir fluxos de dados de equipamentos \(medições\)](#).

- 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 obter mais informações, consulte [Transformar 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 obter mais informações, consulte [Agregar dados de propriedades e outros ativos \(métricas\)](#).

Para obter mais informações, consulte [Crie modelos de ativos em AWS IoT SiteWise](#).

Para obter um exemplo de como usar medições, transformações e métricas para calcular a Eficácia Geral do Equipamento (OEE), consulte [Calcule o OEE em AWS IoT SiteWise](#).

Tópicos

- [Definir dados estáticos \(atributos\)](#)
- [Definir fluxos de dados de equipamentos \(medições\)](#)
- [Transformar dados \(transformações\)](#)
- [Agregar dados de propriedades e outros ativos \(métricas\)](#)
- [Usar expressões de fórmula](#)

Definir 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 \(console\)](#)
- [Definir 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 [-10¹⁰⁰, 10¹⁰⁰] e precisão dupla IEEE 754.
 - Booleano — true ou false.
- ID externo: (opcional) é um ID definido pelo usuário. Consulte mais informações em [Objetos de referência com objetos externos IDs](#) no Guia de Usuário AWS IoT SiteWise .

Para obter mais informações, consulte [Criar um modelo de ativo \(console\)](#).

Definir 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 [-10¹⁰⁰, 10¹⁰⁰] e precisão dupla IEEE 754.

- BOOLEAN – true ou false.
- externalId: (opcional) é um ID definido pelo usuário. Consulte mais informações em [Objetos de referência com objetos externos IDs](#) no Guia de Usuário AWS IoT SiteWise .

Exemplo 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 um [AssetModelProperty](#) que contém um [Atributo](#). Você pode especificar esse objeto como parte da carga útil da solicitação [CreateAssetModel](#) para criar uma propriedade de atributo. Para obter mais informações, consulte [Criar um modelo de ativo \(AWS CLI\)](#).

```
{
  ...
  "assetModelProperties": [
    {
      "name": "Model number",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "BLT123"
        }
      }
    }
  ],
  ...
}
```

Definir fluxos de dados de equipamentos (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

- [Definir medições \(console\)](#)
- [Definir medições \(AWS CLI\)](#)

Definir 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 [-10¹⁰⁰, 10¹⁰⁰] e precisão dupla IEEE 754.
 - Booleano — true ou false.
- ID externo: (opcional) é um ID definido pelo usuário. Consulte mais informações em [Objetos de referência com objetos externos IDs](#) no Guia de Usuário AWS IoT SiteWise .

Para obter mais informações, consulte [Criar um modelo de ativo \(console\)](#).

Definir medições (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 [-10¹⁰⁰, 10¹⁰⁰] e precisão dupla IEEE 754.
 - BOOLEAN – true ou false.
- unit – (opcional) unidade científica da propriedade, como mm ou Celsius.
- externalId: (opcional) é um ID definido pelo usuário. Consulte mais informações em [Objetos de referência com objetos externos IDs](#) 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 um [AssetModelProperty](#) que contém uma [medida](#). Você pode especificar esse objeto como parte da carga útil da solicitação [CreateAssetModel](#) para criar uma propriedade de medição. Para obter mais informações, consulte [Criar 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 [Gerencie fluxos de dados para AWS IoT SiteWise](#).

```
{
    ...
    "assetModelProperties": [
        {
            "name": "Temperature C",
            "dataType": "DOUBLE",
            "type": {
                "measurement": {}
            },
            "unit": "Celsius"
        }
    ],
    ...
}
```

Transformar 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.

 Note

Para atualizações de propriedades com o mesmo carimbo de data/hora, os valores de saída podem ser substituídos por atualizações de outras propriedades de entrada.

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 string que identifica o tipo de peça.
- `Good_Count`: um inteiro que aumenta em uma unidade caso a peça atenda ao padrão.
- `Bad_Count`: um inteiro que aumenta em uma unidade caso a peça não atenda 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 \(console\)](#)
- [Definir 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 externo: (opcional) é um ID definido pelo usuário. Consulte mais informações em [Objetos de referência com objetos externos IDs](#) 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 obter mais informações, consulte [Usar 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 atributo não inicializam 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 obter mais informações, consulte [Valores indefinidos, infinitos e excedidos](#).

Para obter mais informações, consulte [Criar um modelo de ativo \(console\)](#).

Definir 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) é um ID definido pelo usuário. Consulte mais informações em [Objetos de referência com objetos externos IDs](#) 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 obter mais informações, consulte [Usar 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 atributo não inicializam 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 obter mais informações, consulte [Valores indefinidos, infinitos e excedidos](#).

Exemplo 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 um [AssetModelProperty](#) que contém uma [transformação](#). Você pode especificar esse objeto como parte da carga útil da solicitação [CreateAssetModel](#) para criar uma propriedade de transformação. Para obter mais informações, consulte [Criar um modelo de ativo \(AWS CLI\)](#).

```
{
  ...
  "assetModelProperty": [
    ...
    {
      "name": "Temperature F",
      "dataType": "DOUBLE",
      "type": {
        "transform": {
          "expression": "9/5 * temp_c + 32",
          "variables": [
            {
              "name": "temp_c",
              "value": {
                "propertyId": "Temperature C"
              }
            }
          ]
        }
      },
      "unit": "Fahrenheit"
    }
  ],
  ...
}
```

Exemplo 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 BLT123 peças 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"
              }
            }
          ]
        }
      }
    }
  ]
}
...
}
```


Agregar 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 [Definir hierarquias de modelos de ativo](#).

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 obter mais informações, consulte [Consulte agregados de propriedades de ativos em AWS IoT SiteWise](#).

Tópicos

- [Definir métricas \(console\)](#)
- [Definir 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 externo: (opcional) é um ID definido pelo usuário. Consulte mais informações em [Objetos de referência com objetos externos IDs](#) 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 obter mais informações, consulte [Usar 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 obter 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

Exemplo 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 a métrica é criada em 1º de julho de 2021, até as 18h30min30s (PST), você recebe o primeiro resultado da agregação em 1º de julho de 2021, às 18h30min30s (PST). O segundo resultado da agregação chega em 2 de julho de 2021, às 6h30min30s (PST), e assim por diante.

Definir 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) é um ID definido pelo usuário. Consulte mais informações em [Objetos de referência com objetos externos IDs](#) 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 obter mais informações, consulte [Usar 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 [TumblingWindow](#) na Referência de APIs do AWS IoT SiteWise .

Exemplo 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 a métrica é criada em 1º de julho de 2021, até as 18h30min30s (PST), você recebe o primeiro resultado da agregação em 1º de julho de 2021, às 18h30min30s (PST). O segundo resultado da agregação chega em 2 de julho de 2021, às 6h30min30s (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 obter 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 um [AssetModelProperty](#) que contém uma [métrica](#). Você pode especificar esse objeto como parte da carga útil da solicitação [CreateAssetModel](#) para criar uma propriedade de métrica. Para obter mais informações, consulte [Criar um modelo de ativo \(AWS CLI\)](#).

```
{  
  ...  
  "assetModelProperty": [  
    ...  
    {  
      "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 um [AssetModelProperty](#) que contém uma [métrica](#). Você pode especificar esse objeto como parte da carga útil da solicitação [CreateAssetModel](#) para criar uma propriedade de 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"
},
...
}
```

Usar 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 [Transformar dados \(transformações\)](#) e [Agregação de dados de propriedades e outros ativos \(métricas\)](#).

Transformações e métricas são propriedades da fórmula.

Tópicos

- [Usar variáveis em expressões de fórmula](#)
- [Usar literais em expressões de fórmula](#)
- [Usar operadores em expressões de fórmula](#)
- [Usar constantes em expressões de fórmula](#)
- [Usar funções em expressões de fórmula](#)
- [Tutoriais de expressão de fórmulas](#)

Usar variáveis em expressões de fórmula

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 [ExpressionVariable](#) estrutura, 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](#).

Usar variáveis para fazer referência a propriedades

O valor de uma variável define a propriedade que ela referencia. O AWS IoT SiteWise oferece maneiras diferentes de fazer isso.

- Por ID da propriedade: você pode especificar o ID exclusivo da propriedade (UUID) para identificá-la.
- Por nome: se a propriedade estiver no mesmo modelo de ativo, você poderá especificar o nome no campo de ID da propriedade.
- Por caminho: o valor de uma variável pode fazer referência a uma propriedade pelo caminho. Para obter mais informações, consulte [Usar caminhos para fazer referência a propriedades do modelo composto personalizado](#).

 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), AWS SDKs e.

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 especificar o caminho, você não precisará fornecer o ID.

Usar literais em expressões de fórmula

AWS IoT SiteWise suporta o uso de literais em expressões e fórmulas. Literais são valores fixos que representam um tipo de dados específico. Em AWS IoT SiteWise, você pode definir literais numéricos e de seqüências de caracteres em expressões de fórmula. Os literais podem ser usados em vários contextos, inclusive transformações de dados, condições de alarme e cálculos de visualização.

- 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"}'

Usar 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 <code>1 + 2 + " is three"</code> é avaliada como <code>"3 is three"</code>. 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. 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).

Operador	Descrição
	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.
$x \leq y$	Retorna 1 se x for menor ou igual a y, caso contrário, 0.
$x \geq y$	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.
$x \neq y$	Retorna 1 se x não for igual a y, caso contrário, 0.

Operador	Descrição
<code>! x</code>	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.
<code>x and y</code>	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
<code>x or y</code>	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.
<code>not x</code>	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.
<code>[]</code> <code>s[index]</code>	Retorna o caractere em um índice <code>index</code> da string <code>s</code>. Isso é equivalente à sintaxe do índice em Python. Example Exemplos • <code>"Hello!"[1]</code> Retorna e. • <code>"Hello!"[-2]</code> Retorna o.

Operador	Descrição
[] <code>s[start:end:step]</code>	Retorna uma fatia da string <code>s</code>. Isso é equivalente à fatia da sintaxe do índice em Python. Esse operador tem os seguintes argumentos: • <code>start</code> — (opcional) índice inicial inclusivo da fatia. O padrão é 0. • <code>end</code> — (opcional) índice final exclusivo da fatia. O padrão é o comprimento da string. • <code>step</code> — (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. O padrão é 1. Você pode omitir o argumento <code>step</code> para usar seu valor padrão. Por exemplo, <code>s[1:4:1]</code> equivale a <code>s[1:4]</code>. Os argumentos devem ser números inteiros ou a constante nenhum. Se você especificar <code>nenhum</code>, AWS IoT SiteWise usa o valor padrão para esse argumento. Example Exemplos • <code>"Hello!"[1:4]</code> Retorna <code>"ell"</code>. • <code>"Hello!"[:2]</code> Retorna <code>"He"</code>. • <code>"Hello!"[3:]</code> Retorna <code>"lo!"</code>. • <code>"Hello!"[:-4]</code> Retorna <code>"He"</code>. • <code>"Hello!"[:2]</code> Retorna <code>"Hlo"</code>. • <code>"Hello!"[::-1]</code> Retorna <code>"!olleH"</code>.

Usar constantes em expressões de fórmula

Em AWS IoT SiteWise, você pode usar constantes em suas expressões e fórmulas para representar valores fixos ou parâmetros predefinidos. As constantes podem ser usadas em vários contextos, como transformações de dados, condições de alarme ou cálculos de visualização. Ao usar constantes, você pode simplificar as expressões e deixá-las mais legíveis e fáceis de sustentáveis.

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 .

Usar funções em expressões de fórmula

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	Métricas
Usar funções comuns em expressões de fórmula	 Yes (Sim)	 Yes (Sim)
Usar funções de comparação em expressões de fórmula	 Yes (Sim)	 Yes (Sim)
Usar funções condicionais em expressões de fórmula	 Yes (Sim)	 Yes (Sim)
Usar funções de string em expressões de fórmula	 Yes (Sim)	 Yes (Sim)
Usar funções de agregação em expressões de fórmula	 Não	 Yes (Sim)

Tipo de função	Transformações	Métricas
Usar funções temporais em expressões de fórmula	 Yes (Sim)	 Yes (Sim)
Usar funções de data e hora em expressões de fórmula	 Yes (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.

Usar funções comuns em expressões de fórmula

Em [transformações](#) e [métricas](#), você pode usar as seguintes funções para calcular funções matemáticas comuns em transformações e métricas:

Função	Descrição
<code>abs(x)</code>	Retorna o valor absoluto de x.
<code>acos(x)</code>	Retorna o arco cosseno de x.
<code>asin(x)</code>	Retorna o arco seno de x.
<code>atan(x)</code>	Retorna o arco tangente de x.
<code>cbrt(x)</code>	Retorna a raiz cúbica de x.
<code>ceil(x)</code>	Retorna o inteiro mais próximo maior que x.
<code>cos(x)</code>	Retorna o cosseno de x.
<code>cosh(x)</code>	Retorna o cosseno hiperbólico de x.
<code>cot(x)</code>	Retorna o co-tangente de x.
<code>exp(x)</code>	Retorna e à potência de x.
<code>expm1(x)</code>	Retorna $\exp(x) - 1$. Use essa função para calcular com mais precisão $\exp(x) - 1$ para valores pequenos de x.
<code>floor(x)</code>	Retorna o inteiro mais próximo menor que x.

Função	Descrição
$\log(x)$	Retorna o $\log_e$ (base e) de x.
$\log_{10}(x)$	Retorna o $\log_{10}$ (base 10) de x.
$\log_{1p}(x)$	Retorna $\log(1 + x)$. Use essa função para calcular com mais precisão $\log(1 + x)$ para valores pequenos de x.
$\log_2(x)$	Retorna o $\log_2$ (base 2) de x.
$\text{pow}(x, y)$	Retorna x à potência de y. Isso é equivalente a x^y .
$\text{signum}(x)$	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.
$\text{sqrt}(x)$	Retorna a raiz quadrada de x.
$\tan(x)$	Retorna a tangente de x.
$\tanh(x)$	Retorna a tangente hiperbólica de x.

Usar funções de comparação em expressões de fórmula

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
$\text{gt}(x, y)$	Retorna 1 se x for maior que y, caso contrário 0 ($x > y$).

Função	Descrição
	Essa função não retorna um valor se x e y forem tipos incompatíveis, como um número e uma string.
<code>gte(x, y)</code>	Retorna 1 se x for maior ou igual a y, caso contrário 0 ($x \geq y$). 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.
<code>eq(x, y)</code>	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.
<code>lt(x, y)</code>	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
<code>lte(x, y)</code>	Retorna 1 se x for menor ou igual a y, caso contrário 0 ($x \leq y$). 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.
<code>isnan(x)</code>	Retorna 1 se x for igual a NaN, caso contrário, 0. Essa função não retorna um valor se x for uma string.

Usar funções condicionais em expressões de fórmula

Em [transformações](#) e [métricas](#), você pode usar a função a seguir para verificar uma condição e retornar resultados diferentes de acordo com a avaliação da condição como verdadeira ou falsa.

Função	Descrição
<code>if(condition, result_if_true, result_if_false)</code>	Avalia <code>condition</code> e retorna <code>result_if_true</code> se a condição for avaliada como verdadeira ou <code>result_if_false</code> se a condição for avaliada como <code>false</code>. <code>condition</code> deve ser um número. Essa função considera 0 uma string vazia como <code>false</code> e todo o resto (inclusive NaN) como <code>true</code>. 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 obter mais informações, consulte Filtrar pontos de dados. Example Exemplos • <code>if(0, x, y)</code> retorna a variável <code>y</code>. • <code>if(5, x, y)</code> retorna a variável <code>x</code>. • <code>if(gt(temp, 300), x, y)</code> retorna a variável <code>x</code> se a variável <code>temp</code> for maior que 300. • <code>if(gt(temp, 300), temp, none)</code> retorna a variável <code>temp</code> se for maior ou igual a 300, ou <code>none</code> (sem valor), se <code>temp</code> for menor que 300. Recomendamos que você use UFCS para funções condicionais aninhadas onde um ou mais argumentos forem funções condicionais. Você pode usar <code>if(condition, result_if_true)</code> para avaliar uma condição e <code>elif(condition, result_if_true, result_if_false)</code> para avaliar condições adicionais. Por exemplo, você pode usar <code>if(condition1, result1_if_true).elif(condition2, result2_if_true, result2_if_false)</code>, em vez de <code>if(condition1, result1_if_true, if(condition2, result2_if_true, result2_if_false))</code>.

Função	Descrição
	Você também pode encadear funções condicionais intermediárias adicionais. Por exemplo, você pode usar <code>if(condition1, result1_if_true).elif(condition2, result2_if_true).elif(condition3, result3_if_true, result3_if_false)</code> em vez de aninhar várias instruções <code>if</code>, como <code>if(condition1, result1_if_true, if(condition2, result2_if_true, if(condition3, result3_if_true, result3_if_false)))</code>.
	 Important Você deve usar <code>elif(condition, result_if_true, result_if_false)</code> com UFCS.

Usar funções de string em expressões de fórmula

Em [transformações](#) e [métricas](#), você pode usar as seguintes funções para operar em cadeias de caracteres: Para obter mais informações, consulte [Usar strings 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 obter mais informações, consulte [Valores indefinidos, infinitos e excedidos](#).

Função	Descrição
<code>len(s)</code>	Retorna o tamanho da string <code>s</code> .
<code>find(s, substring)</code>	Retorna o índice da string <code>substring</code> na string <code>s</code> .
<code>contains(s, substring)</code>	Retorna 1 se a string <code>s</code> contiver a string <code>substring</code> , caso contrário, 0.
<code>upper(s)</code>	Retorna a string <code>s</code> em maiúsculas.
<code>lower(s)</code>	Retorna a string <code>s</code> em minúsculas.
<code>jp(s, json_path)</code>	Avalia a string <code>s</code> com a JsonPath expressão <code>json_path</code> 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 <code>jp('111', '\$')</code> 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 <code>jp</code>. A função externa <code>jp</code> extrai a string da estrutura JSON e a função interna <code>jp</code> converte a string em um número. A string <code>json_path</code> deve conter uma literal de string. Isso significa que <code>json_path</code> não pode ser uma expressão avaliada como uma string.

Função	Descrição
	Example Exemplos • <code>jp('{ "status": "active", "value": 15 }', '\$.value')</code> Retorna 15. • <code>jp('{ "measurement": { "reading": 25, "confidence": 0.95 } }', '\$.measurement.reading')</code> Retorna 25. • <code>jp('[2, 8, 23]', '\$[2]')</code> Retorna 23. • <code>jp('{ "values": [3, 6, 7] }', '\$.values[1]')</code> Retorna 6. • <code>jp('111', '\$')</code> Retorna 111. • <code>jp(jp('{ "measurement": { "reading": 25, "confidence": "0.95" } }', '\$.measurement.confidence'), '\$')</code> Retorna 0.95.
<code>join(s0, s1, s2, s3, ...)</code>	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: • <code>join("-", "aa", "bb", "cc")</code> retorna aa-bb-cc

Função	Descrição
<code>format(expression: "format")</code> ou <code>format("format", expression)</code>	Retorna uma string no formato especificado. Essa função valia <code>expression</code> 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 • <code>format(100+1: "d")</code> retorna uma string, 101. • <code>format("The result is %d", 100+1)</code> 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 literals 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') .

Usar funções de agregação em expressões de fórmula

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](#), [literals 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, $\text{avg}(x \cdot (x-1))$ e $\text{sum}(x/2) / \text{avg}(y^2)$ são suportadas.

Por exemplo, $\text{min}(x/y)$ não é suportada.

- Cada argumento pode ter expressões aninhadas de vários níveis.

Example

Por exemplo, $\text{sum}(\text{avg}(x^2)/2)$ é suportada.

- Argumentos diferentes podem ter variáveis diferentes.

Example

Por exemplo, $\text{sum}(x/2, y^2)$ 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
$\text{avg}(x_0, \dots, x_n)$	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
$\text{sum}(x_0, \dots, x_n)$	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.
$\text{min}(x_0, \dots, x_n)$	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.
$\text{max}(x_0, \dots, x_n)$	Retorna o valor máximo 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.
$\text{count}(x_0, \dots, x_n)$	Retorna o número total de pontos de dados das variáveis fornecidas ao longo do intervalo de tempo atual. Para obter mais informações sobre como contar o número de pontos de dados que atendem a uma condição, consulte Contar pontos de dados que correspondem a uma condição. Esta função calcula um ponto de dados para cada intervalo de tempo.

Função	Descrição
<code>stdev($x_0, \dots, x_n$)</code>	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.

Usar funções temporais em expressões de fórmula

Use funções temporais para retornar valores com base em carimbos de data/hora dos pontos de dados.

Usar 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
<code>first(x)</code>	Retorna o valor da variável fornecida com o primeiro a função de hora ao longo do intervalo de tempo atual.
<code>last(x)</code>	Retorna o valor da variável fornecida com o a função de hora mais recente ao longo do intervalo de tempo atual.
<code>earliest(x)</code>	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-definition.
<code>latest(x)</code>	Retorna o último valor da variável fornecida com o último carimbo de data/hora antes do fim 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-definition.
<code>statetime(x)</code>	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 <code>statetime</code> consumir. Por exemplo, se tiver uma propriedade <code>Idle</code> que seja 0 ou 1, você poderá calcular o

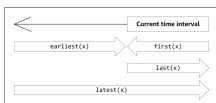
Função	Descrição
	tempo ocioso por intervalo de tempo com esta expressão: <code>IdleTime = statetime (Idle)</code> . Para obter mais informações, consulte o exemplo de cenário de statetime. Essa função não é compatível com as propriedades de métrica como variáveis de entrada. Se a propriedade de entrada tiver pelo menos um ponto de dados em seu histórico, esta função calcula um ponto de dados para cada intervalo de tempo.

Função	Descrição
<code>TimeWeightedAvg(x, [interpolation])</code>	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 <code>interpolation</code> deve ser uma constante de string: • <code>locf</code> – 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. • <code>linear</code> — 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
<code>TimeWeightedStDev(x, [algo])</code>	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 <code>algo</code> deve ser uma constante de string: • <code>f</code> – esse é o padrão. Ele retorna uma variância de amostra ponderada imparcial com pesos de frequência, onde <code>TimeWeight</code> 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. • <code>p</code> — 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`, `latest`, 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 obter 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 qualidade GOOD.

03:00:00	4,0
03:01:00	2,0
03:01:10	8.0

03:01:50	20.0
03:02:00	14.0
03:02:05	10.0
03:02:10	3.0
03:02:30	20.0
03:03:30	0.0

Saída de resultados agregados:

 **Note**
Nenhum — resultado não produzido para esta janela.

Tempo	Avg(x)	TimeWeigh tedAvg(x)	TimeWeigh tedAvg(X, "linear")	stDev(X)	timeWeigh tedStDev(x)	timeWeigh tedStDev(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	5.4306100 41581775	5.3851648 07134504
3:03:00	11	13	12.875	8.5440037 4531753	7.7240544 37220943	7.6594168 62050705
3:04:00	0	10	2,5	0	10.084389 681792215	10
3:05:00	Nenhum	0	0	Nenhum	0	0

Usar 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 [Usar funções condicionais em expressões de fórmula](#) 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 tem 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	
$z = x + y$ + <code>pretrigger</code> <code>r(y)</code>	y não recebe nenhum ponto de dados antes das 09:00. Portanto, z não é calculado às 09:00.	$23 = 20 + 2 + 1$ <code>pretrigger</code> <code>r(y)</code> é igual a 1.	$25 = 20 + 3 + 2$ x não recebe um novo ponto de dados. <code>pretrigger</code> <code>r(y)</code> é igual a 2.	$36 = 30 + 3 + 3$ y não recebe um novo ponto de dados. Portanto, <code>pretrigger</code> <code>r(y)</code> é igual a 3 às 09:15.

Usar 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.
- Estructure 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
<code>now()</code>	Retorna a data e a hora atuais, em segundos, no formato Unix epoch.
<code>timestamp()</code>	• 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 <code>timestamp</code> (<i>variable-name</i>) 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 <code>Temperature_F</code> que use a fórmula $9/5 * \text{Temperature\_C}$ para converter cada ponto de dados de temperatura de Celsius para Fahrenheit, você pode usar a função <code>timestamp(Temperature_F)</code> para obter a função de hora do valor de qualidade mais recente GOOD da propriedade de <code>Temperature_F</code>. • Use a função <code>pretrigger()</code> como argumento para a função. A função <code>timestamp(pretrigger(<i>variable-name</i>))</code> 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 obter mais informações, consulte Usar 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
<code>mktime(time_zone, year, month, day_of_month, hour, minute, second)</code>	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 especificado, 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: • <code>year</code> - valores válidos estão entre 1970 e 2250. • <code>month</code> - valores válidos estão entre 1 e 12. • <code>day-of-month</code> - valores válidos estão entre 1 e 31. • <code>hour</code> - valores válidos estão entre 0 e 23. • <code>minute</code> - valores válidos estão entre 0 e 59. • <code>second</code> - valores válidos estão entre 0 e 60. Ele pode ser um número de ponto flutuante. Exemplos: • <code>mktime(2020, 2, 29)</code>

Função	Descrição
	• <code>mktime('UTC+3', 2021, 12, 31, 22)</code> • <code>mktime(2022, 10, 13, 2, 55, 13.68, 'PST')</code>

Função	Descrição
<code>localtime(unix_time, time_zone)</code>	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 especificado, o fuso horário padrão será UTC. • O argumento Unix time é a hora em segundos, no formato Unix epoch. O intervalo válido é entre 1-31556889864403199. Ele pode ser um número de ponto flutuante. Exemplo de resposta: 2007-12-03T10:15:30+01:00[Europe/Paris] <code>localtime(unix_time, time_zone)</code> não é uma função independente. As funções <code>year()</code>, <code>mon()</code>, <code>mday</code>, <code>wday()</code>, <code>yday()</code>, <code>hour()</code>, <code>minute()</code> e <code>sec()</code> usam <code>localtime(unix_time, time_zone)</code> como argumento. Exemplos: • <code>year(localtime('GMT', 1605898608.8113723))</code> • <code>now().localtime().year()</code> • <code>timestamp().localtime('PST').year()</code>

Função	Descrição
	<code>localtime(1605289736, 'Europe/London').year()</code>
<code>year(localtime(unix_time, time_zone))</code>	Retorna o ano de <code>localtime(unix_time, time_zone)</code> .
<code>mon(localtime(unix_time, time_zone))</code>	Retorna o mês a partir de <code>localtime(unix_time, time_zone)</code> .
<code>mday(localtime(unix_time, time_zone))</code>	Retorna o dia do mês a partir de <code>localtime(unix_time, time_zone)</code> .
<code>wday(localtime(unix_time, time_zone))</code>	Retorna o dia da semana a partir de <code>localtime(unix_time, time_zone)</code> .
<code>yday(localtime(unix_time, time_zone))</code>	Retorna o dia do ano a partir de <code>localtime(unix_time, time_zone)</code> .
<code>hour(localtime(unix_time, time_zone))</code>	Retorna a hora a partir de <code>localtime(unix_time, time_zone)</code> .
<code>minute(localtime(unix_time, time_zone))</code>	Retorna o minuto a partir de <code>localtime(unix_time, time_zone)</code> .
<code>sec(localtime(unix_time, time_zone))</code>	Retorna o segundo a partir de <code>localtime(unix_time, time_zone)</code> .

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').
- Deslocamento IDs - 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.
- Com base na região IDs - Por exemplo, 'Etc/GMT+12' 'Pacific/Pago_Pago' e.

Abreviações de fuso horário compatíveis

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 - _Aires America/Argentina/Buenos
- 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 - Asia/Shanghai
- EAT - África/Addis_Ababa
- DIETA - America/Indiana/Indianapolis
- 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

Com base na região suportada IDs

As funções de data e hora oferecem suporte às seguintes funções baseadas em região IDs, organizadas 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/ HST1 0 (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/ YST9 (UTC- 09:00)
- 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/ PST8 (UTC- 08:00)
- América/Nome (UTC - 08:00)
- Sistema V/ YST9 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)
- PST8PDT (UTC- 07:00)
- Sistema V/ MST7 (UTC- 07:00)
- América/Dawson (UTC - 07:00)
- México/ BajaNorte (UTC- 07:00)
- América/Tijuana (UTC - 07:00)
- América/Creston (UTC - 07:00)
- América/Hermosillo (UTC - 07:00)
- América/Santa_Isabel (UTC - 07:00)
- América/Vancouver (UTC - 07:00)
- América/Ensenada (UTC - 07:00)
- América/Phoenix (UTC - 07:00)
- América/Whitehorse (UTC - 07:00)
- América/Fort_Nelson (UTC - 07:00)
- Sistema V/ PST8 PDT (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)
- MST7MDT (UTC- 06:00)
- Sistema V/ CST6 (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/ MST7 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)
- America/Indiana/Knox(UTC- 05:00)
- America/North_Dakota/Beulah(UTC- 05:00)
- América/Monterrey (UTC - 05:00)
- América/Jamaica (UTC - 05:00)
- América/Atikokan (UTC - 05:00)
- América/Coral_Harbour (UTC - 05:00)
- America/North_Dakota/Center(UTC- 05:00)
- América/Cayman (UTC - 05:00)
- America/Indiana/Tell_Cidade (UTC- 05:00)
- América/Cidade do México (UTC- 05:00)
- América/Matamoros (UTC - 05:00)
- CST6CDT (UTC- 05:00)
- América/Knox_IN (UTC - 05:00)
- América/Bogotá (UTC - 05:00)
- América/Menominee (UTC - 05:00)
- América/Resolute (UTC - 05:00)
- Sistema V/ EST5 (UTC- 05:00)
- Canadá/Central (UTC-05:00)
- Brasil/Acre (UTC - 05:00)

- América/Cancún (UTC - 05:00)
- América/Lima (UTC - 05:00)
- América/Bahia_Banderas (UTC - 05:00)
- US/Indiana-Starke (UTC - 05:00)
- América/Rio_Branco (UTC - 05:00)
- Sistema V/ CST6 CDT (UTC- 05:00)
- Jamaica (UTC - 05:00)
- América/Mérida (UTC - 05:00)
- America/North_Dakota/New_Salem (UTC- 05:00)
- América/Winnipeg (UTC - 05:00)
- América/Cuiabá (UTC - 04:00)
- América/Marigot (UTC - 04:00)
- America/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/ AST4 (UTC- 04:00)
- America/Indiana/Vevay(UTC- 04:00)
- America/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)
- America/Kentucky/Louisville(UTC- 04:00)
- América/Dominica (UTC - 04:00)
- América/Assunção (UTC - 04:00)
- EST5EDT (UTC- 04:00)
- América/Nassau (UTC - 04:00)
- America/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)
- America/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/ Port-au-Prince (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)
- America/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/ EST5 EDT (UTC- 04:00)
- America/Argentina/Catamarca(UTC- 03:00)
- Canadá/Atlântico (UTC - 03:00)
- America/Argentina/Cordoba(UTC- 03:00)
- América/Araguaina (UTC - 03:00)
- America/Argentina/Salta(UTC- 03:00)
- ETC/GMT+3 (UTC - 03:00)
- América/Montevidéu (UTC - 03:00)
- Brasil/Leste (UTC - 03:00)
- America/Argentina/Mendoza(UTC- 03:00)

- America/Argentina/Rio_Gallegos (UTC- 03:00)
- América/Catamarca (UTC - 03:00)
- América/Córdoba (UTC - 03:00)
- América/São Paulo (UTC - 03:00)
- America/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)
- America/Argentina/San_Luis (UTC- 03:00)
- America/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)
- America/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)

- America/Argentina/San_Juan (UTC- 03:00)
- America/Argentina/ComodRivadavia(UTC- 03:00)
- America/Argentina/Tucuman(UTC- 03:00)
- América/Rosário (UTC - 03:00)
- Sistema V/ AST4 ADT (UTC- 03:00)
- America/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/Fakaofu (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/Srednekolymk (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/Volgogrado (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/Moscú (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/Ljubliana (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

- [Usar strings em fórmulas](#)
- [Filtrar pontos de dados](#)
- [Contar pontos de dados que correspondem a uma condição](#)
- [Dados atrasados em fórmulas](#)
- [Qualidade de dados em fórmulas](#)

- [Valores indefinidos, infinitos e excedidos](#)

Usar strings 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 obter 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 função `jp` capaz de analisar objetos JSON serializados e converter strings em números

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.

Contar pontos de dados que correspondem 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 $x / \sqrt{-1}$, ou $\log(0)$) 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.
- $\text{sqrt}(-1)$ 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.

Criar modelos compostos personalizados (componentes)

Os modelos compostos personalizados, ou componentes se você estiver usando o console, oferecem outro nível de organização para os modelos de ativo e modelos de componente. Você pode usá-los para estruturar os modelos, agrupando propriedades ou fazendo referência a outros modelos. Para ter mais informações sobre como trabalhar com modelos compostos personalizados, consulte [Modelos compostos personalizados \(componentes\)](#).

Crie 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 dentro de 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 component-model-based personalizado.

As seções a seguir descrevem como usar a AWS IoT SiteWise API para criar modelos compostos personalizados.

Tópicos

- [Criar um componente em linha \(console\)](#)

- [Criar um modelo composto personalizado em linha \(AWS CLI\)](#)
- [Criar um component-model-based componente \(console\)](#)
- [Crie um modelo composto component-model-based personalizado \(AWS CLI\)](#)

Criar um componente em linha (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 em linha, essas propriedades só se aplicam 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 ativo ou para incluir várias instâncias em um modelo de ativo), crie um componente com base em um modelo de componente. Para conferir detalhes, consulte a seção a seguir.

Como 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 entre todos os componentes da conta nessa região.
 - b. (Opcional) Adicione Definições de atributo ao modelo. Os atributos representam informações que raramente mudam. Para obter mais informações, consulte [Definir dados estáticos \(atributos\)](#).
 - c. (Opcional) Adicione Definições de medição ao modelo. As medições representam fluxos de dados do seu equipamento. Para obter mais informações, consulte [Definir fluxos de dados de equipamentos \(medições\)](#).

- d. (Opcional) Adicione Definições de transformação ao modelo. As transformações são fórmulas que mapeiam dados de um formulário para outro. Para obter mais informações, consulte [Transformar 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 obter mais informações, consulte [Agregação de dados de propriedades e outros ativos \(métricas\)](#).
- f. Escolha Criar componente.

Criar 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 [CreateAssetModelCompositeModel](#) operação para criar um modelo em linha com propriedades. Essa operação espera uma carga útil com a seguinte estrutura.

Note

Como trata-se de um componente composto em linha, essas propriedades só se aplicam ao modelo de ativo atual, e não são compartilhadas em nenhum outro lugar. O que faz dele “em linha” é que ele não fornece um valor para o campo `composedAssetModelId`.

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 `component-model-based` composto. Para conferir detalhes, consulte a seção a seguir.

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

Criar 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 entre todos os componentes da conta nessa região.
 - c. Escolha Criar componente.

Crie 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 [CreateAssetModelCompositeModel](#) operação 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 o ID ou o ID externo do modelo de ativo de um modelo de componente existente. Consulte mais informações em [Objetos de referência com objetos externos IDs](#) no Guia de Usuário AWS IoT SiteWise . Para conferir um exemplo de como criar um modelo de componente, consulte [Criar 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 aninhar componentes dentro de 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.

Crie ativos para modelos de ativos em AWS IoT SiteWise

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 [Crie modelos de ativos em AWS IoT SiteWise](#).

 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 obter mais informações, consulte [Estados de ativos e modelos](#).

Tópicos

- [Criar um ativo \(console\)](#)
- [Criar um ativo \(AWS CLI\)](#)
- [Configurar um novo ativo](#)

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 obter mais informações, consulte [Marque seus AWS IoT SiteWise recursos](#).
- 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 obter mais informações, consulte [Estados de ativos e modelos](#).

Depois de criar um ativo, consulte [Configurar um novo ativo](#).

Criar 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 ativos, mas não o `conheceassetModelId`, use a [ListAssetModels](#) API para visualizar todos os seus modelos de ativos.

Para criar um ativo a partir de um modelo de ativo, use a [CreateAsset](#) API com os seguintes parâmetros:

- `assetName` – o nome do novo ativo. Dê um nome ao ativo para ajudar a identificá-lo.
- `assetModelId` – O ID do ativo. Esse é o ID real no formato UUID, ou `externalId:myExternalId` se ele tiver um. Consulte mais informações em [Objetos de referência com objetos externos IDs](#) no Guia de Usuário AWS IoT SiteWise .

Como criar um ativo (AWS CLI)

- Execute o seguinte comando para criar um ativo. *asset-name* Substitua 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 [DescribeAsset](#) operação 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 obter mais informações, consulte [Estados de ativos e modelos](#).

Depois de criar um ativo, consulte [Configurar um novo ativo](#).

Configurar um novo ativo

Depois de criar um ativo em AWS IoT SiteWise, há várias próximas etapas que você pode seguir para utilizar totalmente o ativo e seus dados. Essas etapas podem incluir a configuração de fluxos de dados para ingerir dados do ativo, a configuração de alarmes e notificações para monitorar o desempenho do ativo, a criação de visualizações e painéis para exibir os dados do ativo e a integração do ativo com outros AWS serviços ou aplicativos de terceiros para análise ou automação adicionais.

Conclua a configuração do seu ativo com as seguintes ações opcionais:

- [Gerencie fluxos de dados para AWS IoT SiteWise](#) 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.

Pesquise ativos em Console do AWS IoT SiteWise

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 [ExecuteQuery](#) API. Se você não concedeu permissões e precisa de ajuda para AWS IoT SiteWise começar, consulte [Integre AWS IoT SiteWise e 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 o nome completo de um ativo ou um nome parcial para uma pesquisa ampla.
 - b. Nome da propriedade: insira o nome completo de uma propriedade ou um nome parcial para uma pesquisa ampla.
 - c. Operador: escolha um dos seguintes operadores:
 - =
 - <
 - >
 - <=
 - >=

- d. Valor da propriedade: este 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 Resultados da pesquisa, escolha o ativo na coluna Nome. Isso leva você para a página detalhada do ativo em questão.

The screenshot shows the AWS IoT SiteWise console interface. At the top, there's a navigation bar with the AWS logo, 'Services', a search bar, and a region dropdown set to 'N. Virginia'. Below this, the 'Assets' page is displayed. The page title is 'Assets', and there's a 'Create asset' button. A description states: 'Assets represent Industrial devices and processes that send data streams to SiteWise. Models are structures that enforce a specific model of properties and hierarchies for all instances of each asset. You must create every asset from a model.'

The 'Advanced search' section is active, showing a 'Metadata search' tab. The search criteria are as follows:

Asset name	Property name	Operator	Property value	Property value type
Level-2	power_max	>	20	Double

Below the search criteria, there are 'Clear' and 'Search' buttons. The 'Search results (2)' section shows a table with two results:

Name	Asset Id	Description
Level-2-asset-1	d0e9019b-9c38-4316-b574-38317aa38143	
Level-2-asset-2	b9c0d2fc-1527-42ce-8ba2-d1a4e8ff43de	Example description

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 apenas no campo Nome do ativo.
- Os campos Nome da propriedade e Valor da propriedade permanecem vazios.
- Encontre ativos que contêm propriedades com um nome específico:
 - Insira um valor apenas no campo Nome da propriedade.
 - Os campos Nome do ativo e Valor da propriedade permanecem vazios.
- Encontre ativos com base nos valores mais recentes das propriedades:
 - Insira valores nos campos Nome da propriedade e Valor da propriedade.
 - Selecione um Operador e Tipo de valor da propriedade.

Pesquisa do construtor de consultas

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 Construtor de consultas.
4. No painel Construtor de consultas, escreva a consulta SQL para recuperar `asset_name`, `asset_id` e `asset_description`.
5. Selecione a opção Pesquisar.
6. Na tabela Resultados da pesquisa, escolha o ativo na coluna Nome. Isso leva você para a página detalhada do ativo em questão.

The screenshot shows the AWS IoT SiteWise 'Assets' page. At the top, there's a navigation bar with the AWS logo, 'Services', a search bar, and a region dropdown set to 'N. Virginia'. Below the navigation bar, the page title 'Assets' is displayed with a 'Create asset' button. A descriptive paragraph explains that assets represent industrial devices and processes. The 'Advanced search' section is active, showing a 'Query builder' tab. The query entered is: `SELECT a.asset_id, a.asset_name, a.asset_description FROM asset a, asset_property p, latest_value_time_series ts WHERE a.asset_name LIKE '%asset-2%' AND a.property_name = 'temperature_f' AND ts.double_value > 50.0`. Below the query, there are 'Clear' and 'Search' buttons. The search results are displayed in a table with 2 results. The table has columns for Name, Asset Id, and Description. The results are: 'Level-2a-asset-2' with Asset Id '4fed596d-e903-4338-86db-34ca9301233a' and Description 'Generator #3'; and 'Level-2b-asset-2' with Asset Id 'b4ac2b24-4fce-4a72-9fea-ef6d0f741e8d' and Description 'Generator #2'.

Assets

Assets represent Industrial devices and processes that send data streams to SiteWise. Models are structures that enforce a specific model of properties and hierarchies for all instances of each asset. You must create every asset from a model.

Advanced search

Use advanced search to find assets based on specific metadata. In addition, you can enter SQL queries directly in the query builder.

Metadata search Query builder

Query builder

```
SELECT a.asset_id, a.asset_name, a.asset_description
FROM asset a, asset_property p, latest_value_time_series ts
WHERE a.asset_name LIKE '%asset-2%' AND a.property_name = 'temperature_f' AND ts.double_value > 50.0
```

Clear Search

Search results (2)

Name	Asset Id	Description
Level-2a-asset-2	4fed596d-e903-4338-86db-34ca9301233a	Generator #3
Level-2b-asset-2	b4ac2b24-4fce-4a72-9fea-ef6d0f741e8d	Generator #2

Note

- A cláusula SELECT na consulta SQL deve incluir os campos `asset_name` e `asset_id` para garantir um ativo válido na tabela Resultados da pesquisa.
- O Construtor de consultas só exibe o Nome, o ID do ativo e a Descrição na tabela de resultados. A adição de mais campos à cláusula SELECT não adiciona mais colunas à tabela de resultados.

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.

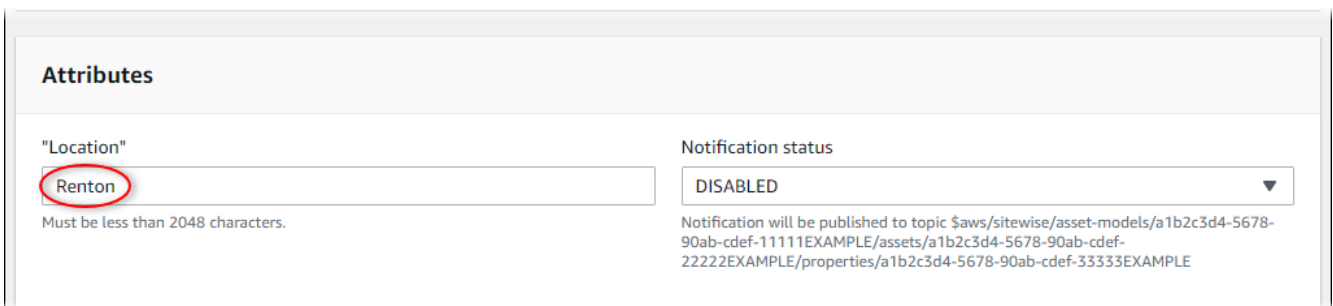
Como atualizar o valor de um atributo (console)

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. Escolha Editar.
5. Localize o atributo a ser atualizado e insira seu novo valor.



The screenshot shows the 'Attributes' section of the AWS IoT SiteWise console. It features a table with two columns: 'Attribute' and 'Value'. The 'Location' attribute is highlighted with a red circle, and its value is 'Renton'. Below the attribute name, it says 'Must be less than 2048 characters.' To the right, the 'Notification status' is set to 'DISABLED' in a dropdown menu. Below the dropdown, there is a notification message: 'Notification will be published to topic \$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/assets/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE/properties/a1b2c3d4-5678-90ab-cdef-33333EXAMPLE'.

6. Escolha 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 `conneassetId`, use a [ListAssets](#) API para listar todos os ativos de um modelo específico. Use a [DescribeAsset](#) operação para visualizar as propriedades do seu ativo, incluindo propriedades IDs.

Use a operação [BatchPutAssetPropertyValue](#) para atribuir valores de atributo ao 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.

Como 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 os IDs valores e os carimbos de data/hora para modificar a carga útil do seu caso de uso.

```
{
  "entries": [
    {
      "entryId": "windfarm3-turbine7-latitude",
      "assetId": "a1b2c3d4-5678-90ab-cdef-2222EXAMPLE",
      "propertyId": "a1b2c3d4-5678-90ab-cdef-3333EXAMPLE",
      "propertyValues": [
        {
          "value": {
            "doubleValue": 47.6204
          },
          "timestamp": {
            "timeInSeconds": 1575691200
          }
        }
      ]
    },
    {
      "entryId": "windfarm3-turbine7-longitude",
      "assetId": "a1b2c3d4-5678-90ab-cdef-2222EXAMPLE",
      "propertyId": "a1b2c3d4-5678-90ab-cdef-5555EXAMPLE",
      "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`
 - `nullValue`
 - `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 útil para [BatchPutAssetPropertyValue](#), consulte [Injira dados com AWS IoT SiteWise APIs](#).

2. Execute o seguinte comando para enviar os valores de atributo ao 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 [Definir hierarquias de modelos de ativo](#).

Tópicos

- [Associar e desassociar ativos \(console\)](#)
- [Associar e desassociar ativos \(AWS CLI\)](#)

Associar e desassociar ativos (console)

Você pode usar o AWS IoT SiteWise console para associar e desassociar ativos.

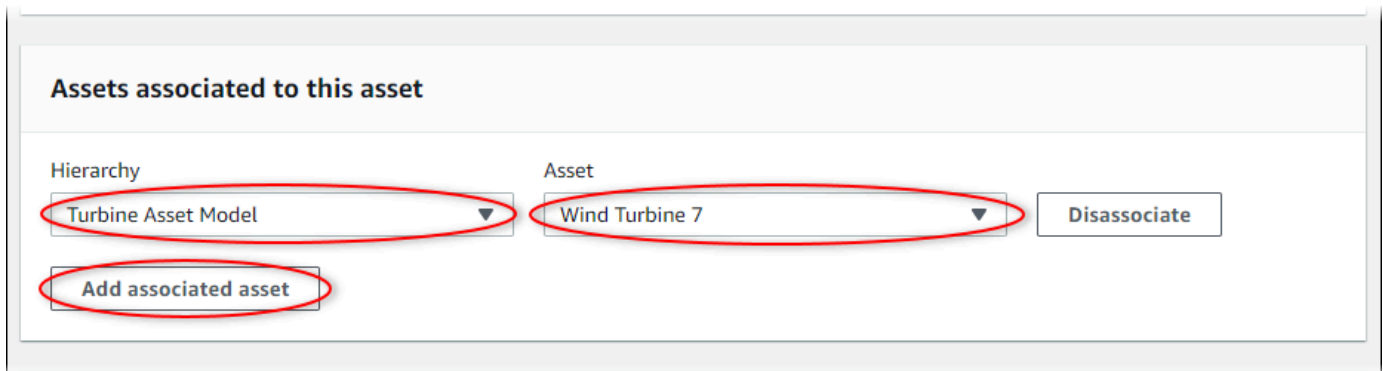
Como associar um ativo (console)

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. Escolha 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. Escolha Salvar.

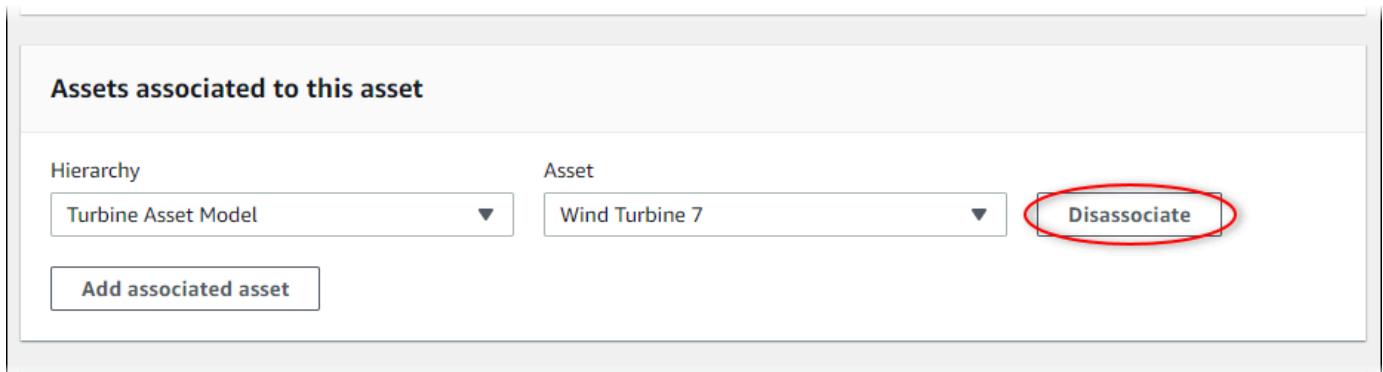
Como desassociar um ativo (console)

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. Escolha Editar.
5. Em Ativos associados a este ativo, escolha Desassociar para o ativo.



6. Escolha Salvar.

Associar e desassociar 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 [DescribeAsset](#) operação para encontrar o ID da hierarquia na resposta.

Como localizar um ID de hierarquia

- Execute o seguinte comando para descrever o ativo pai. *parent-asset-id* Substitua 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 lista de `assetHierarchies` que tem 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 [AssociateAssets](#) operação. Para desassociar um ativo secundário de um ativo principal, use a [DisassociateAssets](#) operação. Especifique os seguintes parâmetros, que são os mesmos para as duas operações:

- `assetId`: o ID ou o ID externo do ativo pai.
- `hierarchyId`: o ID ou o ID externo da hierarquia no ativo pai.
- `childAssetId`: o ID ou o ID externo do ativo filho.

Como 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* pelo respectivo IDs:

```
aws iotsitewise associate-assets \
  --asset-id parent-asset-id \
  --hierarchy-id hierarchy-id \
  --child-asset-id child-asset-id
```

Como desassociar um ativo (AWS CLI)

- Execute o seguinte comando para desassociar um ativo filho de um ativo pai. Substitua *parent-asset-id* e *child-asset-id* pelo respectivo 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 do 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 em AWS IoT SiteWise](#)
- [Atualizar modelos de ativo e modelos de componente](#)
- [Atualizar modelos compostos personalizados \(componentes\)](#)
- [Bloqueio positivo para gravações do modelo de ativo](#)

Atualizar ativos em AWS IoT SiteWise

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 obter mais informações, consulte [Estados de ativos e modelos](#).

Tópicos

- [Atualizar um ativo \(console\)](#)
- [Atualizar 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. Escolha Editar.
5. Atualize o Nome do ativo.
6. (Opcional) Nessa página, atualize outras informações para o ativo. Para obter mais informações, consulte:
 - [Gerencie fluxos de dados para AWS IoT SiteWise](#)
 - [Atualizar valores de atributo](#)
 - [Interaja com outros AWS serviços](#)
7. Escolha Salvar.

Atualizar um ativo (AWS CLI)

Você pode usar o AWS Command Line Interface (AWS CLI) para atualizar o nome de um ativo.

Use a [UpdateAsset](#) operação 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. Consulte mais informações em [Objetos de referência com objetos externos IDs](#) no Guia de Usuário AWS IoT SiteWise .
- `assetName` – o novo nome do ativo.

Como atualizar o nome de um ativo (AWS CLI)

- Execute o seguinte comando para atualizar o nome de um ativo. *asset-id* Substitua pelo ID ou ID externo do ativo. Atualize o *asset-name* com o novo nome do ativo.

```
aws iotsitewise update-asset \  
  --asset-id asset-id \  
  --asset-name asset-name
```

Atualizar modelos de ativo e modelos de componente

Use o AWS IoT SiteWise console ou a API para atualizar um modelo de ativo ou modelo de componente.

Não é possível alterar o tipo de uma propriedade existente ou o respectivo tipo de dado, ou ainda a janela de uma métrica existente. Você também não pode alterar o tipo 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 componente, isso afeta todos os modelos de ativo que usam esse modelo de componente, por isso tome muito cuidado e entenda até que ponto a 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, todo modelo de ativo que incorpora esse modelo de componente reflete as alterações. Até que as alterações do modelo de componente se propaguem, cada modelo de ativo afetado tem o estado UPDATING, seguido de PROPAGATING à

medida que ele atualiza os ativos associados, conforme descrito no parágrafo anterior. Aguarde até que esses modelos de ativo retornem ao estado ACTIVE para interagir com eles. Durante esse período, o status do modelo de componente atualizado será PROPAGATING.

Para obter mais informações, consulte [Estados de ativos e modelos](#).

Tópicos

- [Atualizar um modelo de ativo ou de componente \(console\)](#)
- [Atualizar um modelo de ativo ou de componente \(AWS CLI\)](#)

Atualizar um modelo de ativo ou de componente (console)

Você pode usar o AWS IoT SiteWise console para atualizar um modelo de ativo ou modelo de componente.

Como atualizar um modelo de ativo ou um modelo de componente (console)

1. Navegue até o [console do AWS IoT SiteWise](#).
2. No painel de navegação, selecione Modelos.
3. Escolha o modelo de ativo ou o modelo de componente a ser atualizado.
4. Escolha 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 obter mais informações, consulte [Definir dados estáticos \(atributos\)](#).
 - Altere qualquer uma das Definições de medição. Não é possível alterar o Tipo de dados das medições existentes. Para obter mais informações, consulte [Definir fluxos de dados de equipamentos \(medições\)](#).
 - Altere qualquer uma das Definições de transformação. Para obter mais informações, consulte [Transformar dados \(transformações\)](#).
 - Altere qualquer uma das Definições de métrica. Não é possível alterar o Intervalo de tempo das métricas existentes. Para obter mais informações, consulte [Agregar dados de propriedades e outros ativos \(métricas\)](#).

- (Somente modelos de ativo) Altere qualquer uma das Definições da hierarquia. Não é possível alterar o Modelo de hierarquia das hierarquias existentes. Para obter mais informações, consulte [Definir hierarquias de modelos de ativo](#).

6. Escolha Salvar.

Note

As solicitações de atualização feitas no console serão rejeitadas se outro usuário atualizar com êxito o modelo de ativo desde a última vez em que você abriu a página Editar modelo. O console solicita que o usuário clique em Atualizar na página Editar modelo para buscar o modelo atualizado. Você deve fazer as atualizações novamente e tentar salvar mais uma vez. Consulte [Bloqueio positivo para gravações do modelo de ativo](#) para obter mais detalhes.

Atualizar um modelo de ativo ou de componente (AWS CLI)

Use o AWS Command Line Interface (AWS CLI) para atualizar um modelo de ativo ou modelo de componente.

Use a [UpdateAssetModel](#) API para atualizar o nome, a descrição e as propriedades de um modelo de ativo ou modelo de componente. Somente para modelos de ativo, você pode atualizar as 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. Consulte mais informações em [Objetos de referência com objetos externos IDs](#) 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 de um modelo de componente, consulte [Crie modelos de ativos em AWS IoT SiteWise](#).

Warning

A [UpdateAssetModel](#) API substitui o modelo existente pelo modelo que você fornece na carga. Para evitar a exclusão das propriedades ou hierarquias do seu modelo, você deve

incluir suas definições IDs e suas na carga útil atualizada do modelo. Para saber como consultar a estrutura existente do seu modelo, consulte a [DescribeAssetModel](#) operação.

 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 obter mais informações, consulte [Atualizar modelos compostos personalizados \(componentes\)](#).

Como atualizar um modelo de ativo ou um modelo de componente (AWS CLI)

1. Execute o comando a seguir para recuperar a definição do modelo existente. *asset-model-id* Substitua 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
```

O comando acima retorna a definição do modelo correspondente à versão mais recente do modelo.

Para um caso de uso em que um modelo de ativo está em um estado FAILED, recupere a definição de modelo válida correspondente à versão ativa para criar a solicitação de atualização. Para mais detalhes, consulte [Versões do modelo de ativo](#). Execute o seguinte comando para recuperar a definição de modelo válida:

```
aws iotsitewise describe-asset-model --asset-model-id asset-model-id --asset-model-version ACTIVE
```

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"
},
"assetModelVersion": "String",
"eTag": "String"
}
```

Para obter mais informações, consulte a operação [DescribeAssetModel](#).

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`
 - `assetModelVersion`
 - `eTag`

A [UpdateAssetModel](#) operação 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 obter 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 obter mais informações, consulte [Definir hierarquias de modelos de ativo](#).
- 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 [Monitore dados com alarmes em AWS IoT SiteWise](#) e [Defina alarmes em modelos de ativos em AWS IoT SiteWise](#).

5. Execute o seguinte comando para atualizar o modelo de ativo com a definição armazenada no `update-asset-model.json`. `asset-model-id` Substitua pelo ID do modelo de ativo:

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

Important

Quando vários usuários atualizam um modelo de ativo ao mesmo tempo, as alterações de um usuário podem ser inadvertidamente substituídas por outro. Para evitar isso, defina uma

solicitação de atualização condicional. Consulte [Bloqueio positivo para gravações do modelo de ativo](#).

Atualizar 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

- [Atualizar um componente \(console\)](#)
- [Atualizar um modelo composto personalizado \(AWS CLI\)](#)

Atualizar um componente (console)

Você pode usar o AWS IoT SiteWise console para atualizar um componente.

Como 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 no qual o componente está.
4. Na guia Propriedades, escolha Componentes.
5. Selecione o componente que você deseja atualizar.
6. Escolha Editar.
7. Na página Editar componente, faça uma das seguintes ações:
 - 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 obter mais informações, consulte [Definir dados estáticos \(atributos\)](#).
 - Altere qualquer uma das Definições de medição. Não é possível alterar o Tipo de dados das medições existentes. Para obter mais informações, consulte [Definir fluxos de dados de equipamentos \(medições\)](#).
 - Altere qualquer uma das Definições de transformação. Para obter mais informações, consulte [Transformar dados \(transformações\)](#).

- Altere qualquer uma das Definições de métrica. Não é possível alterar o Intervalo de tempo das métricas existentes. Para obter mais informações, consulte [Agregação de propriedades e outros ativos \(métricas\)](#).

8. Escolha Salvar.

Atualizar um modelo composto personalizado (AWS CLI)

Use o AWS Command Line Interface (AWS CLI) para atualizar um modelo composto personalizado.

Para atualizar o nome ou a descrição, use a [UpdateAssetModelCompositeModel](#) operação. 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. Não é possível alterar o tipo de uma propriedade existente ou o respectivo tipo de dado.

Para substituir uma propriedade de modelo composto existente por uma nova com o mesmo nome, faça o seguinte:

1. Envie uma solicitação `UpdateAssetModelCompositeModel` com toda a propriedade existente removida.
2. Envie uma segunda solicitação `UpdateAssetModelCompositeModel` que inclua a nova propriedade. A nova propriedade do ativo terá a mesma nome que a anterior e AWS IoT SiteWise gerará uma nova propriedade exclusiva `id`.

Como atualizar um modelo composto personalizado (AWS CLI)

1. Para recuperar a definição do modelo composto existente, execute o comando a seguir.
`composite-model-id` Substitua pela ID ou pela ID externa 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 o Guia do usuário do AWS IoT SiteWise .
 - a. Execute o comando abaixo:

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

- b. O comando acima retorna a definição do modelo composto correspondente à versão mais recente do modelo associado. Para um caso de uso em que um modelo de ativo está em um estado FAILED, recupere a definição de modelo válida correspondente à versão ativa para criar a solicitação de atualização. Para mais detalhes, consulte [Versões do modelo de ativo](#).
- c. Execute o seguinte comando para recuperar a definição de modelo válida:

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

- d. Para obter mais informações, consulte a operação [DescribeAssetModelCompositeModel](#).
2. Crie um arquivo chamado `update-custom-composite-model.json`, depois copie a resposta do comando anterior para o arquivo.
 3. Remova todos os pares de chave/valor do objeto JSON em `update-custom-composite-model.json`, exceto os 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 ou remova `assetModelCompositeModelDescription`, ou altere o 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`. *composite-model-id* Substitua 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
```

Important

Quando vários usuários atualizam um modelo de ativo ao mesmo tempo, as alterações de um usuário podem ser inadvertidamente substituídas por outro. Para evitar isso, defina uma solicitação de atualização condicional. Consulte [Bloqueio positivo para gravações do modelo de ativo](#).

Bloqueio positivo para gravações do modelo de ativo

Ao atualizar um modelo de ativo, o usuário faz o seguinte:

1. Lê a definição do modelo de ativo atual.
2. Edita a definição do modelo de ativo com as alterações necessárias.
3. Atualiza o modelo de ativo com a nova definição.

Em um cenário com dois usuários atualizando um modelo, pode acontecer o seguinte:

- O usuário A lê a definição do modelo de ativo X.
- O usuário B lê a definição do modelo de ativo X e confirma alterações, modificando a definição de X.
- O usuário A confirma alterações e substitui a alteração feita no modelo de ativo X pelo usuário B, sem verificar ou incorporar as alterações do usuário B.

O bloqueio otimista é um mecanismo usado AWS IoT SiteWise para evitar substituições acidentais, como no cenário acima. O bloqueio positivo é uma estratégia para garantir que a versão atual

do modelo de ativo que esteja sendo atualizada ou excluída seja igual à versão atual no AWS IoT SiteWise. Isso evita que gravações do modelo de ativo sejam substituídas por atualizações acidentais.

Siga estas etapas para realizar gravações do modelo de ativo com bloqueio positivo:

Tópicos

- [Realizar gravações do modelo de ativo com bloqueio positivo \(console\)](#)
- [Realizar gravações do modelo de ativo com bloqueio positivo \(AWS CLI\)](#)

Realizar gravações do modelo de ativo com bloqueio positivo (console)

O procedimento abaixo descreve como realizar gravações do modelo de ativo com um bloqueio positivo na versão ativa do modelo de ativo no console.

1. Navegue até o [console do AWS IoT SiteWise](#).
2. No painel de navegação, selecione Modelos.
3. Escolha o modelo de ativo ou o modelo de componente a ser atualizado.
4. Escolha Editar.
5. Faça alterações na página Editar modelo.
6. Escolha Salvar.

Note

Às vezes, pode ocorrer uma ou mais atualizações de modelo bem-sucedidas entre o momento em que o usuário começa a editar o modelo e o momento em que salva as edições feitas no modelo.

Para garantir que o usuário não substitua acidentalmente novas atualizações bem-sucedidas, a gravação do usuário é rejeitada. O console desabilita o botão Salvar e solicita que o usuário atualize a página Editar modelo. O usuário deve atualizar novamente a nova versão ativa do modelo. O usuário deve realizar as seguintes etapas adicionais:

7. Escolha Refresh.
8. Siga novamente as etapas 5 e 6.

Realizar gravações do modelo de ativo com bloqueio positivo (AWS CLI)

O procedimento abaixo descreve como realizar gravações do modelo de ativo com bloqueio positivo na AWS CLI.

1. Busque o ETag associado à definição do modelo atual

ETag é um token exclusivo gerado para cada nova representação de um modelo de ativo. Chame a [DescribeAssetModel](#) API para buscar a definição atual do modelo de ativo e a associada a ETag partir da resposta.

Durante atualizações simultâneas, os usuários realizam atualizações bem-sucedidas (modelo no estado ACTIVE) ou atualizações malsucedidas (modelo no estado FAILED). Para garantir que um usuário não substitua acidentalmente uma atualização bem-sucedida, você deve recuperar a versão ativa do modelo de ativo de [Versões do modelo de ativo](#) e encontrar o valor da ETag.

Execute o seguinte comando:

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

A resposta retorna a seguinte estrutura:

```
{
  "assetModelId": "String",
  "assetModelArn": "String",
  "assetModelName": "String",
  ...
  "eTag": "String"
}
```

Note

Você deve recuperar a versão mais recente do modelo de ativo e a respectiva ETag para não substituir nenhuma atualização.

2. Realizar operações UPDATE e DELETE com condições de gravação

O seguinte modelo de ativos APIs oferece suporte ao bloqueio otimista:

- [UpdateAssetModel](#)
- [DeleteAssetModel](#)
- [CreateAssetModelCompositeModel](#)
- [UpdateAssetModelCompositeModel](#)
- [DeleteAssetModelCompositeModel](#)

 Note

Os cenários abaixo usam a API `UpdateAssetModel` como referência. As condições se aplicam a todas as operações listadas acima.

Os cenários abaixo descrevem as diferentes condições de gravação, dependendo dos requisitos de controle da simultaneidade:

- Execute o comando a seguir para não substituir nenhuma atualização bem-sucedida. Não deve existir nenhuma nova versão ativa desde a última versão ativa lida. Substitua `e-tag` pela `ETag` retornada na operação de API usada na leitura da versão ativa.

```
aws iotsitewise update-asset-model \  
  --asset-model-id asset-model-id \  
  --if-match e-tag \  
  --match-for-version-type ACTIVE \  
  --cli-input-json file://model-payload.json
```

- Quando a criação de um modelo falha, ainda não existe uma versão ativa para ele, pois ele está em um estado `FAILED`. Ainda é possível substituir uma nova versão ativa que esteja presente, antes que as alterações sejam confirmadas. Execute o comando a seguir para não substituir uma nova versão ativa quando não existir uma versão ativa durante a leitura mais recente.

```
aws iotsitewise update-asset-model \  
  --asset-model-id asset-model-id \  
  --if-none-match "*" \  
  --match-for-version-type ACTIVE \  
  --cli-input-json file://model-payload.json
```

```
--cli-input-json file://model-payload.json
```

- Execute o comando a seguir para evitar a substituição de atualizações bem-sucedidas ou malsucedidas. Esse comando define uma condição de gravação que garante que uma versão mais recente não seja criada desde a última versão lida. Substitua e-tag pela ETag retornada na operação de API usada na leitura da versão ativa.

```
aws iotsitewise update-asset-model \  
  --asset-model-id asset-model-id \  
  --if-match eTag \  
  --match-for-version-type LATEST \  
  --cli-input-json file://model-payload.json
```

Se a condição de gravação for avaliada como FALSE, a solicitação de gravação falhará com `PreconditionFailedException`.

Exclua ativos e modelos em AWS IoT SiteWise

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 em AWS IoT SiteWise](#)
- [Excluir modelos de ativos em AWS IoT SiteWise](#)

Excluir ativos em AWS IoT SiteWise

Você pode usar o AWS IoT SiteWise console ou a API para excluir um ativo que não é mais necessário em seu ambiente. A exclusão de um modelo de ativo também exclui todos os ativos e modelos de componente associados. No entanto, é importante observar que a exclusão de um ativo ou modelo é uma ação permanente, e todos os dados associados aos recursos excluídos também são removidos. Antes de excluir ativos ou modelos, é recomendável revisar todas as dependências ou integrações que possam ser afetadas e garantir que haja um backup de todos os dados importantes.

Para excluir um ativo, primeiro você deve desassociar seus ativos filho e desassociá-lo do ativo pai. Para obter mais informações, consulte [Associar e desassociar ativos](#). Se você usar o AWS

Command Line Interface (AWS CLI), poderá usar a [ListAssociatedAssets](#) operação para listar os filhos de um ativo.

Ao excluir um ativo, seu status será DELETING até que as alterações sejam propagadas. Para obter 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 \(console\)](#)
- [Excluir um ativo \(AWS CLI\)](#)

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.

Excluir um ativo (AWS CLI)

Você pode usar o AWS Command Line Interface (AWS CLI) para excluir um ativo.

Use a [DeleteAsset](#) operação 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. Consulte mais informações em [Objetos de referência com objetos externos IDs](#) no Guia de Usuário AWS IoT SiteWise .

Como excluir um ativo (AWS CLI)

1. Execute o seguinte comando para listar as hierarquias do ativo. `asset-id` Substitua pela ID ou pela ID externa 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 lista de `assetHierarchies` que tem a seguinte estrutura:

```
{
  ...
  "assetHierarchies": [
    {
      "id": "String",
      "name": "String"
    }
  ],
  ...
}
```

Para obter mais informações, consulte a operação [DescribeAsset](#).

2. Para cada hierarquia, execute o seguinte comando para listar os filhos do ativo que estão associados a essa hierarquia. `asset-id` Substitua pela ID ou ID externa do ativo e `hierarchy-id` pela ID ou ID externa 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. *asset-id* Substitua pelo ID ou ID externo do ativo.

```
aws iotsitewise delete-asset --asset-id asset-id
```

Excluir modelos de ativos em AWS IoT SiteWise

Você pode usar o AWS IoT SiteWise console ou a API para excluir um modelo de ativo.

Para excluir um modelo de ativo, primeiro é necessário excluir todos os ativos criados por meio do modelo de ativo.

Ao excluir um modelo de ativo, seu status será DELETING até que as alterações sejam propagadas. Para obter 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 \(console\)](#)
- [Excluir 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 obter 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.

Excluir um modelo de ativo (AWS CLI)

Você pode usar o AWS Command Line Interface (AWS CLI) para excluir um modelo de ativo.

Use a [DeleteAssetModel](#) operação 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. Consulte mais informações em [Objetos de referência com objetos externos IDs](#) no Guia de Usuário AWS IoT SiteWise .

Como excluir um modelo de ativo (AWS CLI)

1. Execute o seguinte comando para listar todos os ativos criados usando o modelo. *asset-model-id* Substitua pela ID ou pela ID externa do modelo de ativo.

```
aws iotsitewise list-assets --asset-model-id asset-model-id
```

Para obter mais informações, consulte a operação [ListAssets](#).

2. Se o comando anterior retornar quaisquer ativos do modelo, exclua cada ativo. Para obter mais informações, consulte [Excluir um ativo \(AWS CLI\)](#).
3. Execute o comando a seguir para excluir o modelo de ativo. *asset-model-id* Substitua pelo ID ou ID externo do modelo de ativo.

```
aws iotsitewise delete-asset-model --asset-model-id asset-model-id
```

Important

Para evitar a exclusão de um modelo de ativo que foi atualizado simultaneamente desde a última operação de leitura, você deve definir uma solicitação de exclusão condicional. Consulte [Bloqueio positivo para gravações do modelo de ativo](#).

Operações em massa com ativos e modelos

Para trabalhar com um grande número de ativos ou modelos de ativo, use operações 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 ativo em um bucket do Amazon S3 e usar a importação em massa para criar ou atualizá-los no 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. Basta ter um bucket do Amazon S3 no qual possa colocar o conteúdo do AWS IoT SiteWise .

Tópicos

- [Principais conceitos e terminologia](#)
- [Funções compatíveis](#)
- [Pré-requisitos das operações em massa](#)
- [Executar um trabalho de importação em massa](#)
- [Executar um trabalho de exportação em massa](#)
- [Acompanhamento do progresso dos trabalhos e tratamento de erros](#)
- [Exemplos de importação de metadados](#)
- [Exemplos de exportação de metadados](#)
- [AWS IoT SiteWise esquema de trabalho de transferência de metadados](#)

Principais conceitos e terminologia

AWS IoT SiteWise Os recursos de importação e exportação em massa dependem dos seguintes conceitos e terminologia:

- **Importar:** a ação de mover ativos ou modelos de ativo 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 para onde você deseja mover o 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. Entre os exemplos estão propriedades, hierarquias e modelos compostos.
- **Metadados:** informações importantes necessárias para importar ou exportar recursos com êxito. Entre os exemplos de metadados estão definições de ativos e modelos de ativo.
- **metadataTransferJob:** o objeto criado quando você executa `CreateMetadataTransferJob`.

Funções compatíveis

Este tópico explica o que você pode fazer ao executar uma operação em massa. As operações em massa oferecem suporte à seguinte funcionalidade:

- **Criação de recursos de nível superior:** quando você importa um ativo ou um modelo de ativo que não define um ID ou cujo ID não corresponde ao de um existente, ele é criado como um novo recurso.
- **Substituição de recursos de nível superior:** quando você importa um ativo ou um modelo de ativo cujo ID corresponde a um já existente, o recurso existente é substituído.
- **Criação, substituição ou exclusão de sub-recursos:** quando a importação substitui um recurso de nível superior, como um ativo ou um 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: as operações em massa não excluem ativos ou modelos de ativo. As operações em massa apenas os criam ou atualizam.

Pré-requisitos das operações 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 AWS serviços e sua máquina local. Antes de começar uma operação em massa, cumpra o seguinte pré-requisito:

- Crie um bucket do Amazon S3 para armazenar recursos. Para ter mais informações sobre como usar o 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. Para obter mais informações sobre como criar políticas do IAM, consulte [Criar políticas do IAM](#).

Para realizar operações em massa, você precisa das políticas a seguir.

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 concede acesso aos buckets do Amazon S3 para transferência de metadados para operações em massa.

For a specific Amazon S3 bucket

Se você usar um bucket específico para trabalhar com os metadados de operações em massa, essa política concederá 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 os metadados das operações em massa, essa política concederá acesso a todos os buckets:

```
{
  "Effect": "Allow",
  "Action": [
    "s3:PutObject",
    "s3:GetObject",
    "s3:GetBucketLocation",
    "s3:ListBucket",
    "s3:AbortMultipartUpload",
    "s3:ListBucketMultipartUploads",
    "s3:ListMultipartUploadParts"
  ],
}
```

```
"Resource": "*"
}
```

Para ter informações sobre como solucionar problemas nas operações de importação e exportação, consulte [Solucionar problemas de importação e exportação em massa](#).

Executar 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 para importação

Faça o download do arquivo em 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: fazer upload do arquivo preparado no Amazon S3

Faça upload do arquivo no Amazon S3. Consulte [Uploading a file to Amazon S3](#) no Guia do usuário do Amazon Simple Storage Service para conferir detalhes.

Importar metadados (console)

Você pode usar o Console do AWS IoT SiteWise para importar metadados em massa. Siga [Etapa 1: preparar o arquivo para importação](#) e [Etapa 2: fazer upload do arquivo preparado no Amazon S3](#) para preparar 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 > Novo no painel de navegação.
3. Escolha Nova importação para iniciar o processo de importação.
4. Na página Importar metadados:
 - Escolha Procurar no Amazon S3 para exibir o bucket do Amazon S3 e os arquivos.

- 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 seguinte procedimento:

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 no bucket do Amazon S3.

Para conferir exemplos de arquivos de metadados a serem importados, consulte [Exemplos de importação de metadados](#).

2. Agora, crie um arquivo JSON com o corpo da solicitação. O corpo da solicitação especifica a fonte e o destino do trabalho de transferência. Esse arquivo é diferente do arquivo da etapa anterior. Não se esqueça de especificar o bucket do Amazon S3 como uma fonte e `iotsitewise` como o destino.

O seguinte exemplo mostra o corpo da solicitação:

```
{
  "metadataTransferJobId": "your-transfer-job-Id",
  "sources": [{
    "type": "s3",
    "s3Configuration": {
      "location": "arn:aws:s3::amzn-s3-demo-bucket/"
    }
  }],
  "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 se chama `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.

Executar 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 seção `iotSiteWiseConfiguration` dentro da seção de fontes da solicitação JSON.

Note

É possível incluir vários filtros na solicitação. A operação em massa vai exportar modelos de ativo e ativos correspondentes a qualquer um dos filtros.

Se você não fornecer nenhum filtro, a operação em massa exportará todos os modelos de ativo e 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:::amzn-s3-demo-bucket"
  }
}
}
```

Exportar metadados (console)

O seguinte procedimento 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 > Novo 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 nome será usado para o arquivo exportado no bucket do Amazon S3.
 - Escolha os recursos a serem exportados, o que define os filtros para o trabalho:
 - Exportar todos os ativos e modelos de ativos. Use filtros em ativos e modelos de ativo.
 - Exportar ativos. Filtre os ativos.
 - Selecione o ativo a ser usado no filtro de exportação.
 - (Opcional) Adicione o descendente ou o modelo de ativo associado.
 - Exportar modelos de ativos. Filtre os modelos de ativo.
 - Selecione o modelo de ativo a ser usado no filtro de exportação.
 - (Opcional) Adicione o descendente ou o ativo associado, ou ambos.
 - Escolha Próximo.
 - Navegue até o bucket do Amazon S3:
 - Escolha Procurar no Amazon S3 para exibir o bucket do Amazon S3 e os arquivos.
 - Navegue até o bucket do Amazon S3 no qual o arquivo deve ser colocado.
 - Escolha 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 fonte e o destino do trabalho de transferência. O seguinte exemplo mostra o corpo de um exemplo de corpo da solicitação:

```
{
```



```
{
  "metadataTransferJobId": "your-transfer-job-Id",
  "sources": [{
    "type": "iotsitewise"
  }],
  "destination": {
    "type": "s3",
    "s3Configuration": {
      "location": "arn:aws:s3:::amzn-s3-demo-bucket"
    }
  }
}
```

Não se esqueça de especificar o bucket do Amazon S3 como o destino do trabalho de transferência dos metadados.

Note

Este exemplo exportará todos os modelos de ativo e ativos. Para limitar a exportação a modelos de ativo ou ativos específicos, você pode incluir filtros no corpo da solicitação. Para ter mais informações sobre como aplicar filtros de exportação, consulte [Exemplos de exportação de metadados](#).

2. Salve o arquivo do corpo da solicitação a ser usado 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 JSON de entrada `createMetadataTransferJobExport.json` pelo nome do seu próprio arquivo de transferência.

Acompanhamento do progresso dos trabalhos e tratamento de erros

Um trabalho de processo em massa demora 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:** validação do trabalho, inclusive o formato do arquivo enviado e o conteúdo.
- **PENDING:** o trabalho está em uma fila. Você pode cancelar trabalhos nesse estado pelo console do AWS IoT SiteWise, mas todos os outros estados continuarão até o final.
- **RUNNING:** processamento do trabalho. Ele está criando e atualizando recursos conforme definido pelo arquivo de importação ou exportando recursos com base nos filtros do trabalho de exportação escolhidos. Se cancelado, nenhum recurso importado por esse trabalho é excluído. Consulte [Revisar o progresso dos trabalhos e os detalhes \(console\)](#) para obter mais informações.
- **CANCELLING:** o trabalho está sendo cancelado ativamente.
- **ERROR:** falha no processamento de um ou mais recursos. Consulte o relatório de trabalho detalhado para ter mais informações. Consulte [Inspeccionar detalhes de erros \(console\)](#) para obter mais informações.
- **COMPLETED:** trabalho 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 dos trabalhos](#)
- [Inspeccione erros para AWS IoT SiteWise](#)

Acompanhamento do progresso dos trabalhos

Revisar o progresso dos trabalhos e os detalhes (console)

Consulte [Importar metadados \(console\)](#) ou [Exportar metadados \(console\)](#) para iniciar 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 > Novo 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. É possível selecionar um trabalho para ver detalhes sobre o trabalho.
6. O trabalho selecionado mostra Êxito quando bem-sucedido, ou uma lista de falhas caso o trabalho falhe. 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 trabalho para ver mais detalhes.
2. Para um trabalho de importação, o `Data source ARN` representa o local do arquivo de importação no Amazon S3.
3. Para um trabalho de exportação, o `Data destination ARN` representa o local do arquivo depois da exportação no Amazon S3.
4. O `Status` e o `Status reason` dão detalhes adicionais sobre o trabalho atual. Consulte [Acompanhamento do progresso dos trabalhos e tratamento de erros](#) para obter mais detalhes.
5. A `Queued position` representa a posição do trabalho na fila do processo. Os trabalhos são processados um de cada vez. Uma posição 1 na fila indica que o trabalho será processado em seguida.
6. A página de detalhes dos trabalhos também exibe as contagens de progresso dos trabalhos.
 - Os tipos de contagem de progresso dos trabalhos são:
 - i. `Total resources`: indica a contagem total de ativos no processo de transferência.
 - ii. `Succeeded`: indica a contagem de ativos transferidos com êxito 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. Um status de trabalho de `PENDING` ou `VALIDATING` exibe todas as contagens de progresso dos trabalhos como `-`. Isso indica que as contagens de progresso dos trabalhos estão sendo avaliadas.

8. Um status de trabalho de `RUNNING` exibe a contagem `Total resources`, o trabalho enviado para processamento. As contagens detalhadas (`Succeeded`, `Failed` e `Skipped`) se aplicam aos recursos processados. A soma das contagens detalhadas é menor do que a contagem `Total resources`, até que o status do trabalho seja `COMPLETED` ou `ERROR`.
9. Se o status de um trabalho for `COMPLETED` ou `ERROR`, a contagem `Total resources` será igual à soma das contagens detalhadas (`Succeeded`, `Failed` e `Skipped`).
10. Se o status de um trabalho for `ERROR`, verifique a tabela Falhas de trabalhos para conferir detalhes sobre as falhas e os erros específicos. Consulte [Inspeccionar detalhes de erros \(console\)](#) para obter mais detalhes.

Revisar o progresso dos trabalhos e os detalhes (AWS CLI)

Depois de iniciar uma operação em massa, você poderá verificar ou atualizar o status usando as seguintes ações de API:

- Para recuperar informações sobre um trabalho específico, use a ação da [GetMetadataTransferJob](#) API.

Recupere informações com a API **GetMetadataTransferJob**:

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 API `GetMetadataTransferJob` retorna um objeto `MetadataTransferJobProgress` com os seguintes parâmetros:
 - `succeededCount`: indica a contagem de ativos transferidos com êxito 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 de progresso dos trabalhos. Se o status for `RUNNING`, eles ajudarão a acompanhar o número de recursos que ainda precisam ser processados.

Se você encontrar erros na validação do esquema, ou se `failedCount` for maior ou igual a 1, o estado de progresso do trabalho será alterado para `ERROR`. O relatório de erros completo do trabalho é colocado no bucket do Amazon S3. Consulte [Inspeção de erros para AWS IoT SiteWise](#) para obter mais detalhes.

- Para listar os trabalhos atuais, use a ação [ListMetadataTransferJobs](#) da API.

Use um arquivo JSON para filtrar os trabalhos retornados com base no estado atual. Consulte o seguinte procedimento:

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 [ListMetadataTransferJobsFilter](#) 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 [CancelMetadataTransferJob](#) da API. Essa API cancela o trabalho de transferência de metadados específico, 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 para AWS IoT SiteWise

Inspecionar detalhes de erros (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 exibir os detalhes do trabalho.
4. Se o status de um trabalho for COMPLETED ou ERROR, a contagem `Total resources` será igual à soma das contagens detalhadas (`Succeeded`, `Failed` e `Skipped`).
5. Se o status de um trabalho for ERROR, verifique a tabela Falhas de trabalhos para conferir detalhes sobre as falhas e os erros específicos.
6. A tabela Falhas de trabalhos exibe o conteúdo do relatório do trabalho. O campo `Resource type` indica o local do erro ou das falhas, como o seguinte:
 - Por exemplo, um erro de validação em `Bulk operations template`, no campo `Resource type`, indica que o modelo de importação e o formato do arquivo do esquema de metadados não coincidem. Consulte [AWS IoT SiteWise esquema de trabalho de transferência de metadados](#) para obter mais informações.
 - Uma falha em `Asset`, no campo `Resource type`, 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.

Inspecionar detalhes de erros (AWS CLI)

Para tratar e diagnosticar erros produzidos durante um trabalho de transferência, consulte o seguinte procedimento sobre como usar a ação de API `GetMetadataTransferJob`:

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 mudar para COMPLETED, você poderá começar a verificar os resultados do trabalho.

3. Quando você chama `GetMetadataTransferJob`, é retornado 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 transferidos com êxito no processo de transferência.
 - `totalCount`: indica a contagem total de ativos envolvidos no processo de transferência.
4. Além disso, a chamada de API retorna um elemento `reportUrl`, que contém um URL pré-assinado. Se o trabalho de transferência tiver algum problema que você precise investigar mais detalhadamente, visite esse URL.

Exemplos de importação de metadados

Esta seção mostra como criar arquivos de metadados para importar modelos de ativo e ativos com uma única operação de importação em massa.

Exemplo de uma importação em massa

Você pode importar muitos modelos de ativo e ativos com uma única operação de importação em massa. O exemplo a seguir mostra como criar um arquivo de metadados para isso.

Neste cenário de exemplo, há vários locais de trabalho que contêm robôs industriais em células de trabalho.

O exemplo define dois modelos de ativo:

- `RobotModel1`: este modelo de ativo representa um tipo específico de robô disponível nos locais de trabalho. O robô tem uma propriedade de medição, `Temperature`.
- `WorkCell`: este modelo de ativo representa um conjunto de robôs dentro de um dos locais de trabalho. O modelo de ativos define uma hierarquia, `robotHierarchyOEM1`, para representar a relação em que uma célula de trabalho contém robôs.

O exemplo também define alguns ativos:

- WorkCell11: uma célula de trabalho dentro do local 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 de ativo e 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": "workCellHierarchyWith0EM1Robot",
          "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, há vários locais de trabalho que contêm robôs industriais em uma empresa.

O exemplo define vários modelos de ativo:

- **Sample_Enterprise:** este modelo de ativo representa a empresa da qual os locais fazem parte. O modelo de ativo define uma hierarquia, **Enterprise** to **Site**, para representar a relação dos locais com a empresa.

- **Sample_Site**: este modelo de ativo representa os locais de fabricação dentro da empresa. O modelo de ativo define uma hierarquia, **Site** to **Line**, para representar a relação das linhas com o local.
- **Sample_Welding Line**: este modelo de ativo representa uma linha de montagem dentro dos locais de trabalho. O modelo de ativo define uma hierarquia, **Line** to **Robot**, para representar a relação dos robôs com a linha.
- **Sample_Welding Robot**: este modelo de ativo representa um tipo específico de robô nos locais de trabalho.

O exemplo também define ativos baseados nos modelos de ativo.

- **Sample_AnyCompany Motor**: este ativo é criado com base no modelo de ativo **Sample_Enterprise**.
- **Sample_Chicago**: este ativo é criado com base no modelo de ativo **Sample_Site**.
- **Sample_Welding Line 1**: este ativo é criado com base no modelo de ativo **Sample_Welding Line**.
- **Sample_Welding Robot 1**: este ativo é criado com base no modelo de ativo **Sample_Welding Robot**.
- **Sample_Welding Robot 2**: este ativo é criado com base no modelo de ativo **Sample_Welding Robot**.

O arquivo de metadados JSON a seguir define esses modelos de ativo e 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_T0_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_T0_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_T0_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_T0_Robot",

```

```

        "childAssetExternalId": "External_Id_Welding_Robot_1"
    },
    {
        "externalId": "External_Id_Welding_Line_T0_Robot",
        "childAssetExternalId": "External_Id_Welding_Robot_2"
    }
]
},
{
    "assetExternalId": "External_Id_Site_Chicago",
    "assetName": "Sample_Chicago",
    "assetModelExternalId": "External_Id_Site",
    "assetHierarchies": [
        {
            "externalId": "External_Id_Site_T0_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_T0_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.

IoT SiteWise > Models

Models (4) Refresh Create component model Create asset model

Assets represent industrial devices and processes that send data streams to SiteWise. Models are structures that enforce a specific model of properties and hierarchies for all instances of each asset. You must create every asset from a model.

Name	Status	Model type	Date created	Date modified
Sample_Enterprise	ACTIVE	Asset model	November 10, 2023 at 11:22:13 (UT...)	November 10, 202...
Sample_Site	ACTIVE	Asset model	November 10, 2023 at 11:21:57 (UT...)	November 10, 202...
Sample_Welding Line	ACTIVE	Asset model	November 10, 2023 at 11:21:40 (UT...)	November 10, 202...
Sample_Welding Robot	ACTIVE	Asset model	November 10, 2023 at 11:21:24 (UT...)	November 10, 202...

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.

IoT SiteWise > Assets

Assets (1) Refresh Create asset

Assets represent industrial devices and processes that send data streams to SiteWise. Models are structures that enforce a specific model of properties and hierarchies for all instances of each asset. You must create every asset from a model.

Name	Description	Status	Date created	Date modified
☒ Sample_AnyEnterprise Motor		ACTIVE	November 10, 2023 at 11:23:06 (UTC-5:00)	November 10, 2023 at 11:23:06 (UTC-...
☒ Sample_Chicago		ACTIVE	November 10, 2023 at 11:22:57 (UTC-5:00)	November 10, 2023 at 11:22:57 (UTC-...
☒ Sample_Welding Line 1		ACTIVE	November 10, 2023 at 11:22:48 (UTC-5:00)	November 10, 2023 at 11:22:48 (UTC-...
☐ Sample_Welding Robot 1		ACTIVE	November 10, 2023 at 11:22:39 (UTC-5:00)	November 10, 2023 at 11:22:39 (UTC-...
☐ Sample_Welding Robot 2		ACTIVE	November 10, 2023 at 11:22:30 (UTC-5:00)	November 10, 2023 at 11:22:30 (UTC-...

Exemplo de integração de ativos adicionais

Este exemplo define ativos adicionais a serem importados para um modelo de ativo existente na conta:

- **Sample_Welding Line 2**: este ativo é criado com base no modelo de ativo **Sample_Welding Line**.
- **Sample_Welding Robot 3**: este ativo é criado com base no modelo de ativo **Sample_Welding Robot**.
- **Sample_Welding Robot 4**: este ativo é criado com base no modelo de ativo **Sample_Welding Robot**.

Para criar os ativos iniciais para esse exemplo, consulte [Exemplo de integração inicial de modelos e ativos](#).

O arquivo de metadados JSON a seguir define esses modelos de ativo e 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_T0_Robot",
            "childAssetExternalId": "External_Id_Welding_Robot_1"
        },
        {
            "externalId": "External_Id_Welding_Line_T0_Robot",
            "childAssetExternalId": "External_Id_Welding_Robot_2"
        },
        {
            "externalId": "External_Id_Welding_Line_T0_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_T0_Robot",
            "childAssetExternalId": "External_Id_Welding_Robot_4"
        }
    ]
},
{
    "assetExternalId": "External_Id_Site_Chicago",
    "assetName": "Sample_Chicago",
    "assetModelExternalId": "External_Id_Site",
    "assetHierarchies": [
        {
            "externalId": "External_Id_Site_T0_Line",

```

```

        "childAssetExternalId": "External_Id_Welding_Line_1"
      },
      {
        "externalId": "External_Id_Site_T0_Line",
        "childAssetExternalId": "External_Id_Welding_Line_2"
      }
    ]
  }
]
}

```

A captura de tela a seguir mostra modelos, ativos e hierarquias que são exibidos no Console do AWS IoT SiteWise após a execução do exemplo de código anterior.

The screenshot shows the AWS IoT SiteWise console with the 'Assets' tab selected. It displays a list of assets under the 'Sample_AnyCompany Motor' model. The assets are organized into a hierarchy: 'Sample_Chicago' (containing 'Sample_Welding Line 1' and 'Sample_Welding Robot 2', 'Sample_Welding Robot 3', and 'Sample_Welding Robot 1'), and 'Sample_Welding Line 2' (containing 'Sample_Welding Robot 4'). All assets are in an 'ACTIVE' status.

Name	Description	Status	Date created	Date modified
Sample_AnyCompany Motor		ACTIVE	November 09, 2023 at 19:18:05 (UTC-5:00)	November 09, 2023 at 19:18:05 (UTC-5:00)
Sample_Chicago		ACTIVE	November 09, 2023 at 19:17:56 (UTC-5:00)	November 09, 2023 at 19:17:56 (UTC-5:00)
Sample_Welding Line 1		ACTIVE	November 09, 2023 at 19:17:48 (UTC-5:00)	November 09, 2023 at 19:17:48 (UTC-5:00)
Sample_Welding Robot 2		ACTIVE	November 09, 2023 at 19:17:39 (UTC-5:00)	November 09, 2023 at 19:51:05 (UTC-5:00)
Sample_Welding Robot 3		ACTIVE	November 09, 2023 at 20:40:02 (UTC-5:00)	November 09, 2023 at 20:40:02 (UTC-5:00)
Sample_Welding Robot 1		ACTIVE	November 09, 2023 at 19:17:30 (UTC-5:00)	November 09, 2023 at 19:51:05 (UTC-5:00)
Sample_Welding Line 2		ACTIVE	November 09, 2023 at 20:40:20 (UTC-5:00)	November 09, 2023 at 20:40:20 (UTC-5:00)
Sample_Welding Robot 4		ACTIVE	November 09, 2023 at 20:40:11 (UTC-5:00)	November 09, 2023 at 20:40:11 (UTC-5:00)

Exemplo de integração de novas propriedades

Este exemplo define novas propriedades em modelos de ativo existentes. Consulte [Exemplo de integração de ativos adicionais](#) para integrar ativos e modelos adicionais.

- **Joint 1 Temperature:** esta propriedade é adicionada ao modelo de ativo `Sample_Welding Robot`. Essa nova propriedade também se propagará para cada ativo criado com base no modelo de ativo `Sample_Welding Robot`.

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

de ativo `Sample_Welding Robot` existente deve ser fornecida 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 ativo.

```
{
  "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"
    }
  ]
}

```

Exemplo de gerenciamento dos fluxos de dados

Este exemplo mostra duas maneiras de gerenciar fluxos de dados associados a uma propriedade do ativo. Durante a renomeação de um alias de propriedade do ativo, há duas opções para os dados históricos atualmente armazenados no fluxo de dados da propriedade do ativo.

- Primeira opção: manter o fluxo de dados atual e renomear apenas o alias, permitindo que os dados históricos possam ser acessados com o novo alias.

No exemplo de arquivo de metadados JSON, a propriedade do ativo com ID `External_Id_Welding_Robot_Cycle_Count` muda de alias para `AnyCompany/Chicago/Welding Line/S3000/Count-Updated`. Os dados históricos dessa propriedade do ativo permanecerão os mesmos depois dessa alteração.

- Segunda opção: atribuir um novo fluxo de dados à propriedade do ativo que pode ser acessado com o novo alias. O fluxo de dados anterior com os respectivos dados históricos ainda pode ser acessado com o alias anterior, mas não pode ser associado a nenhuma propriedade do ativo.

No exemplo de arquivo de metadados JSON, a propriedade do ativo com ID `External_Id_Welding_Robot_Joint_1_Current` muda de alias para `AnyCompany/Chicago/Welding Line/S4999/1/Current`. Desta vez, o valor adicional `retainDataOnAliasChange` está presente e definido como `False`. Com essa configuração, o fluxo de dados original é desassociado da propriedade do ativo e um novo fluxo de dados é criado sem dados históricos.

Para acessar o fluxo de dados antigo com os dados históricos originais AWS Console Home, acesse a página Fluxos de dados e pesquise o `AnyCompany/Chicago/Welding Line/S3000/1/Current` alias antigo.

Arquivo JSON para atualizar aliases de propriedade

```
{
  "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-Updated"
    },
    {
      "externalId": "External_Id_Welding_Robot_Joint_1_Current",
      "alias": "AnyCompany/Chicago/Welding Line/S4999/1/Current",
      "retainDataOnAliasChange": "FALSE"
    }
  ]
}

```

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.

Especifique os filtros em uma seção `iotSiteWiseConfiguration` dentro da seção `sources` 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 modelos de ativo e ativos.

```

{
  "metadataTransferJobId": "your-transfer-job-id",
  "sources": [{
    "type": "iotsitewise",
    "iotSiteWiseConfiguration": {
      "filters": [{
        list of filters
      }]
    }
  ]},
  "destination": {
    "type": "s3",

```

```
    "s3Configuration": {
      "location": "arn:aws:s3:::amzn-s3-demo-bucket"
    }
  }
}
```

Filtrar por modelo de ativo

Você pode filtrar um modelo de ativo específico. Você também pode incluir todos os ativos que usam esse modelo ou todos os modelos de ativo dentro da hierarquia. Não é possível incluir ativos e hierarquia.

Para obter mais informações sobre hierarquias, consulte [Definir hierarquias de modelos de ativo](#).

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 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 com todos os modelos de ativo associados na hierarquia:

```
"filterByAssetModel": {
  "assetModelId": "asset model ID",
  "includeOffspring": true
}
```


Filtrar por ativo

Você pode filtrar um ativo específico. Você também pode incluir o respectivo modelo de ativo ou todos os ativos associados dentro da hierarquia. Não é possível incluir o modelo de ativo e a hierarquia.

Para obter mais informações sobre hierarquias, consulte [Definir hierarquias de modelos de ativo](#).

Asset

Esse filtro inclui o ativo especificado:

```
"filterByAsset": {  
  "assetId": "asset ID"  
}
```

Asset and its asset model

Esse filtro inclui o ativo especificado com o modelo de ativo que ele usa:

```
"filterByAsset": {  
  "assetId": "asset ID",  
  "includeAssetModel": true  
}
```

Asset and its hierarchy

Esse filtro inclui o ativo especificado com todos os ativos associados na 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",
    "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",
        "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"
    }
  }
}
}

```

Monitore dados com alarmes em AWS IoT SiteWise

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](#)
- [Estados de alarme](#)
- [Propriedades do estado do alarme](#)
- [Defina alarmes em modelos de ativos em AWS IoT SiteWise](#)
- [Configure alarmes em ativos no AWS IoT SiteWise](#)
- [Responda aos alarmes em AWS IoT SiteWise](#)
- [Ingerir um estado de alarme externo em AWS IoT SiteWise](#)

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

Note

Aviso de fim do suporte: em 20 de maio de 2026, AWS encerrará o suporte para AWS IoT Events. Depois de 20 de maio de 2026, você não poderá mais acessar o AWS IoT Events console ou os AWS IoT Events recursos. Para obter mais informações, consulte [AWS IoT Events Fim do suporte](#).

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 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 obter mais informações, consulte [Defina alarmes em modelos de ativos em AWS IoT SiteWise](#).

O objeto dos dados do estado do alarme contém as seguintes informações:

`stateName`

O estado do alarme. Para obter 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

Defina alarmes em modelos de ativos em AWS IoT SiteWise

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.

Note

Aviso de fim do suporte: em 20 de maio de 2026, AWS encerrará o suporte para AWS IoT Events. Depois de 20 de maio de 2026, você não poderá mais acessar o AWS IoT

Events console ou os AWS IoT Events recursos. Para obter mais informações, consulte [AWS IoT Events Fim do suporte](#).

- **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 obter 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

- [Requisitos para notificações de alarme em AWS IoT SiteWise](#)
- [Defina AWS IoT Events alarmes para AWS IoT SiteWise](#)
- [Defina alarmes externos em AWS IoT SiteWise](#)

Requisitos para notificações de alarme em AWS IoT SiteWise

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.

Note

Aviso de fim do suporte: em 20 de maio de 2026, AWS encerrará o suporte para AWS IoT Events. Depois de 20 de maio de 2026, você não poderá mais acessar o AWS IoT Events console ou os AWS IoT Events recursos. Para obter mais informações, consulte [AWS IoT Events Fim do suporte](#).

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 .

Defina AWS IoT Events alarmes para AWS IoT SiteWise

Note

Aviso de fim do suporte: em 20 de maio de 2026, AWS encerrará o suporte para AWS IoT Events. Depois de 20 de maio de 2026, você não poderá mais acessar o AWS IoT Events console ou os AWS IoT Events recursos. Para obter mais informações, consulte [AWS IoT Events Fim do suporte](#).

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 habilitar esse recurso AWS IoT SiteWise, você deve ter a `iotevents:ListInputRoutings` permissão. Essa permissão permite AWS IoT SiteWise fazer chamadas para a operação de [ListInputRoutings](#) API suportada pelo AWS IoT Events. Para obter mais informações, consulte [ListInputRoutings Permissão \(opcional\)](#).

 Note

O atributo de notificações de alarme não está disponível na região da China (Pequim).

Tópicos

- [Definir um AWS IoT Events alarme \(AWS IoT SiteWise console\)](#)
- [Definir um AWS IoT Events alarme \(AWS IoT Events console\)](#)
- [Definir um AWS IoT Events alarme \(AWS CLI\)](#)

Definir 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 obter mais informações, consulte [Crie modelos de ativos em AWS IoT SiteWise](#).

 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 ter mais informações, consulte [Verifying an email address identity](#) 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 `ss-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.

Definir 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 obter mais informações, consulte [Crie modelos de ativos em AWS IoT SiteWise](#).

 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 `ss-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.

Definir 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: Definir um modelo AWS IoT Events de alarme](#)
- [Etapa 3: Habilitar 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 [Criar um modelo de ativo \(AWS CLI\)](#).
 - Para obter mais informações sobre como atualizar um modelo de ativo existente, consulte [Atualizar um modelo de ativo ou de 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 [ListInstances](#) API 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 [ListUsers](#) API do IAM Identity Center para obter o ID de um usuário cujo nome de usuário você conhece. *d-123EXAMPLE* Substitua pela ID do seu repositório de identidades e *Name* substitua 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 uma ID de remetente AWS End User Messaging SMS no Guia do AWS End User Messaging SMS usuário](#).

```
{
  ...
  "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. *asset-model-id* Substitua pelo 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: Definir 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.

assetModelId Substitua pela ID do modelo de ativo e *propertyId* substitua pela ID da propriedade.

```
$sitewise.assetModel.`assetModelId`.`propertyId` .propertyValue.value
```

- Ativo IDs

Para obter a ID do ativo, use a expressão a seguir. *assetModelId* Substitua pela ID do modelo de ativo e *propertyId* substitua pela 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 essas propriedades no modelo de ativo. IDs *asset-model-id* Substitua pelo 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 os usa IDs ao criar o modelo de AWS IoT Events alarme 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`).
 - *assetModelId* Substitua pelo ID do modelo de ativo.
 - *alarmPropertyId* Substitua pela ID da propriedade que o alarme monitora.
 - *thresholdAttributeId* Substitua pelo ID da propriedade do atributo de limite.
 - *GREATER* Substitua pelo operador a ser usado para comparar os valores da propriedade com o 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.

- *assetModelId* Substitua pelo ID do modelo de ativo.
- *alarmPropertyId* Substitua pela ID da propriedade que o alarme monitora.
- *alarmStatePropertyId* Substitua pela 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 obter mais informações, consulte [Requisitos para notificações de alarme em AWS IoT SiteWise](#). 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.
 - *alarmNotificationFunctionArn* Substitua pelo ARN da função Lambda que gerencia 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.
 - *identityStoreIdAttributeId* Substitua pelo ID do atributo que contém o ID do repositório de identidades do IAM Identity Center.
 - *userIdAttributeId* Substitua pelo ID do atributo que contém o ID do usuário do IAM Identity Center.
 - *senderIdAttributeId* Substitua pelo ID do atributo que contém o ID do remetente do Amazon SNS ou remova-o senderId da carga.

- *additionalMessageAttributeId* Substitua pela ID do atributo que contém a mensagem adicional 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."
    }
    ]
    }
    ]
    }
    }

```

- 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.
- *identityStoreIdAttributeId* Substitua pelo ID da propriedade do atributo ID do repositório de identidades do IAM Identity Center.
 - *userIdAttributeId* Substitua pelo ID da propriedade do atributo ID do usuário do IAM Identity Center.
 - *fromAddressAttributeId* Substitua pela ID da propriedade do atributo de endereço "de" ou remova from da carga.
 - *emailSubjectAttributeId* Substitua pela ID da propriedade do atributo do assunto do e-mail ou subject remova da carga.
 - *additionalMessageAttributeId* Substitua pela ID da propriedade adicional do atributo da mensagem ou additionalMessage remova 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":
                                "$sitewise.assetModel.`assetModelId`.`identityStoreIdAttributeId`.propertyValue.value",
                                "userId":
                                "$sitewise.assetModel.`assetModelId`.`userIdAttributeId`.propertyValue.value"
                            }
                        }
                    ],
                    "senderId":
                    "$sitewise.assetModel.`assetModelId`.`senderIdAttributeId`.propertyValue.value",
                    "additionalMessage":
                    "$sitewise.assetModel.`assetModelId`.`additionalMessageAttributeId`.propertyValue.value"
                }
            ],
            "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.value"
            }
        }
    ]
}

```

- 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.value"
        }
      ],
      "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.value"
            }
        }
    ],
    },
    "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 você 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":
    "$sitewise.assetModel.`assetModelId`.`additionalMessageAttributeId`.propertyValue.value"
    },
    "emailConfigurations": [
    {
        "from":
        "$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.value"
        }
    }
    ],
    },
    "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: Habilitar 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. `asset-model-id` Substitua pelo 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. *`alarmModelArn`* Substitua pelo ARN do modelo de alarme, que define o valor da propriedade da fonte de 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`. *asset-model-id* Substitua pelo 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 obter mais informações, consulte [Configure alarmes em ativos no AWS IoT SiteWise](#).

Defina alarmes externos em AWS IoT SiteWise

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 obter mais informações, consulte [Crie modelos de ativos em AWS IoT SiteWise](#).

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:

- [Criar um modelo de ativo \(AWS CLI\)](#)
- [Atualizar um modelo de ativo ou de 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 obter mais informações, consulte [Ingerir um estado de alarme externo em AWS IoT SiteWise](#).

Configure alarmes em ativos no AWS IoT SiteWise

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 \(console\)](#)
- [Configurar um valor limite \(AWS CLI\)](#)
- [Defina as configurações de notificação em AWS IoT SiteWise](#)

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. Escolha Editar.
5. Encontre o atributo que o alarme usa para seu valor limite e, então, insira seu novo valor.
6. Escolha Salvar.

Configurar 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 [ListAssets](#) API para listar todos os ativos de um modelo específico. Use a [DescribeAsset](#) operação para visualizar as propriedades do seu ativo, incluindo propriedades IDs.

Use a operação [BatchPutAssetPropertyValue](#) para atribuir valores de atributo ao 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.

Como 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 os IDs valores e os carimbos de data/hora para modificar a carga útil do seu 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`
- `nullValue`
- `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 útil para [BatchPutAssetPropertyValue](#), consulte [Ingira dados com AWS IoT SiteWise APIs](#).

2. Execute o seguinte comando para enviar os valores de atributo ao AWS IoT SiteWise:

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

Defina as configurações de notificação em AWS IoT SiteWise

Você pode definir as configurações de notificação de alarme usando o AWS IoT SiteWise console ou o AWS Command Line Interface (AWS CLI).

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. Escolha 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 `conneceassetId`, use a [ListAssets](#) API para listar todos os ativos de um modelo específico. Use a [DescribeAsset](#) operação para visualizar as propriedades do seu ativo, incluindo propriedades IDs.

Use a operação [BatchPutAssetPropertyValue](#) para atribuir valores de atributo ao 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.

Como 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 os IDs valores e os carimbos de data/hora para modificar a carga útil do seu 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`
 - `nullValue`
- `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 útil para [BatchPutAssetPropertyValue](#), consulte [Ingira dados com AWS IoT SiteWise APIs](#).

2. Execute o seguinte comando para enviar os valores de atributo ao AWS IoT SiteWise:


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

Responda aos alarmes em AWS IoT SiteWise

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 \(console\)](#)
- [Responder a um alarme \(API\)](#)

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 \(console\)](#)
- [Adiar um alarme \(console\)](#)
- [Desabilitar um alarme \(console\)](#)
- [Habilitar um alarme \(console\)](#)

- [Reconfigurar um alarme \(console\)](#)

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 :

- [BatchAcknowledgeAlarm](#)
- [BatchSnoozeAlarm](#)
- [BatchDisableAlarm](#)
- [BatchEnableAlarm](#)
- [BatchResetAlarm](#)

Para obter mais informações, consulte [Responder a alarmes](#), no Guia do desenvolvedor do AWS IoT Events .

Ingerir um estado de alarme externo em AWS IoT SiteWise

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 obter 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 [Definir fluxos de dados de equipamentos \(medições\)](#) e [Ingerir dados para AWS IoT SiteWise](#).

Mapeie fluxos externos de estado de alarme em AWS IoT SiteWise

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 [Gerencie fluxos de dados para AWS IoT SiteWise](#).

Tópicos

- [Mapear fluxos de estado de alarme externo \(console\)](#)
- [Mapear fluxos de estado de alarme externo \(AWS CLI\)](#)

Mapear fluxos de estado de alarme externo (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 [Gerencie fluxos de dados para AWS IoT SiteWise](#).

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. Escolha Editar.
5. Role a tela até Alarmes e expanda a seção.
6. Em Alarmes externos, insira o alias em Alias de propriedade – opcional.
7. Escolha Salvar.

Mapear fluxos de estado de alarme externo (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 [Gerencie fluxos de dados para AWS IoT SiteWise](#).

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 [ListAssets](#) API para listar todos os ativos de um modelo específico. Use a [DescribeAsset](#) operação para visualizar as propriedades do seu ativo, incluindo propriedades IDs.

 Note

A [DescribeAsset](#) resposta 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 [Atualizar um alias de propriedade do ativo](#).

Ingerir dados do estado do alarme em AWS IoT SiteWise

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 [Mapeie fluxos externos de estado de alarme em AWS IoT SiteWise](#).

O exemplo de carga útil [BatchPutAssetPropertyValue](#) da 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 [Ingira dados com AWS IoT SiteWise APIs](#).

Para obter mais informações outras formas de ingerir dados, consulte [Ingerir dados para AWS IoT SiteWise](#).

AWS IoT SiteWise Assistente

O AWS IoT SiteWise Assistant é um assistente generativo alimentado por IA. Ele permite que usuários como gerentes de fábrica, engenheiros de qualidade e técnicos de manutenção obtenham insights, resolvam problemas e tomem medidas diretamente de seus dados operacionais e corporativos.

O AWS IoT SiteWise Assistant consolida informações de AWS IoT dados, modelos de ativos, manuais e documentação em resumos compreensíveis de eventos críticos. Ele também permite sessões interativas de perguntas e respostas aprofundadas para facilitar o diagnóstico, explorar a causa raiz e fazer recomendações guiadas.

Tópicos

- [Configurar o AWS IoT SiteWise Assistente](#)
- [Criar um conjunto de dados](#)
- [Editar um conjunto de dados](#)
- [Excluir um conjunto de dados](#)
- [AWS IoT SiteWise Perguntas do assistente](#)

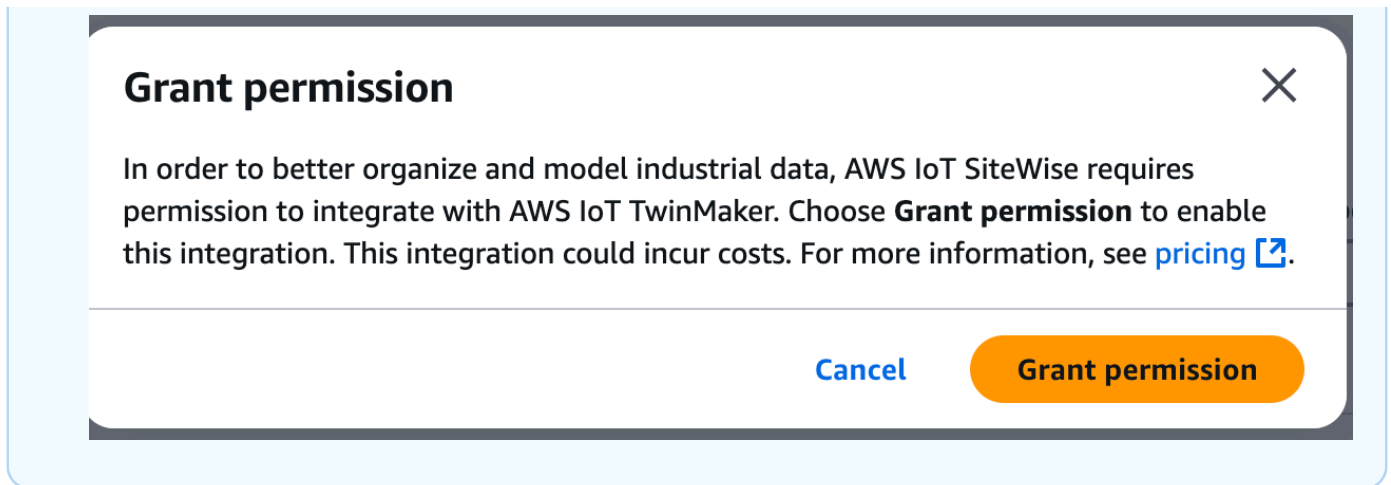
Configurar o AWS IoT SiteWise Assistente

AWS IoT SiteWise Configuração do assistente

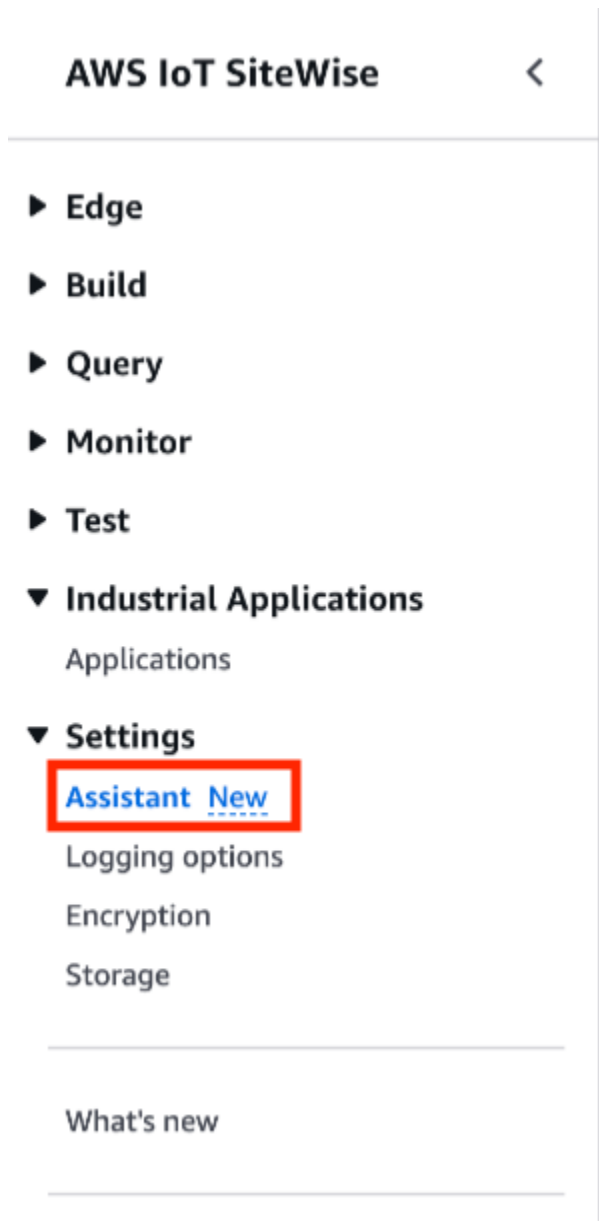
1. Faça login no [console do AWS IoT SiteWise](#).

Note

Conceda permissões para permitir a integração com o AWS IoT TwinMaker serviço. Isso é necessário para que o AWS IoT SiteWise Assistente e o painel executem consultas SQL nos AWS IoT SiteWise recursos. Consulte [AWS IoT SiteWise Integrar AWS IoT TwinMaker](#) e.



2. Escolha Assistente no painel de navegação esquerdo.



Criar um conjunto de dados

Note

O AWS IoT SiteWise Assistente deve usar um conjunto de dados com um índice [Amazon Kendra](#) para obter conhecimento e orientação em nível empresarial. Se você não tiver um índice do Amazon Kendra, [consulte Criação de um índice para criar um](#). Adicionar um [conjunto de dados](#) melhora a qualidade da resposta do Assistente e minimiza as alucinações.

Console

Crie um conjunto de dados no console AWS IoT SiteWise

1. Os conjuntos de dados são exibidos na seção Conjuntos de dados da página do AWS IoT SiteWise Assistente.
2. Se não houver conjuntos de dados, escolha Criar conjunto de dados.
3. Na página de detalhes do conjunto de dados, escolha um índice Kendra no menu suspenso para associar ao conjunto de dados.
4. O nome do conjunto de dados é preenchido pelo índice Kendra selecionado na Etapa 3. Edite o nome, se necessário.
5. (Opcional) A descrição do conjunto de dados é preenchida pelo índice Kendra selecionado na Etapa 3. Edite a descrição, se necessário.
6. Na seção Permissões, escolha uma das opções abaixo:
 - a. Escolha Criar e usar um novo perfil de serviço. Por padrão, cria AWS IoT SiteWise automaticamente uma função de serviço. Essa função permite que o AWS IoT SiteWise Assistente acesse seus índices Kendra.
 - b. Escolha Usar um perfil existente e escolha o perfil de serviço alvo.
7. Escolha Criar.

[AWS IoT SiteWise](#) > [Assistant](#) > Create dataset

Create dataset

Create a dataset for the Assistant.

Dataset details [Info](#)

Kendra index

Select a Kendra index for the Assistant dataset.

test-index

[Amazon Kendra](#)



Dataset name

Dataset name is pre-populated from the Kendra index selected. You can modify the dataset name.

Dataset1

Dataset name must be 1-256 characters. Valid characters are a-z, A-Z, 0-9, _ (underscore) and - (hyphen).

Dataset description - optional

Dataset description is pre-populated from the Kendra index selected. You can modify the dataset description.

Dataset for AWS IoT SiteWise Assistant

Dataset description must be 1-2048 characters.

Permissions

Assistant must have permissions to access the data. To create a custom role, visit the [IAM console](#).

Choose a method to authorize Assistant

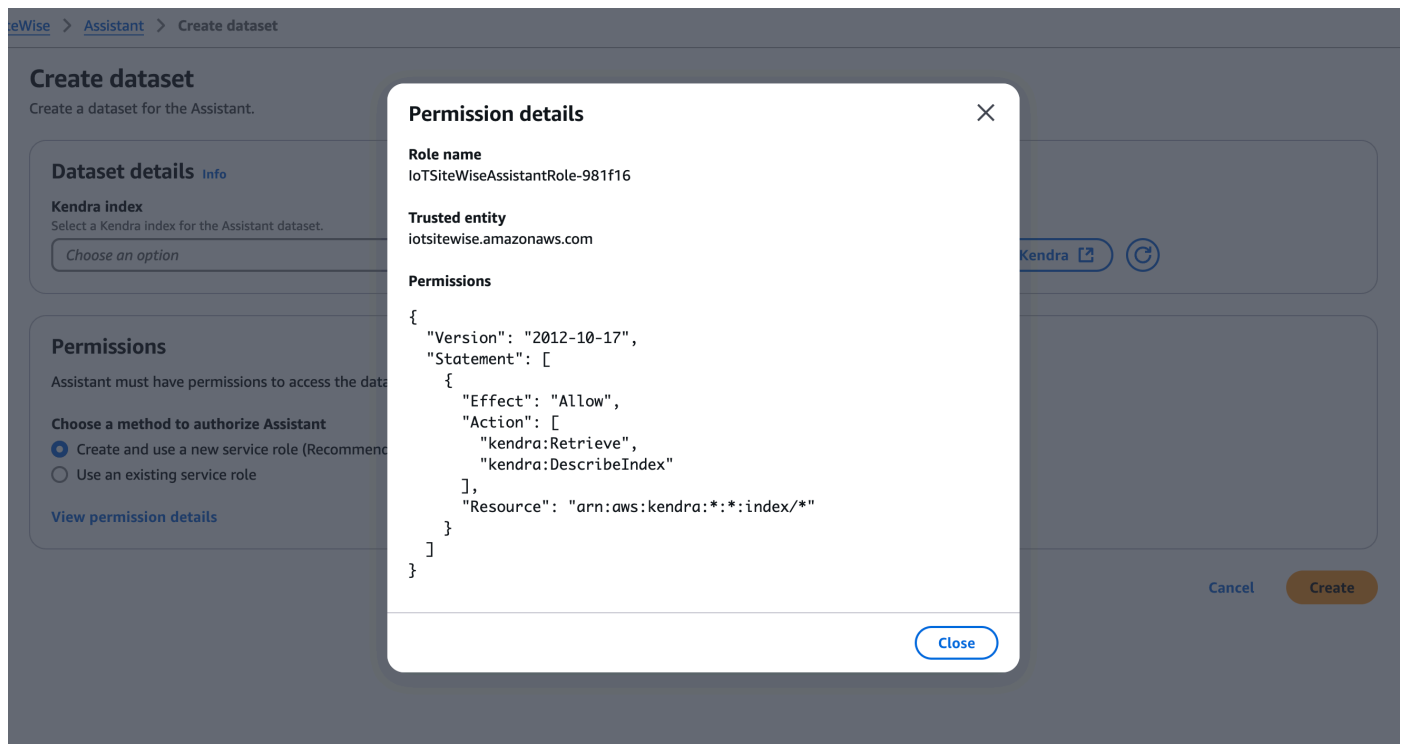
- ☒ Create and use a new service role - *recommended*
- ☐ Use an existing service role

[View permission details](#)

[Cancel](#)

Create

A função de serviço criada por AWS IoT SiteWise para o usuário, se o usuário optar por criar e usar uma nova função de serviço.



AWS CLI

Crie um conjunto de dados em AWS CLI

1. Crie uma função do IAM usada para criar um conjunto de dados. Use a seguinte política de permissões:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kendra:Retrieve"
      ],
      "Resource": "arn:aws:kendra:*:*:index/*"
    }
  ]
}
```

Use a seguinte relação de confiança:

```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "iotsitewise.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. Crie um arquivo `create-dataset.json` com o modelo fornecido no exemplo. Preencha `datasetId` `kendra` `knowledgeBaseArn` e conecte-se `roleArn` a esse conjunto de dados.

```
{
  "datasetId": "<UUID>",
  "datasetName": "DatasetForAssistant",
  "datasetSource": {
    "sourceType": "KENDRA",
    "sourceFormat": "KNOWLEDGE_BASE",
    "sourceDetail": {
      "kendra": {
        "knowledgeBaseArn": "arn:aws:kendra::%s:index/index",
        "roleArn": "arn:aws:iam::%s:role/role"
      }
    }
  }
}
```

3. Crie o conjunto de dados com o seguinte comando:

```
aws iotsitewise create-dataset --cli-input-json file://create-dataset.json --
region us-east-1
```


Editar um conjunto de dados

Console

Editar um conjunto de dados

1. Os conjuntos de dados são exibidos na seção Conjuntos de dados da página do Assistente. Escolha um conjunto de dados para editar. Escolha Editar para começar a editar.
2. Na página de detalhes do conjunto de dados, escolha um índice Kendra no menu suspenso para associar ao conjunto de dados.
3. O nome do conjunto de dados é preenchido pelo índice Kendra selecionado na Etapa 2. Edite o nome, se necessário.
4. (Opcional) A descrição do conjunto de dados é preenchida pelo índice Kendra selecionado na Etapa 2. Edite a descrição, se necessário.
5. Na seção Permissões, escolha uma das opções abaixo:
 - a. Escolha Criar e usar um novo perfil de serviço. Por padrão, cria AWS IoT SiteWise automaticamente uma função de serviço. Essa função permite que o AWS IoT SiteWise Assistente acesse seus índices Kendra.
 - b. Escolha Usar um perfil existente e escolha o perfil de serviço alvo.
6. Escolha Salvar alterações para salvar sua seleção.

[AWS IoT SiteWise](#) > [Assistant](#) > Edit dataset

Edit dataset

Edit a dataset for the Assistant.

Dataset details [Info](#)

Kendra index

Select a Kendra index for the Assistant dataset.

test-index

[Amazon Kendra](#)



Dataset name

Dataset name is pre-populated from the Kendra index selected. You can modify the dataset name.

Dataset1

Dataset name must be 1-256 characters. Valid characters are a-z, A-Z, 0-9, _ (underscore) and - (hyphen).

Dataset description - optional

Dataset description is pre-populated from the Kendra index selected. You can modify the dataset description.

Dataset for AWS IoT SiteWise Assistant

Dataset description must be 1-2048 characters.

Permissions

Assistant must have permissions to access the data. To create a custom role, visit the [IAM console](#).

Choose a method to authorize Assistant

- ☐ Create and use a new service role - *recommended*
- ☒ Use an existing service role

Existing role

IoTSiteWiseAssistantRole-40f994

[View the IoTSiteWiseAssistantRole-40f994 role in the IAM console](#)

[Cancel](#)

[Save changes](#)

AWS CLI

Edite um conjunto de dados no AWS CLI

1. Crie um arquivo update-dataset.json com o modelo fornecido no exemplo. Preencha datasetId, kendra, knowledgeBaseArn e conecte-se roleArn a esse conjunto de dados.

```
{
  "datasetId": "<UUID>",
  "datasetName": "DatasetForAssistant",
  "datasetSource": {
    "sourceType": "KENDRA",
    "sourceFormat": "KNOWLEDGE_BASE",
    "sourceDetail": {
      "kendra": {
        "knowledgeBaseArn": "arn:aws:kendra::%s:index/index",
```

```
        "roleArn": "arn:aws:iam::%s:role/role"
      }
    }
  }
}
```

2. Atualize o conjunto de dados com o seguinte comando:

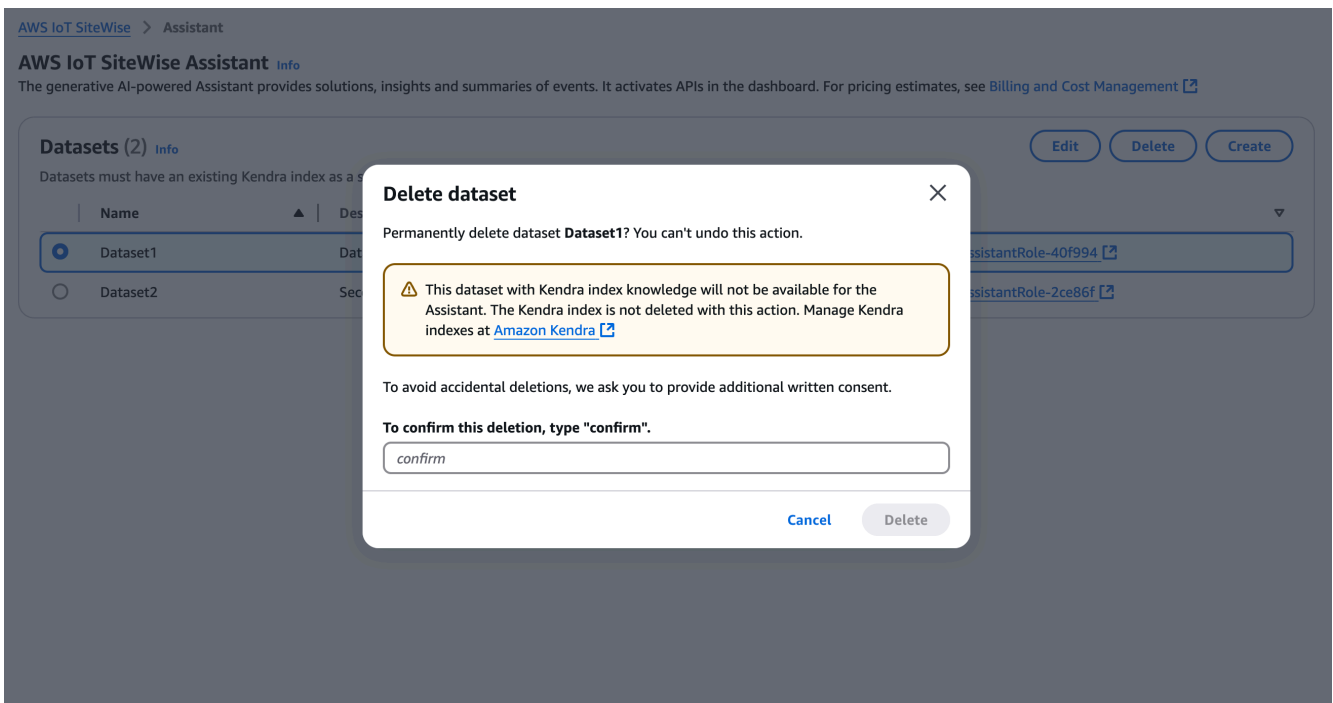
```
aws iotsitewise update-dataset --cli-input-json file://update-dataset.json --  
region us-east-1
```

Excluir um conjunto de dados

Console

Excluir um conjunto de dados

1. Os conjuntos de dados são exibidos na seção Conjuntos de dados da página do Assistente. Escolha um conjunto de dados. Escolha Excluir.
2. Digite confirm no pop-up para confirmar a exclusão.



3. Escolha Excluir.

AWS CLI

Excluir um conjunto de dados

- Exclua o conjunto de dados com `datasetId`.

```
aws iotsitewise delete-dataset --region us-east-1 --dataset-id <UUID>
```

AWS IoT SiteWise Perguntas do assistente

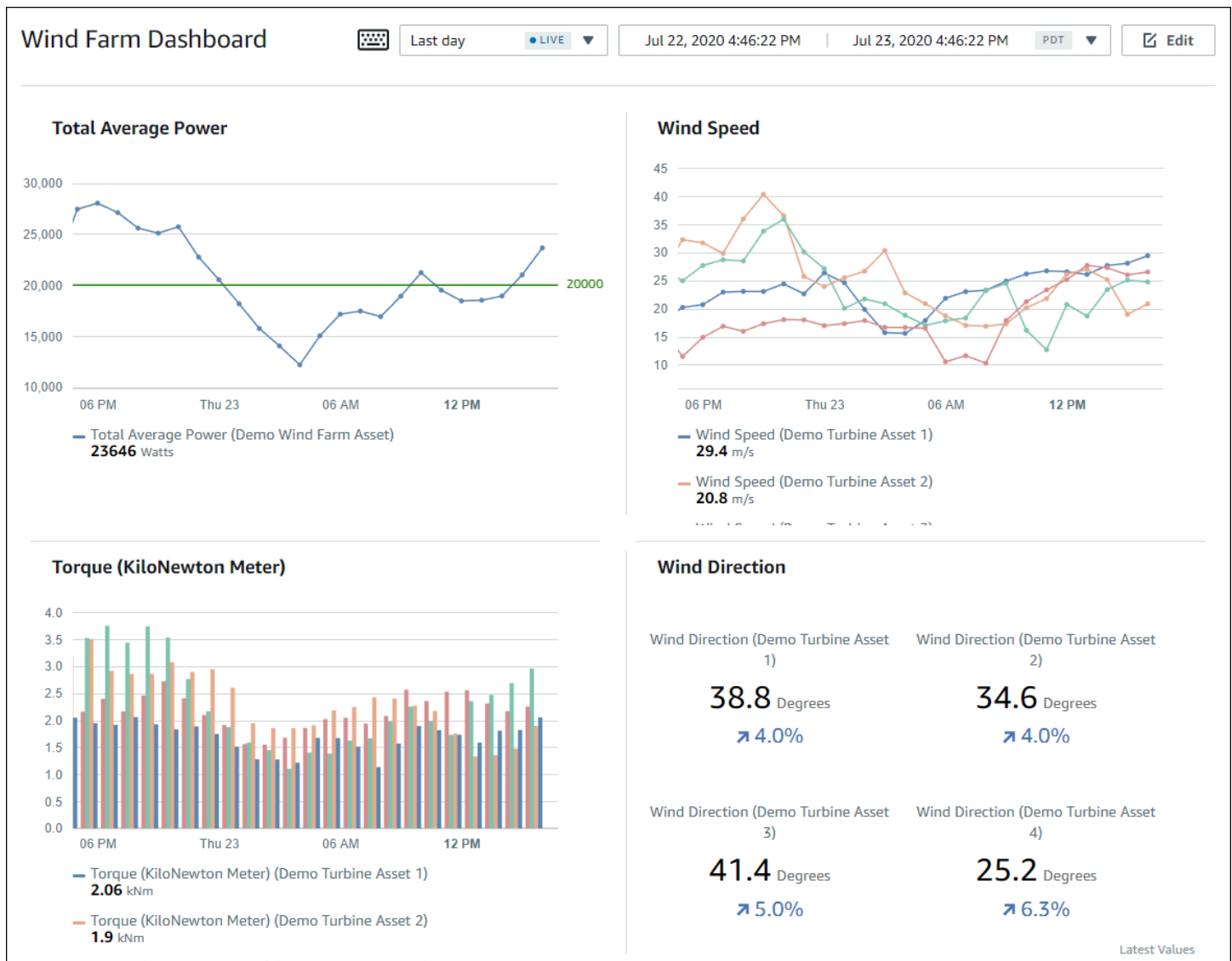
Consulte [Exemplos de perguntas para fazer ao AWS IoT SiteWise Assistente](#) para saber mais sobre como consultar o AWS IoT SiteWise Assistant.

Monitore 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

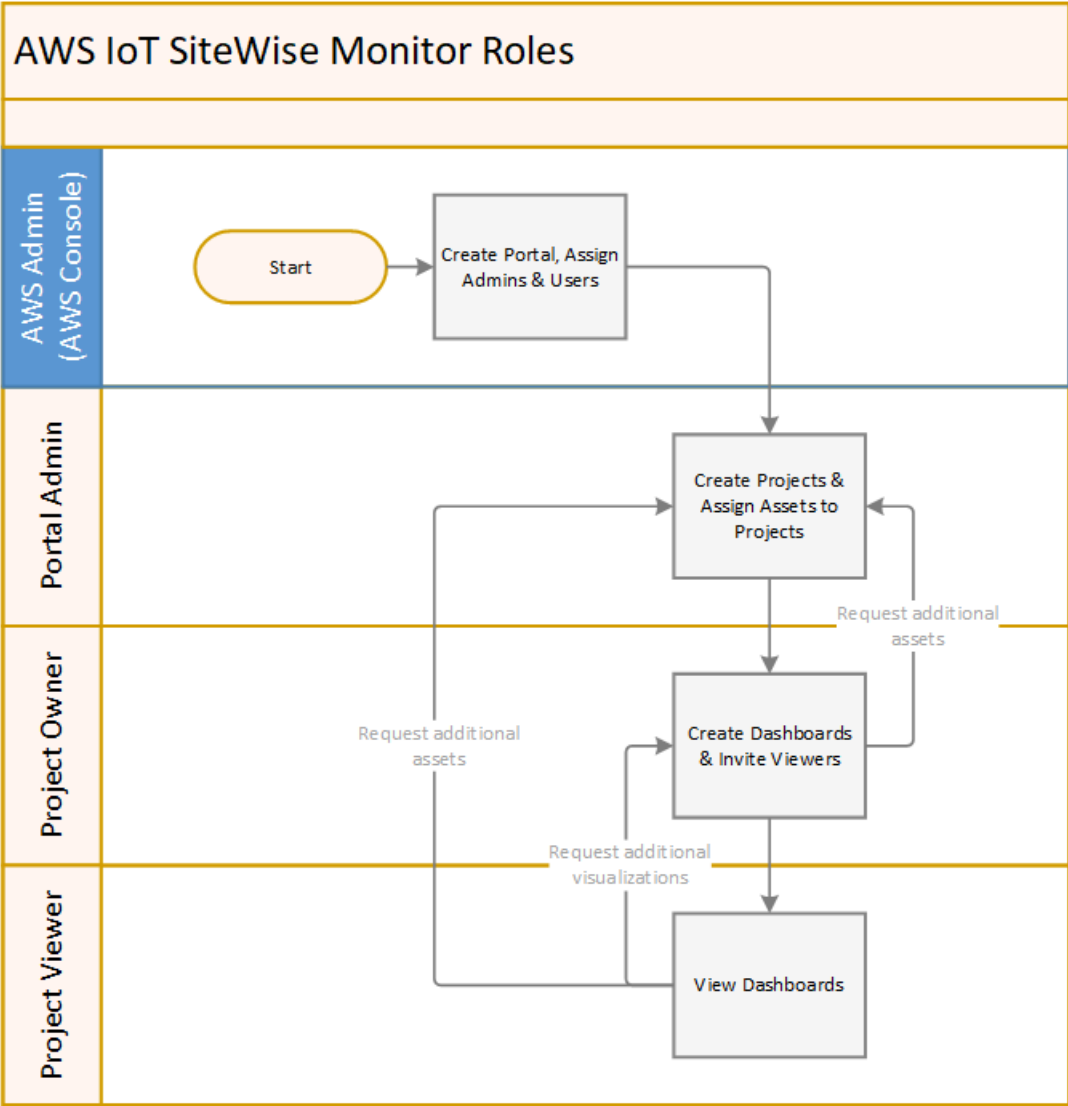
Cada projeto do SiteWise Monitor tem proprietários. Proprietários de projeto criam visualizações na forma de painéis para representar dados operacionais de forma consistente. Quando os painéis estiverem prontos para compartilhar, o proprietário de projeto pode convidar visualizadores. Os proprietários 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 de projeto só podem visualizar painéis nos projetos aos quais possuem 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 pode acessar seus dados usando 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). SPs normalmente 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.

Centro de Identidade do IAM

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. Ao observar os painéis, os visualizadores 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 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.

Comece com AWS IoT SiteWise Monitor (Classic)

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 obter mais informações, consulte [Visualize e compartilhe dados de parques eólicos no Monitor SiteWise](#).

Tópicos

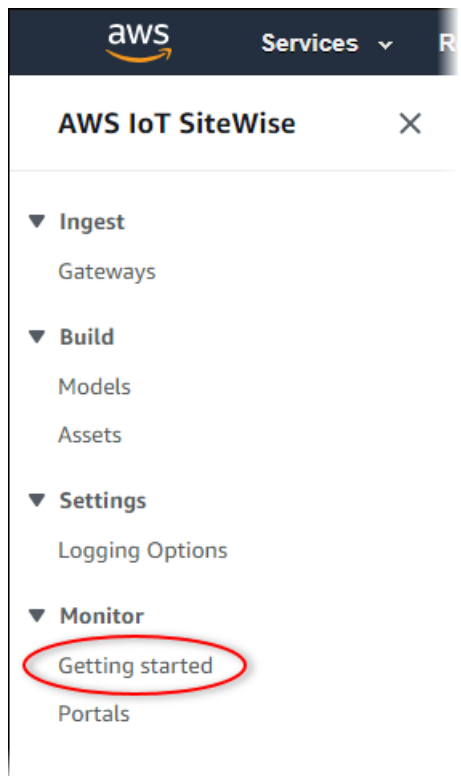
- [Crie um portal no SiteWise Monitor](#)
- [Configure seu portal no SiteWise Monitor](#)
- [Convide administradores no Monitor SiteWise](#)
- [Adicionar usuários do portal no SiteWise Monitor](#)
- [Crie AWS IoT SiteWise painéis \(AWS CLI\)](#)
- [Ative os alarmes para seus portais em AWS IoT SiteWise](#)
- [Habilitando seu AWS IoT SiteWise portal na borda](#)
- [Administre seus portais do SiteWise Monitor](#)

Crie um portal no SiteWise Monitor

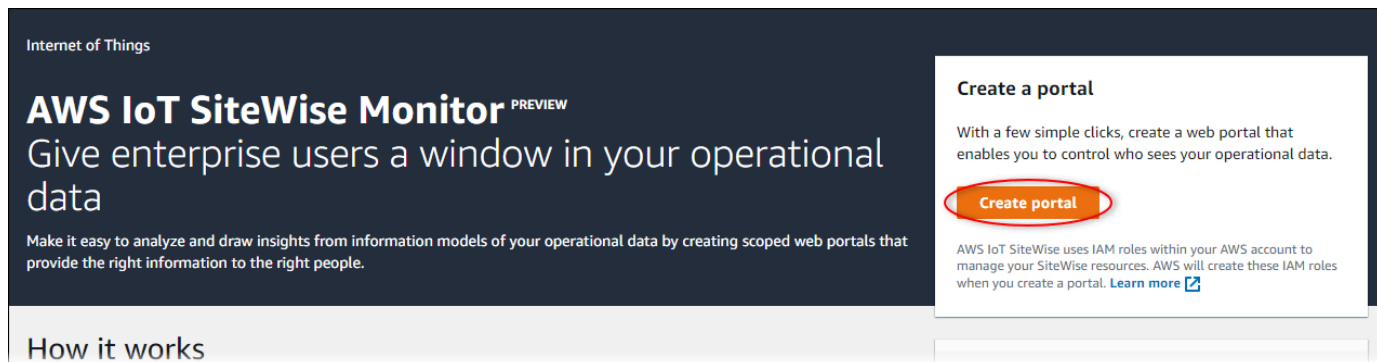
Você cria um portal SiteWise Monitor no AWS IoT SiteWise console.

Para criar um portal

1. Faça login no [console do AWS IoT SiteWise](#).
2. No painel de navegação, escolha Monitor, Conceitos básicos.



3. Escolha Criar Portal.



Depois, forneça algumas informações básicas para configurar o portal.

Configure seu portal no SiteWise Monitor

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 configurationStep 2- optional
Additional featuresStep 3
Invite administratorsStep 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.

Name should be 1-128 characters and only contain A-Z a-z 0-9 _ and -.

Description - optional

Create a description of your portal

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.

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.

☒ 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

Tags

This resource doesn't have any tags.

You can add up to 50 more tags.

Permissions

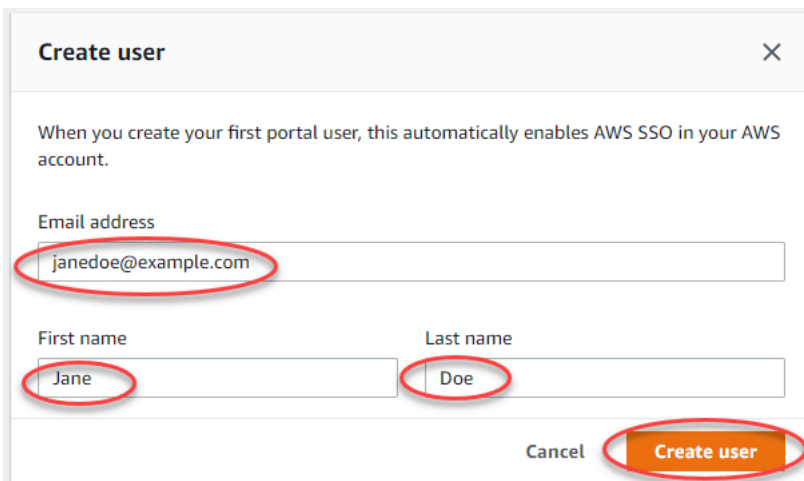
SiteWise Monitor assumes this role to give permissions to your federated users to access AWS IoT SiteWise resources. [Learn](#)

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.



Create user ✕

When you create your first portal user, this automatically enables AWS SSO in your AWS account.

Email address
janedoe@example.com

First name
Jane

Last name
Doe

Cancel Create user

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 obter mais informações, consulte [Marque seus AWS IoT SiteWise recursos](#).
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 obter mais informações, consulte [Use 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 obter mais informações, consulte [Ative os alarmes para seus portais em AWS IoT SiteWise](#).
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 obter mais informações, consulte [Adicionar ou remover administradores do portal no AWS IoT SiteWise](#). Se não quiser manter o portal, exclua-o para que ele não use recursos. Para obter mais informações, consulte [Excluir um portal no AWS IoT SiteWise](#).

A coluna de Status pode ser um dos valores a seguir:

- **CRIANDO** - 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.
- **PENDENTE** - 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.
- **EXCLUINDO** - 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.
- **FALHA** - 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.

A green banner with a white checkmark icon on the left and a white 'X' icon on the right. The text in the center reads: "Successfully created portal URL at https://a1b2c3d4-5678-90ab-cdef-1111EXAMPLE.app.iotsitewise.aws".

Successfully created portal URL at https://a1b2c3d4-5678-90ab-cdef-1111EXAMPLE.app.iotsitewise.aws

Depois, convide um ou mais administradores de portal para o portal. Até agora, você criou um portal, mas ninguém pode acessá-lo.

Convide administradores no Monitor SiteWise

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 obter 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 obter mais informações, consulte [Adicionar ou remover administradores do portal no AWS IoT SiteWise](#).

 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 do portal no SiteWise Monitor

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 usuários da lista de Usuários para adicionar 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.

AWS IoT SiteWise > Monitor > Portals > Create portal

Step 1
Portal configuration

Step 2
Invite administrators

Step 3
Assign users

Assign users

Select the users you want to be able to access and view this portal. Portal administrators will send invitations to these users at a later date. [Learn more](#)

Users (2) Create user

Find resources

	Display name	Email
☐	Jane Doe	janedoe@example.com
☒	John Doe	johndoe@example.com

Selected users (1)

Cancel Previous **Assign users**

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 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.

AWS IoT SiteWise > Monitor > Portals > Create portal

Step 1
Portal configuration

Step 2
[Invite administrators](#)

Step 3
Assign users

Assign users

Select the users you want to be able to access and view this portal. Portal administrators will send invitations to these users at a later date. [Learn more](#)

Users Roles

IAM users (1) [Manage users in IAM console](#)

☒

Name

▼

Date created

▼

☒

raspberrypi-testing

11-08-2019

► Portal users (1) [Remove](#)

Cancel Previous **Assign users**

AWS IoT SiteWise > Monitor > Portals > Create portal

Step 1
Portal configuration

Step 2
Invite administrators

Step 3
Assign users

Assign users

Select the users you want to be able to access and view this portal. Portal administrators will send invitations to these users at a later date. [Learn more](#)

Users **Roles**

IAM roles (66) [Manage roles in IAM console](#)

Find role name

	Name	Date created
☐	[REDACTED]	
☐	[REDACTED]	
☒	AWSIoTSiteWiseMonitorServiceRole_4wZigNpA1	03-16-2021
☐	AWSIoTSiteWiseMonitorServiceRole_ECKT-2Oar	03-11-2021
☐	AWSIoTSiteWiseMonitorServiceRole_GTnd004Wr	03-16-2021
☐	AWSIoTSiteWiseMonitorServiceRole_rHINLNCS-	03-11-2021
☐	AWSIoTSiteWiseMonitorServiceRole_XB330QUIO	03-10-2021
☐	[REDACTED]	
☐	[REDACTED]	
☐	[REDACTED]	

► Portal users (2) [Remove](#)

Cancel Previous **Assign users**

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 obter mais informações, consulte [Adicionar ou remover usuários do portal no AWS IoT SiteWise](#).

Se precisar fazer alterações no portal, consulte [Administre seus portais do SiteWise Monitor](#).

Para começar no portal, consulte [Introdução](#) no Guia de Aplicação do SiteWise Monitor.

Crie AWS IoT SiteWise painéis ()AWS CLI

Ao definir visualizações (ou widgets) em painéis usando o AWS CLI, você deve especificar as seguintes informações no dashboardDefinition documento JSON. Essa definição é um parâmetro das [UpdateDashboard](#) operações [CreateDashboard](#).

widgets

Uma lista de estruturas de definição de widget que contêm as seguintes informações:

type

O tipo de widget. 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 dessa métrica. AWS IoT SiteWise fornece os seguintes tipos de métricas:

- `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. O padrão é `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. O padrão é `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. O padrão é `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-eeeeeeEXAMPLE \  
  --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"
  }
]
}
]
```

Ative os alarmes para seus portais em AWS IoT SiteWise

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 recursos adicionais. Com base no serviço de autenticação do usuário, selecione uma das opções a seguir:

IAM Identity Center

[AWS IoT SiteWise](#) > [Monitor](#) > [Portals](#) > Create portal

Step 1
Portal configuration

Step 2 - optional
Additional features

Step 3
Invite administrators

Step 4
Assign users

Additional features - *optional*

Alarms

Your portal users can create alarms in the portal to monitor equipment or processes. They can also get notified when the equipment or processes perform outside specified range.

☒ **Enable alarms**
If enabled, your portal users can define AWS IoT Events alarms in SiteWise Monitor.

AWS IoT SiteWise access role
Choose an IAM role that allows AWS IoT Events to send data to AWS IoT SiteWise. To edit the role, go to the [IAM console](#).

☒ Create a role from an AWS managed template

☐ Use an existing role

☒ **Enable alarm notifications**
If enabled, alarms can send email or SMS notifications.

Sender
Specify the email address that sends alarm notifications. To edit or add a sender, go to the [Amazon SES console](#).

AWS Lambda role
Choose an IAM role that allows AWS Lambda to send data to Amazon SES and Amazon SNS. To edit the role, go to the [IAM console](#).

☒ Create a role from an AWS managed template

☐ Use an existing role

AWS Lambda function
Choose an AWS Lambda function to manage alarm notifications. To edit the function, go to the [AWS Lambda console](#).

☒ Create a lambda from an AWS managed template

☐ Use an existing lambda

[Previous](#) [Create](#)

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 `ss-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

AWS IoT SiteWise > Monitor > Portals > Create portal

Step 1
Portal configuration

Step 2- optional
Additional features

Step 3
Invite administrators

Step 4
Assign users

Additional features - optional

Alarms

Your portal users can create alarms in the portal to monitor equipment or processes. They can also get notified when the equipment or processes perform outside specified range.

☒ **Enable alarms**
If enabled, your portal users can define AWS IoT Events alarms in SiteWise Monitor.

AWS IoT SiteWise access role
Choose an IAM role that allows AWS IoT Events to send data to AWS IoT SiteWise. To edit the role, go to the [IAM console](#).

☒ Create a role from an AWS managed template

☐ Use an existing role

ⓘ Alarms created in the portal can't send notifications. If you want to send alarm notifications, choose **Previous**. Then, on the **Portal configuration** page, choose **AWS SSO for User authentication**.

Previous **Create**

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.

Habilitando seu AWS IoT SiteWise 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.

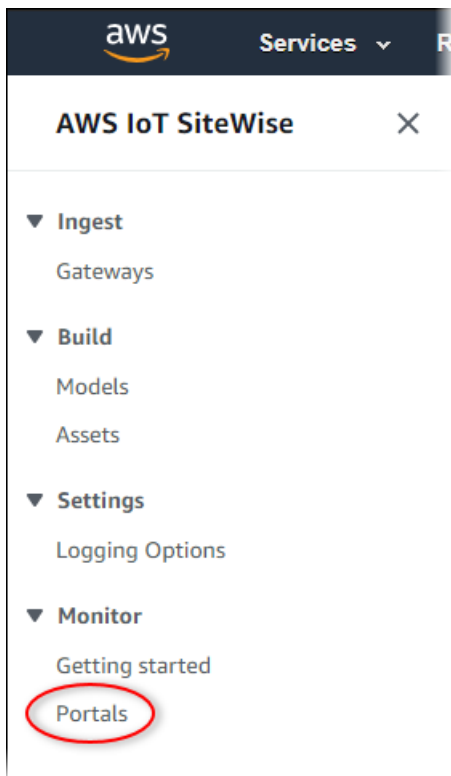
Para habilitar o portal na borda

1. Na seção Configuração de borda, ative Habilitar este portal na borda.
2. Escolha Criar.

Administre seus portais do SiteWise Monitor

Você tem a capacidade de gerenciar e configurar vários aspectos do portal. Isso inclui adicionar e remover usuários ou administradores, definir permissões e perfis de usuário, personalizar o URL e o nome do portal, definir informações de contato de suporte e enviar convites por e-mail para administradores do portal.

1. Faça login no [console do AWS IoT SiteWise](#).
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 detalhes do portal em AWS IoT SiteWise](#)
 - [Adicionar ou remover administradores do portal no AWS IoT SiteWise](#)
 - [Enviar convites por e-mail para administradores do portal](#)
 - [Adicionar ou remover usuários do portal no AWS IoT SiteWise](#)
 - [Excluir um portal no AWS IoT SiteWise](#)

Para obter informações sobre como criar um portal, consulte [Comece com AWS IoT SiteWise Monitor \(Classic\)](#).

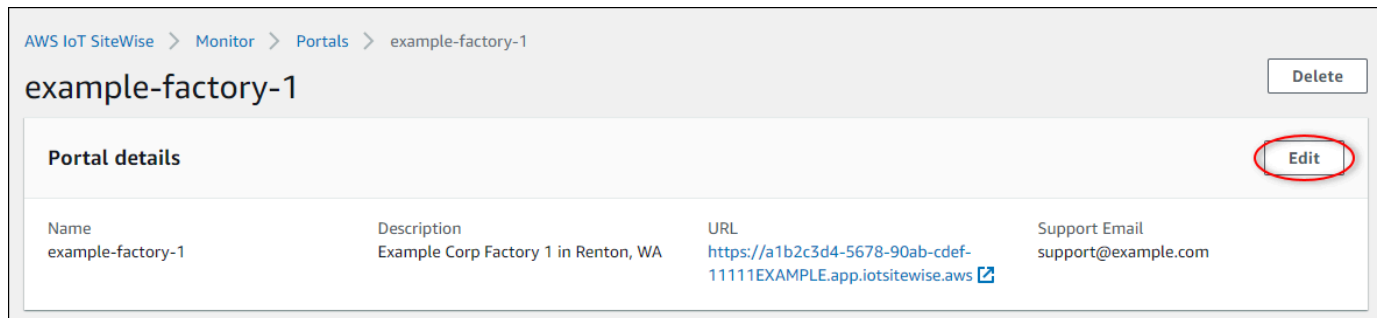
Tópicos

- [Alterar detalhes do portal em AWS IoT SiteWise](#)
- [Adicionar ou remover administradores do portal no AWS IoT SiteWise](#)
- [Enviar convites por e-mail para administradores do portal](#)
- [Adicionar ou remover usuários do portal no AWS IoT SiteWise](#)
- [Excluir um portal no AWS IoT SiteWise](#)

Alterar detalhes do portal em AWS IoT SiteWise

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.

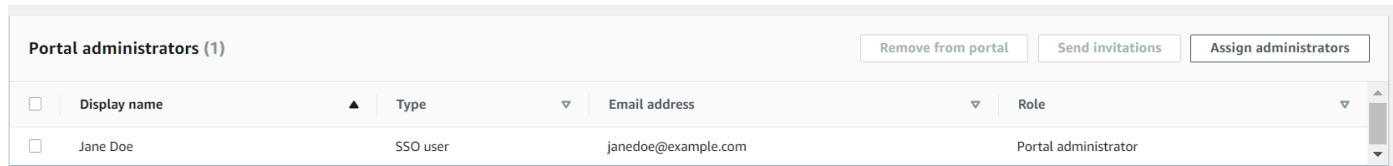


2. Atualize o Nome, a Descrição, a Marca do portal, o E-mail de contato do suporte ou as Permissões.
3. Ao terminar, escolha Salvar.

Adicionar ou remover administradores do portal no AWS IoT SiteWise

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.

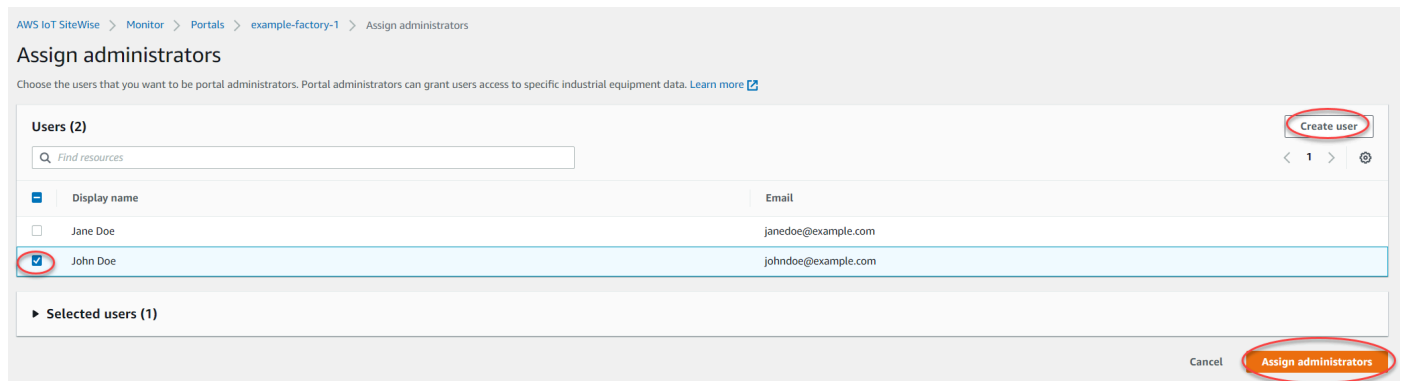


Note

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

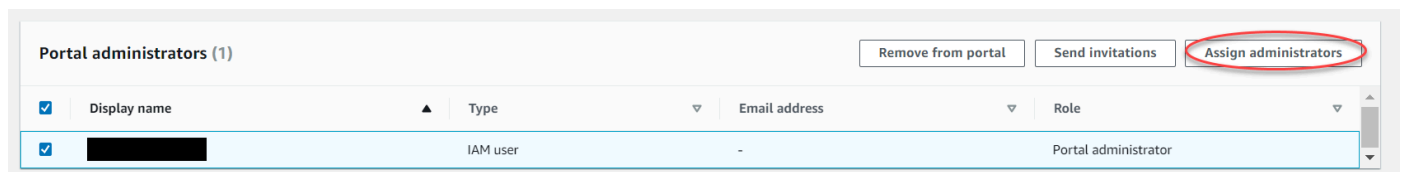
- Na página de detalhes do portal, na seção Administradores do portal, marque a caixa de seleção dos usuários a serem removidos e escolha Remover do portal.



Note

Recomendamos que você selecione pelo menos um administrador do portal.

IAM



Como adicionar administradores do portal

- Na página de detalhes do portal, na seção Administradores do portal, selecione Atribuir usuários.
- 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.

AWS IoT SiteWise > Monitor > Portals > example-factory-2 > Assign administrators

Assign administrators

Choose the users that you want to be portal administrators. Portal administrators can grant users access to specific industrial equipment data. [Learn more](#)

 IAM users or roles must have the `iotsitewise:DescribePortal` permission to sign in to the portal.

Users

Roles

IAM users (1)

Manage users in IAM console

< 1 >

☒	Name	Date created
☒	raspberrypi-testing	11-08-2019

► Portal administrators (1)

Remove

Cancel

Assign administrators

AWS IoT SiteWise > Monitor > Portals > example-factory-2 > Assign administrators

Assign administrators

Choose the users that you want to be portal administrators. Portal administrators can grant users access to specific industrial equipment data. [Learn more](#)

① IAM users or roles must have the `iot:DescribePortal` permission to sign in to the portal.

Users **Roles**

IAM roles (66) [Manage roles in IAM console](#)

Find role name

	Name	Date created
☐	[REDACTED]	
☒	AWSIoTSiteWiseMonitorServiceRole_4wZigNpA1	03-16-2021
☐	AWSIoTSiteWiseMonitorServiceRole_ECKT-2Oar	03-11-2021
☐	AWSIoTSiteWiseMonitorServiceRole_GTnd0O4Wr	03-16-2021
☐	AWSIoTSiteWiseMonitorServiceRole_rHINLNCs-	03-11-2021
☐	AWSIoTSiteWiseMonitorServiceRole_XB330QUIO	03-10-2021
☐	[REDACTED]	
☐	[REDACTED]	
☐	[REDACTED]	

► Portal administrators (2) Remove

Cancel **Assign administrators**

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.

- Na página de detalhes do portal, na seção Administradores do portal marque as caixas de seleção dos administradores do portal.

Portal administrators (1) Remove from portal **Send invitations** Assign users

☒	Display name	Email address	Role
☒	John Doe	john.doe@example.com	Portal administrator

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 no AWS IoT SiteWise

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

Portal users (1)					Remove from portal Assign users	
☐	Display name	Type	Email address	Role		
☐	John Doe	SSO user	johndoe@example.com	Portal viewer		

Como adicionar usuários do portal

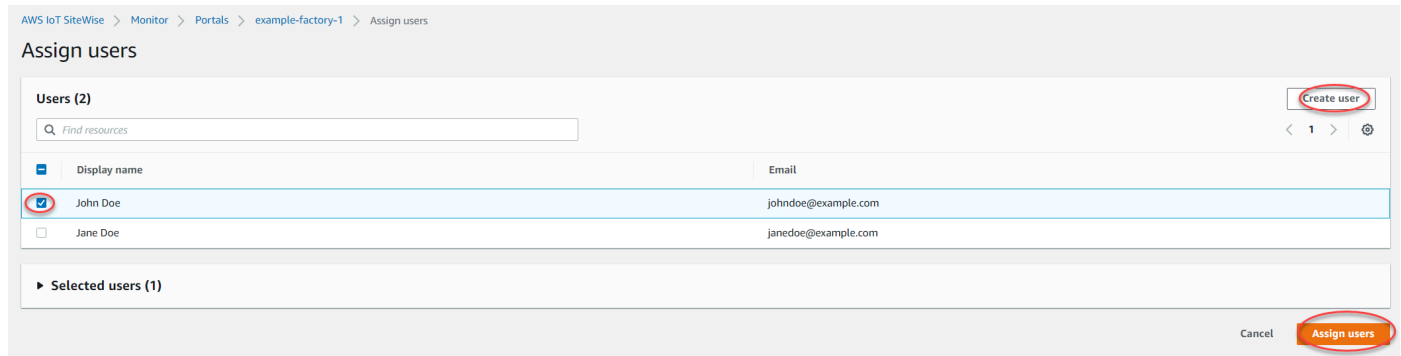
1. Na página de detalhes do portal, na seção Usuários do portal, selecione Atribuir usuários.
2. Na página Atribuir usuários, marque a caixa de seleção dos usuários a serem adicionados ao portal.

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](#).

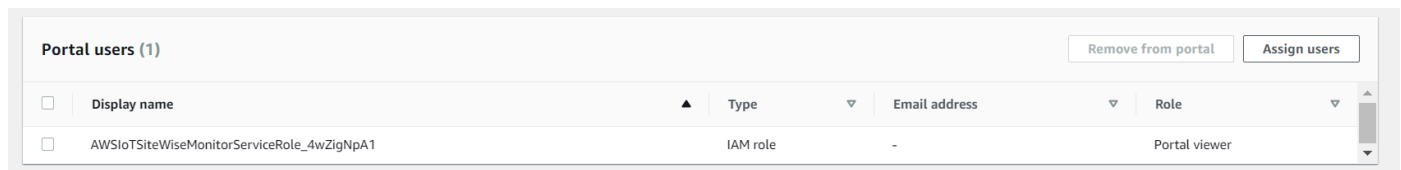
3. Escolha Atribuir usuários.



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

- Na página de detalhes do portal, na seção Usuários do portal, selecione Atribuir usuários.
- 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 seu usuário do portal.
- 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.
- Escolha Atribuir usuários.

AWS IoT SiteWise > Monitor > Portals > example-factory-2 > Assign users

Assign users

Users Roles

IAM users (1) [Manage users in IAM console](#)

Find user name

< 1 >

☒	Name	Date created
☒	[REDACTED]	11-08-2019

► Portal users (1) [Remove](#)

Cancel [Assign users](#)

AWS IoT SiteWise > Monitor > Portals > example-factory-2 > Assign users

Assign users

Users **Roles**

IAM roles (66) [Manage roles in IAM console](#)

Find role name

< 1 2 3 4 5 6 7 >

☐	Name	Date created
☐	[REDACTED]	
☒	AWSIoTSiteWiseMonitorServiceRole_4wZigNpA1	03-16-2021
☐	AWSIoTSiteWiseMonitorServiceRole_ECKT-2Oar	03-11-2021
☐	AWSIoTSiteWiseMonitorServiceRole_GTnd0O4Wr	03-16-2021
☐	AWSIoTSiteWiseMonitorServiceRole_RHINLNC5-	03-11-2021
☐	AWSIoTSiteWiseMonitorServiceRole_XB33OQUIO	03-10-2021
☐	[REDACTED]	
☐	[REDACTED]	
☐	[REDACTED]	

► Portal users (2) [Remove](#)

Cancel [Assign users](#)

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 no AWS IoT SiteWise

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.

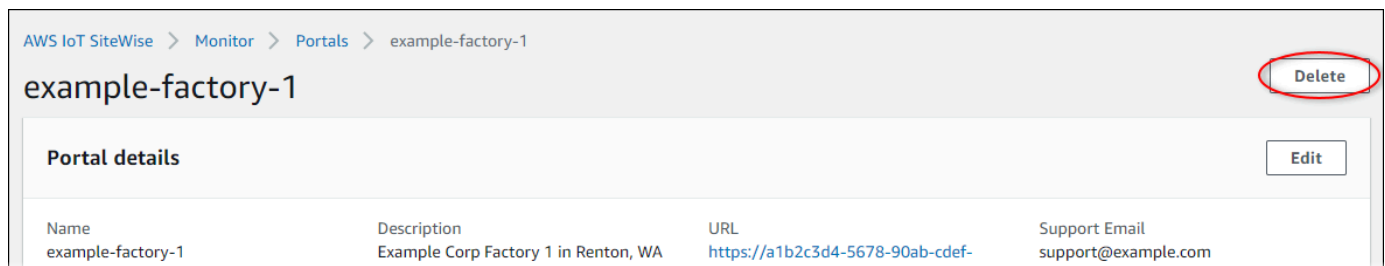
Note

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.

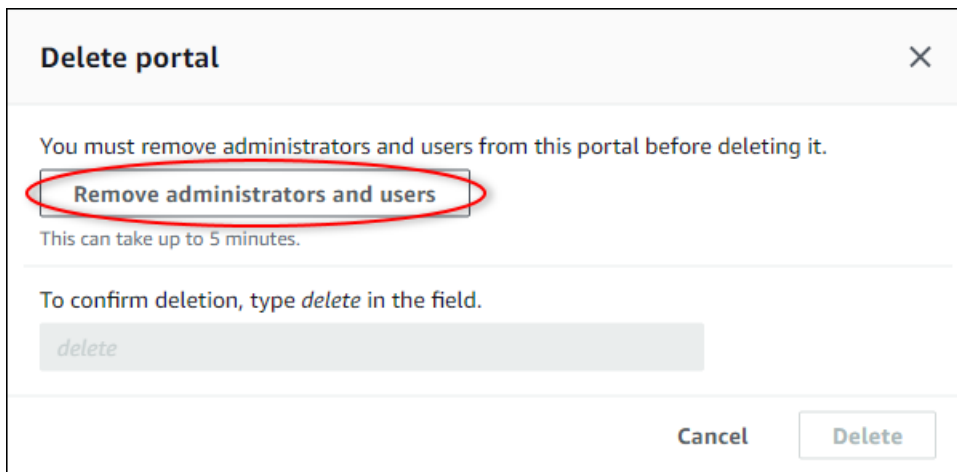
Important

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.

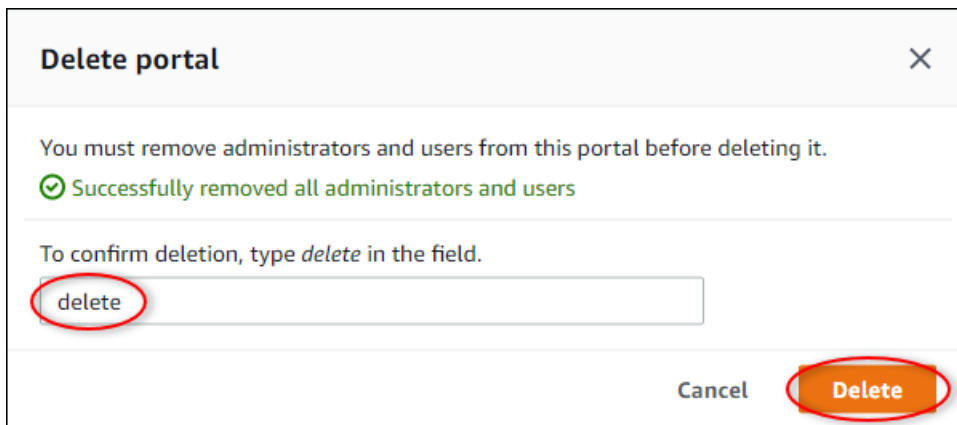


2. Na caixa de diálogo Excluir portais escolha Remover administradores e usuários.

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.

Comece a usar AWS IoT SiteWise Monitor (com reconhecimento de IA) - pré-visualização

Como AWS administrador da sua organização, você pode criar portais a partir do AWS IoT SiteWise console, permitindo que os membros da sua organização visualizem seus AWS IoT SiteWise dados. Conclua as etapas a seguir para começar.

1. Configure e crie um portal.
2. Adicione administradores do portal e envie e-mails de convite.
3. Adicione usuários do portal.

Depois de criar um portal, o administrador do portal pode criar projetos e adicionar usuário ao projeto. Em seguida, os membros do projeto criam painéis para visualizar os dados conectados AWS IoT SiteWise, permitindo que monitorem o desempenho de seus dispositivos, processos e equipamentos conectados.

 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.

Crie projetos para compartilhar com suas equipes. Os proprietários do projeto podem então criar painéis para visualizar as propriedades dos ativos que ajudam os espectadores do projeto a entender o desempenho dos dispositivos, processos e equipamentos. Ele também fornece uma visão consistente das operações para suas equipes.

Os painéis ajudam a visualizar e entender os dados do seu projeto. Ele ajuda empresas e usuários de aplicativos a acompanhar seus AWS IoT dispositivos e dados. Escolha um tipo de visualização que melhor exiba seus dados de acordo com suas necessidades. Reorganize e redimensione as visualizações para criar um layout adequado à sua equipe. Explore seus ativos e dados de dispositivos, processos e equipamentos, identifique problemas rapidamente e melhore a eficiência operacional.

Tópicos

- [Criar um portal](#)
- [Configurar o portal do](#)
- [Administrar portais](#)
- [Excluir um portal](#)
- [Crie painéis com AWS CLI](#)
- [Login do portal](#)
- [Criar um projeto](#)
- [Atualizar um projeto](#)
- [Excluir um projeto](#)
- [Criar um painel](#)

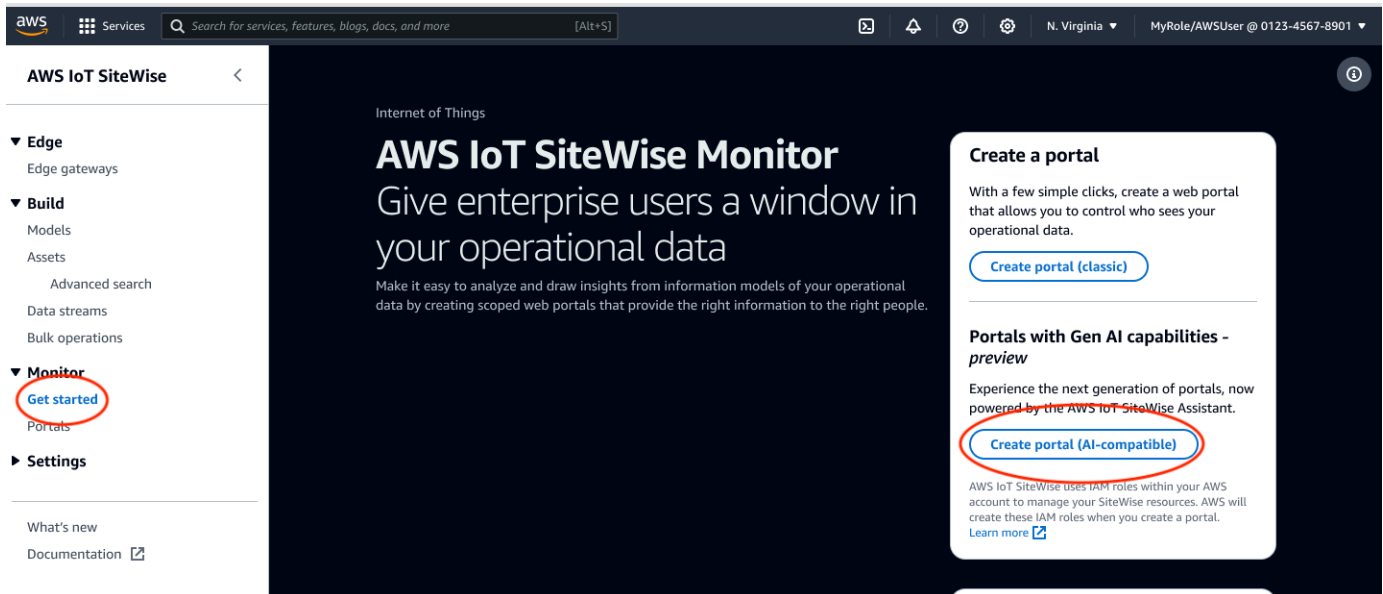
- [Atualizar um painel](#)
- [Excluir um painel](#)
- [Configurar painel](#)

Criar um portal

Você cria um portal SiteWise Monitor no AWS IoT SiteWise console.

Para criar um portal

1. Faça login no [console do AWS IoT SiteWise](#).
2. No painel de navegação, escolha Monitor, Começar.
3. Escolha Criar portal (compatível com IA).



Depois, forneça algumas informações básicas para configurar o portal.

Configurar o portal do

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.

Etapas para 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. Insira um endereço de e-mail na caixa de e-mail de contato do Support para problemas de suporte.
5. Na caixa Autenticação do usuário, escolha a seguinte opção:
 - 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

O suporte para credenciais do IAM estará disponível em breve.

6. Escolha uma das seguintes opções na seção Acesso ao serviço:
 - 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 obter mais informações, consulte [Use funções de serviço para AWS IoT SiteWise Monitor](#).
 - Escolha Usar um perfil existente e escolha o perfil de serviço alvo.
7. Escolha ativar o AWS IoT SiteWise Assistente para este portal. O AWS IoT SiteWise Assistente fornece análise rápida de dados, insights em tempo real e recomendações guiadas.

 Note

A ativação do AWS IoT SiteWise Assistente acarretará custos. Para usar soluções e orientações de conhecimento em nível empresarial, você deve ter um conjunto de dados associado ao índice Amazon Kendra.

8. (Opcional) Adicione tags ao seu portal. Para obter mais informações, consulte [Marque seus AWS IoT SiteWise recursos](#).
9. Escolha Criar portal. AWS IoT SiteWise criará seu portal.

 Note

Se fechar o console, você poderá concluir o processo de configuração adicionando administradores e usuários. Para obter mais informações, consulte [Adicionar ou remover administradores de portal](#). Se não quiser manter o portal, exclua-o para que ele não use recursos. Para obter mais informações, consulte [Excluir um portal](#).

Uma mensagem será exibida quando o portal for criado.

Successfully created portal "example portal".

AWS IoT SiteWise > Monitor > Portals > example portal

example portal

Edit

Delete

Open portal

Portal details

Name example portal	Status  Active	URL  https://p-jfnlf2d8.gamma.iotsitewise.aws
Type AI-compatible	AWS IoT SiteWise Assistant  Disabled	Portal branding -
Description -	Last updated November 1, 2024, 15:37 (UTC-07:00)	Support contact email myemail@mycompany.com
ID f5fc93a1-011c-4c5a-81a6-e001b50d2547	Date created November 1, 2024, 15:37 (UTC-07:00)	

Depois que um portal é criado, ele é listado na seção Portais. A seção Detalhes do portal lista o nome, descrição, ID, URL, status, datas da última atualização e criação, identidade visual do portal e e-mail de suporte para cada portal.

A coluna de Status pode ser um dos valores a seguir:

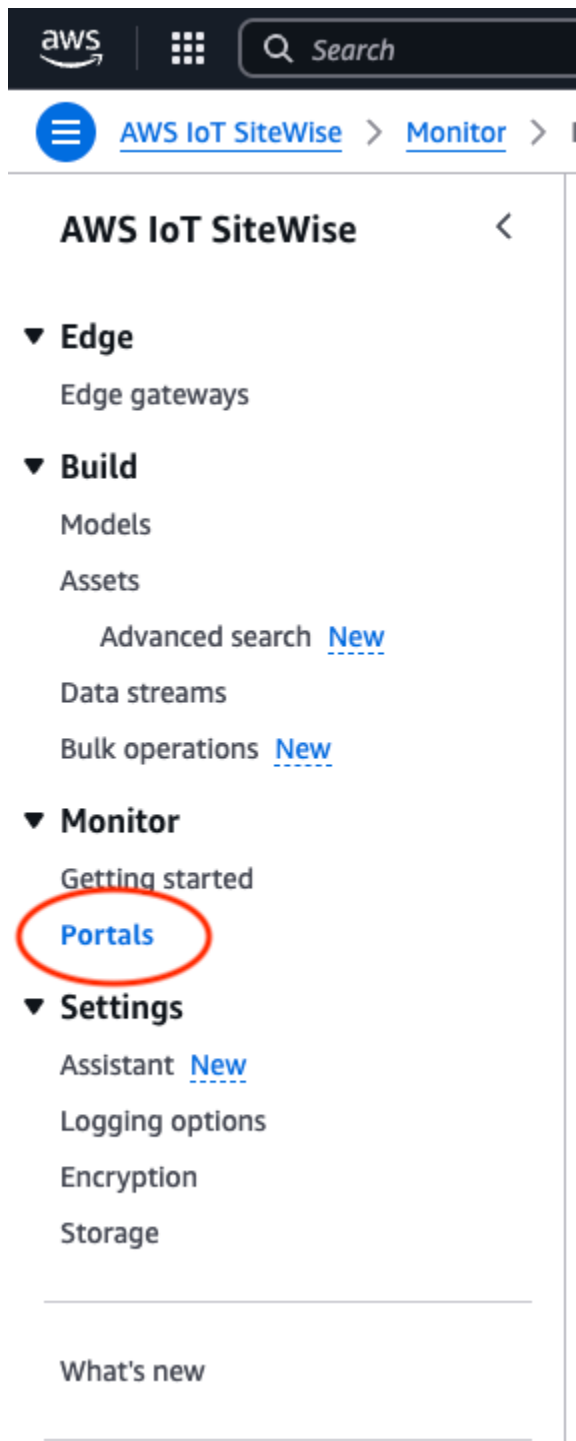
- CREATING - AWS IoT SiteWise está processando sua solicitação para criar o portal. O processo pode demorar vários minutos para ser concluído.
- ATUALIZANDO - AWS IoT SiteWise está processando sua solicitação para atualizar o portal. O processo pode demorar vários minutos para ser concluído.

- **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](#).

Administrar portais

Você tem a capacidade de gerenciar e configurar vários aspectos do portal. Isso inclui adicionar e remover administradores, definir permissões e funções, personalizar o nome, a descrição, configurar o e-mail de suporte e convidar administradores do portal.

1. Faça login no [console do AWS IoT SiteWise](#).
2. No painel de navegação, escolha Monitorar, Portais.



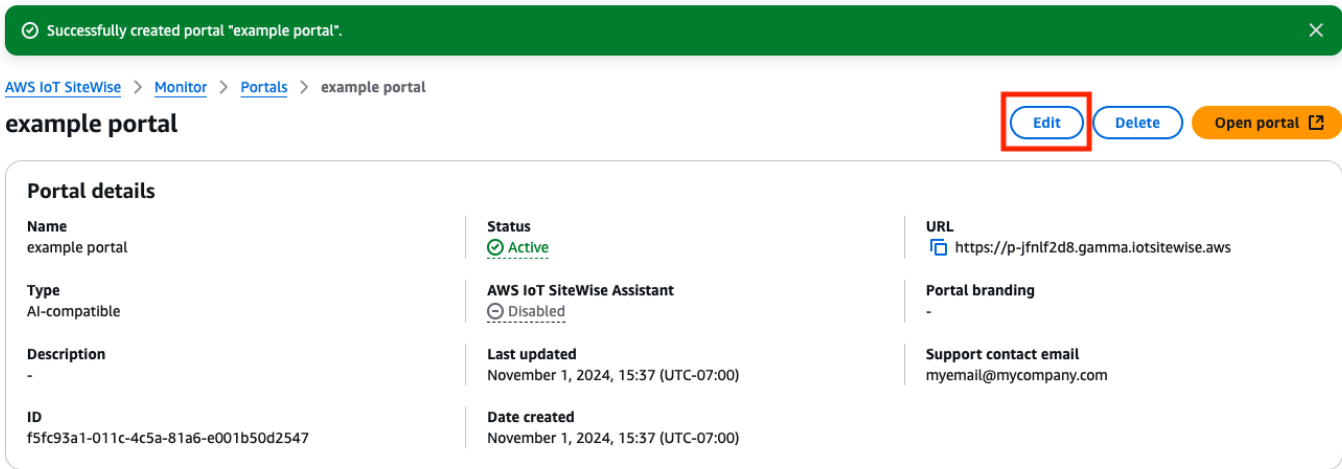
3. Escolha um portal e, em seguida, escolha Abrir portal (ou escolha o Nome do portal).
4. Você pode executar qualquer uma das seguintes tarefas administrativas:
 - [Editar atributos do portal](#)
 - [Adicionar ou remover administradores de portal](#)

- [Enviar convites por e-mail para administradores do portal](#)
- [Excluir um portal no AWS IoT SiteWise](#)

Editar atributos do portal

Você pode alterar o nome, a descrição, a identidade visual, o e-mail de suporte e o acesso ao serviço de um portal.

1. Na página de detalhes do portal, na seção Detalhes do portal escolha Editar.

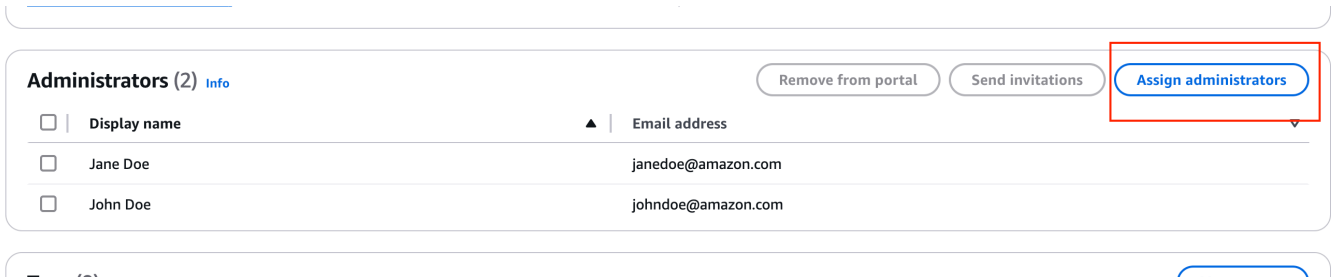


2. Atualize o nome, a descrição, a marca do portal, o e-mail de contato do Support, o acesso ao AWS IoT SiteWise Assistente ou ao Serviço.
3. Ao concluir, escolha Salvar alterações.

Adicionar ou remover administradores de 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, escolha Atribuir administradores.
2. Na página Atribuir administradores, selecione 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.

Assign administrators [Info](#)

Choose portal administrators from the users list. Portal administrators grant access to specific industrial equipment data. [Learn more](#)

Users (11) Create user

X 2 matches < 1 > ⚙

☐	Name	Email
☒	johndoe@amazon.com	johndoe@amazon.com
☐	janedoe@amazon.com	janedoe@amazon.com

Cancel Assign administrators

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

O campo Administradores (#) lista o número de administradores do portal. Você pode adicionar vários administradores do portal para gerenciar e trabalhar em projetos.

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, 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.

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.

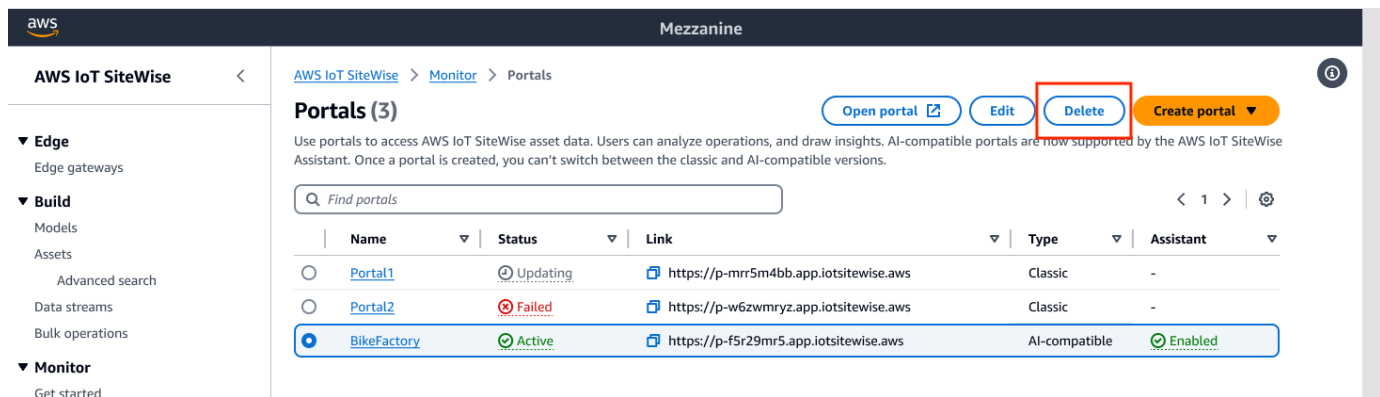
Note

Primeiro, é necessário excluir manualmente todos os painéis e projetos em um portal antes de excluí-lo.

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 portal, 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 **confirm** no campo para confirmar a exclusão.
4. Escolha Excluir.

Crie painéis com AWS CLI

Ao definir visualizações (ou widgets) em painéis usando o AWS CLI, você deve especificar as seguintes informações no `dashboardDefinition` documento JSON. Essa definição é um parâmetro das [UpdateDashboard](#) operações [CreateDashboard](#).

displaySettings

As configurações de exibição com os seguintes parâmetros:

- `numRows`— Número de linhas no layout do painel. Cada linha tem a largura de `CellSize`.
- `numColumns`— Número de colunas no layout do painel. Cada coluna tem a largura de `CellSize`.
- `cellSize`— (Opcional) O tamanho de uma célula no layout em pixels. Deve ser um número positivo. O padrão é 10.
- `significantDigits`— (Opcional) Número de dígitos significativos a serem exibidos no painel. O padrão é 4.

querySettings

As informações da consulta com o seguinte parâmetro:

- **refreshRate**— (Opcional) A taxa na qual os dados são atualizados em milissegundos. Aceita os seguintes valores - 1000, 5000, 10000, 60000, 300000.

defaultViewport

Se não for fornecido, o padrão é os últimos cinco minutos. Contém os seguintes parâmetros:

- **duration**— (Opcional) Determina até que ponto no passado consultar dados a partir do momento presente.
- **start**— (Opcional) É do tipo Data. O intervalo de horário de início para consultar dados. Precisa de uma end data especificada.
- **end**— (Opcional) É do tipo Data. O intervalo de tempo de término para consultar dados. Precisa de uma start data especificada.

widgets

Uma lista de estruturas de definição de widgets que contêm as seguintes informações:

type

O tipo de widget. AWS IoT SiteWise fornece os seguintes tipos de widget:

- **xy-plot**— Um gráfico de linhas ou um gráfico de dispersão, dependendo da configuração.
- **bar-chart**: um gráfico de barras.
- **kpi-chart**— Um gráfico de indicadores-chave de desempenho.
- **status-timeline**— Um widget de status que visualiza e navega pelos dados de séries temporais de uma ou mais fontes de dados.
- **text**— Um widget de texto.
- **table**: um widget de tabela.

id

Um identificador exclusivo para o widget.

x

A posição horizontal do widget, começando pela esquerda do painel. Esse valor se refere à posição do widget na grade do painel.

y

A posição vertical do widget, começando pela parte superior do painel. Esse valor se refere à posição do widget na grade do painel.

z

A ordem relativa dos widgets. Um widget de valor Z maior é exibido na frente do widget de valor Z inferior, se eles se sobreporem.

width

A largura do widget, expressa em número de células no painel.

height

A altura do widget, expressa em número de células no painel.

properties

Uma lista das propriedades do widget. Isso varia de acordo com o tipo de widget. Consulte o [IoT App Kit para obter detalhes](#).

Exemplo 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-eeeeeeEXAMPLE \  
  --dashboard-name "Example 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:

```
{  
  "displaySettings": {  
    "numColumns": 200,  
    "numRows": 1000,
```

```

    "cellSize": 20,
    "significantDigits": 4
  },
  "widgets": [{
    "id": "0t73JcxUoc6oEXAMPLE",
    "type": "xy-plot",
    "width": 33,
    "height": 20,
    "x": 0,
    "y": 0,
    "z": 0,
    "properties": {
      "aggregationType": "AVERAGE",
      "queryConfig": {
        "source": "iotsitewise",
        "query": {
          "assets": [{
            "assetId": "97c97abf-e883-47bb-a3f4-EXAMPLE",
            "properties": [{
              "propertyId": "97cc61f4-57a4-4c5f-a82c-EXAMPLE",
              "refId": "692ce941-f3d9-4074-a297-EXAMPLE",
              "aggregationType": "AVERAGE",
              "color": "#7d2105",
              "resolution": "1m"
            }]
          }]
        },
        "properties": [],
        "assetModels": [],
        "alarms": [],
        "alarmModels": []
      }
    },
    "line": {
      "connectionStyle": "linear",
      "style": "solid"
    },
    "symbol": {
      "style": "filled-circle"
    },
    "axis": {
      "yVisible": true,
      "xVisible": true
    },
    "legend": {

```



```

        "visible": true,
        "position": "right",
        "width": "30%",
        "height": "30%",
        "visibleContent": {
            "unit": true,
            "asset": true,
            "latestValue": true,
            "latestAlarmStateValue": true,
            "maxValue": false,
            "minValue": false
        }
    }
}
}, {
    "id": "fto7rF40Ny1EXAMPLE-G",
    "type": "bar-chart",
    "width": 33,
    "height": 20,
    "x": 0,
    "y": 20,
    "z": 0,
    "properties": {
        "aggregationType": "AVERAGE",
        "queryConfig": {
            "source": "iotsitewise",
            "query": {
                "assets": [{
                    "assetId": "97c97abf-e883-47bb-a3f4-EXAMPLE",
                    "properties": [{
                        "propertyId": "c84ca8f3-3dea-478a-afec-EXAMPLE",
                        "aggregationType": "AVERAGE",
                        "refId": "2960b958-2034-4d6e-bcc2-EXAMPLE"
                    }]
                }]
            },
            "properties": [],
            "assetModels": [],
            "alarms": [],
            "alarmModels": [],
            "requestSettings": {
                "aggregation": "AVERAGE"
            }
        }
    }
},

```

```

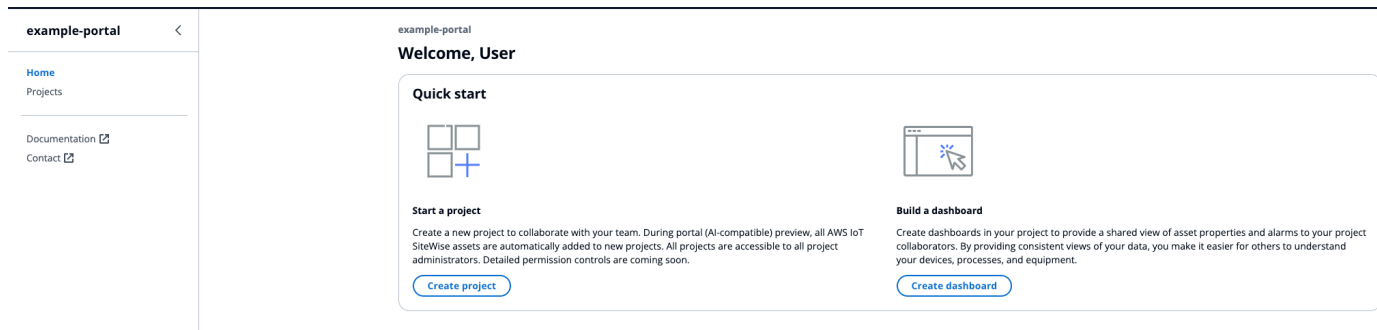
    "axis": {
      "showX": true,
      "showY": true
    },
    "styleSettings": {
      "2960b958-2034-4d6e-bcc2-360f1f02e505": {
        "color": "#7d2105"
      }
    }
  }
},
"querySettings": {
  "refreshRate": 5000
}
}

```

Login do portal

Login do usuário

1. No seu navegador, insira o URL do aplicativo.
2. Insira seu nome de usuário e senha e clique no botão Entrar.
3. Agora você está logado no aplicativo.



Criar um projeto

Criar um projeto

1. Um projeto é criado de duas maneiras:
 - a. Na página inicial, na seção Bem-vindo, em Início rápido, escolha Criar projeto.

- b. No painel de navegação esquerdo, escolha Projetos. Escolha Criar no canto superior direito para criar um projeto.
2. Na seção Criar projetos, insira o nome do projeto e forneça uma descrição opcional.
3. Escolha Criar.

example-portal

example-portal <

Home
Projects
Documentation
Contact

Home > Projects > Create

Create project

Create a project to host your dashboards.

Project name
Example project
The project name must contain from 1 and 256 characters. Character count: 15/256.

Project description - optional
An example project
The project description must contain from 1 and 2048 characters. Character count: 19/2048.

Cancel **Create**

Atualizar um projeto

Editar projeto

1. Escolha o botão Atualizar no canto superior direito da página do projeto para editar os detalhes do projeto.
2. Altere o nome do projeto editando o nome do projeto.
3. Altere a descrição do projeto editando os detalhes da descrição.
4. Selecione Atualizar para salvar suas alterações.

example-portal

example-portal <

Home
Projects
Documentation
Contact

Home > Projects > Example-project

Example-project

Delete **Update**

Project details

Description Example project	Creation date 10/25/2024, 11:17:28 AM	Last update date 10/25/2024, 11:17:28 AM

Dashboards

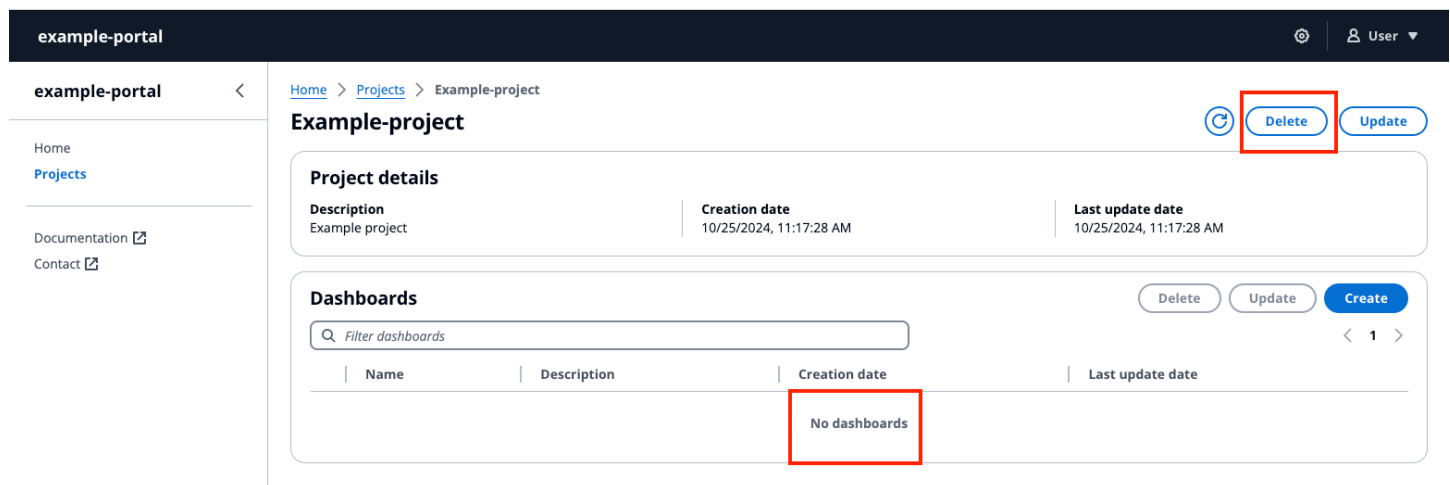
< 1 >

Name	Description	Creation date	Last update date
example dashboard	dashboard	10/25/2024, 11:17:52 AM	10/25/2024, 11:17:52 AM

Excluir um projeto

Excluir projeto

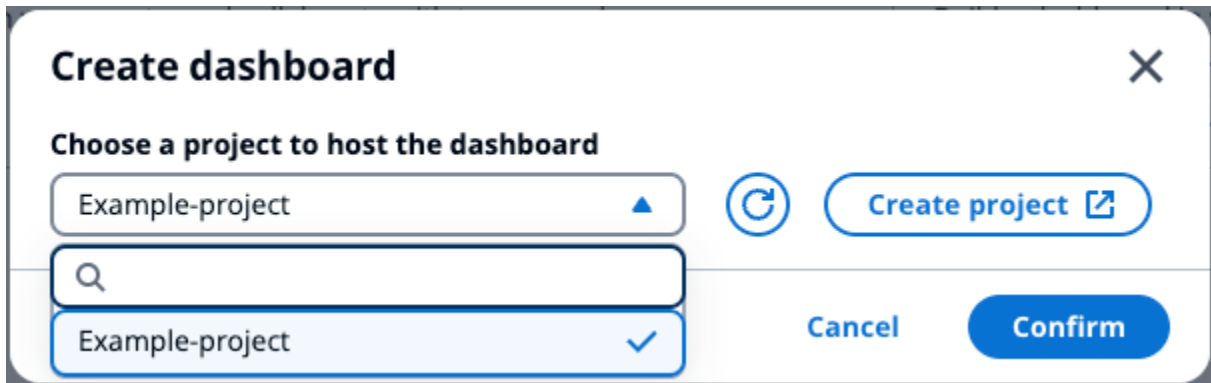
1. Você só pode excluir o projeto depois que todos os painéis do projeto forem excluídos.
2. Selecione o botão Excluir no canto superior direito da página do projeto.
3. Confirme novamente que você deseja excluir o projeto.
4. Selecione Excluir para excluir o projeto.



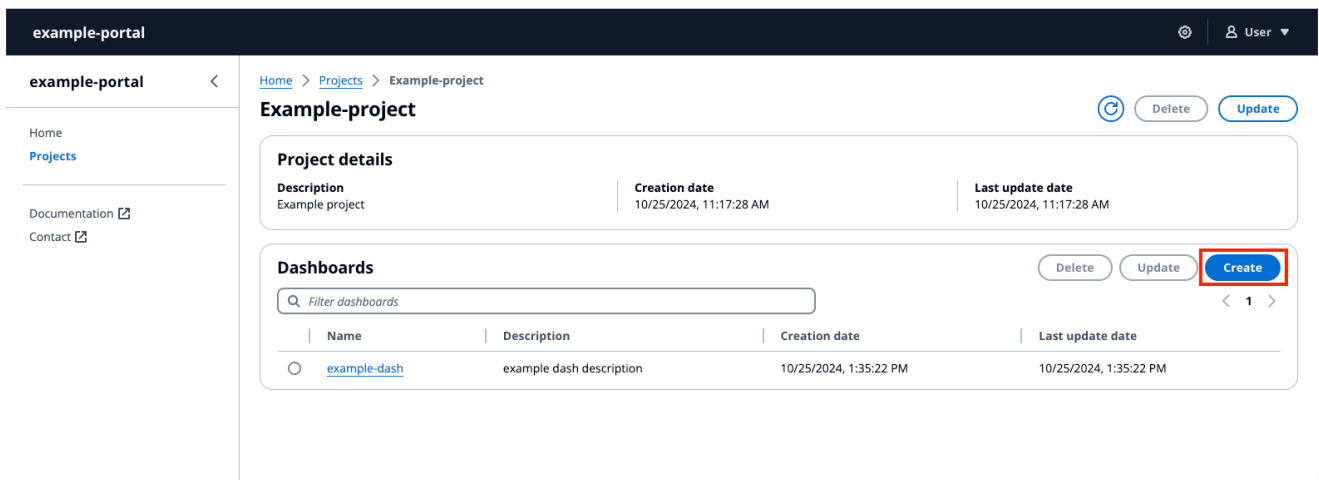
Criar um painel

Criar um painel

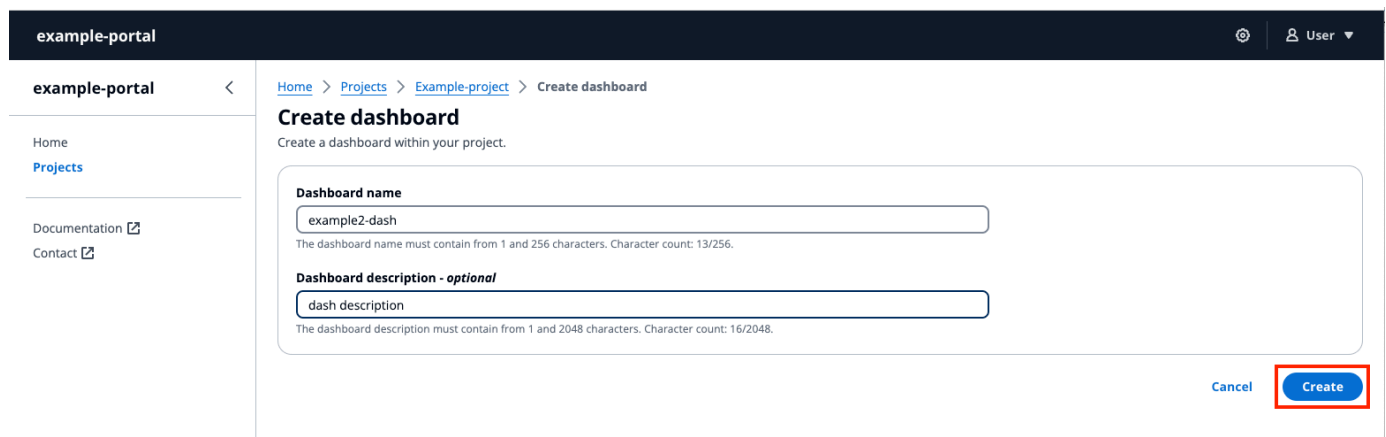
1. Crie um painel de duas maneiras:
 - a. Crie um painel em Criar um painel na página inicial.
 - i. Para criar o painel em um projeto existente, escolha um nome de projeto no menu suspenso em Escolha um projeto para hospedar o painel.
 - ii. Se você não tiver um projeto, escolha Criar projeto e selecione Confirmar.



- b. Crie um painel a partir de um projeto na seção Projetos, em Painéis.



2. Selecione Criar no canto superior direito.
3. Insira o nome do painel e forneça uma descrição opcional do painel.
4. Escolha Criar.



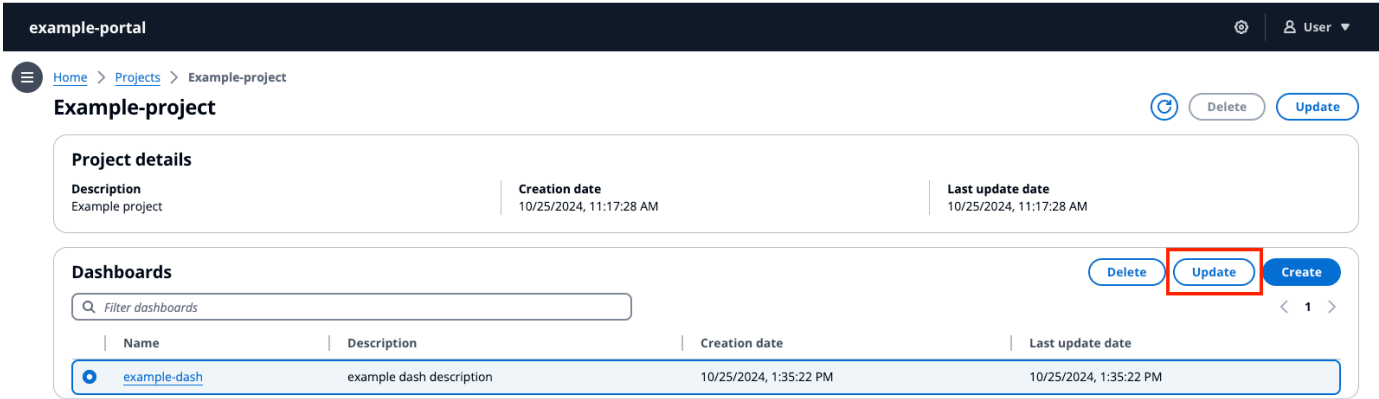
5. Configure seu painel recém-criado.

Atualizar um painel

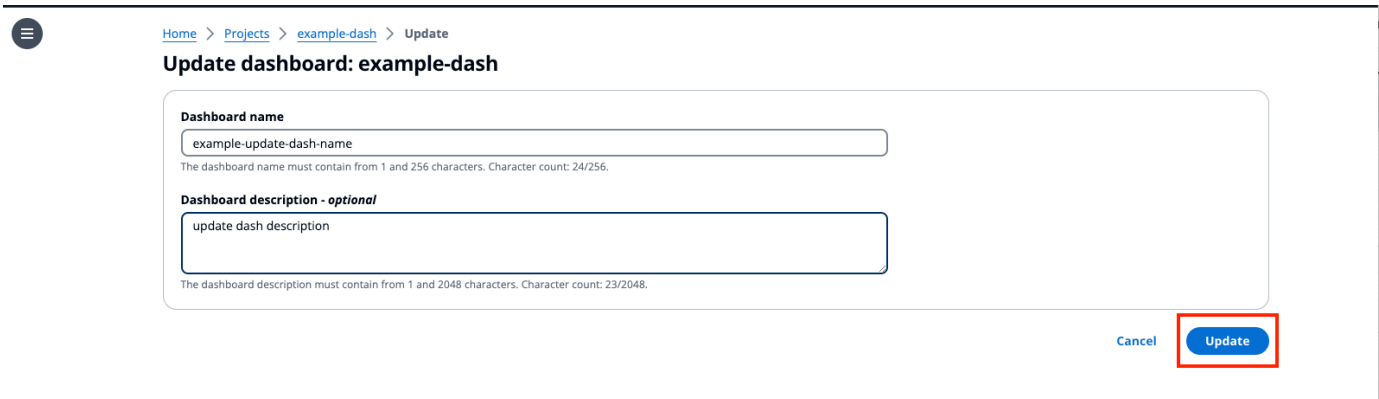
A seção Painéis lista os painéis do projeto. Selecione um painel na lista.

Atualizar um painel

1. Selecione um painel para atualizar.



2. Atualize o nome do painel e, opcionalmente, a descrição do painel. Selecione Atualizar para salvar as alterações.



Excluir um painel

A seção Painéis lista os painéis do projeto. Selecione um painel na lista.

Excluir um painel

1. Selecione um painel para excluir.

The screenshot shows the 'Example-project' page in the AWS IoT SiteWise portal. The page has a dark header with 'example-portal' and a user profile. The main content area is divided into two sections: 'Project details' and 'Dashboards'. The 'Project details' section shows the project name 'Example project', its description 'Example project', creation date '10/25/2024, 11:17:28 AM', and last update date '10/25/2024, 11:17:28 AM'. The 'Dashboards' section shows a list of dashboards with columns for Name, Description, Creation date, and Last update date. The 'example-dash' dashboard is selected and highlighted.

Name	Description	Creation date	Last update date
example-dash	example dash description	10/25/2024, 1:35:22 PM	10/25/2024, 1:35:22 PM

2. Selecione Excluir para excluir o painel. Isso não pode ser desfeito.

Configurar painel

A seção Painéis lista os painéis do projeto. Selecione um painel na lista. O modo Editar permite que você configure seu painel adicionando widgets e configurando-os. O botão Visualizar permite que você visualize suas alterações.

The screenshot shows the 'example-dash' dashboard configuration page. The page has a dark header with 'example-portal' and a user profile. The main content area is divided into two sections: a sidebar on the left and a main panel on the right. The sidebar contains links for Home, Projects, Documentation, and Contact. The main panel shows the dashboard name 'example-dash', a time range selector set to 'Last 5 minutes', a refresh rate selector set to '5s', and buttons for 'Save' and 'Edit'. The 'Edit' button is highlighted with a red box.

Etapas para configurar seu painel:

- Arraste e solte diferentes tipos de widgets de dados na tela do painel para visualização de dados.
- Adicione dados aos widgets desejados, a partir do explorador de recursos à esquerda. O explorador de recursos consiste nas seções de ativos modelados, não modelados e dinâmicos. Pesquise por nome do ativo ou nome da propriedade. Selecione a propriedade a ser adicionada e escolha Adicionar.
- Ajuste o layout e o estilo alterando as configurações nos widgets. Configure componentes, incluindo título, limites e outras especificações de configuração.
- Configure o intervalo de tempo no qual os dados são exibidos.

- Escolha o intervalo de tempo no qual os dados são exibidos. Escolha um intervalo de tempo e uma taxa de atualização no canto superior direito e personalize o intervalo. Escolha uma taxa na qual os dados devem ser atualizados no menu.
- Selecione o intervalo de tempo em um widget usando a roda de rolagem do mouse do trackball ou clique com o botão direito do mouse. Isso move o intervalo de tempo de exibição.
- Escolha Salvar.

Tópicos

- [Explorador de recursos](#)
- [Widgets](#)
- [Configurar widgets](#)
- [Use widgets](#)
- [Alarmes em widgets](#)
- [AWS IoT SiteWise Uso do assistente em widgets](#)
- [Exemplos de perguntas para fazer ao AWS IoT SiteWise Assistente](#)

Explorador de recursos

Esta seção descreve ativos modelados, não modelados e dinâmicos. Escolha ativos de qualquer um dos três, adicione-os aos seus widgets e visualize-os.

Tópicos

- [Modelado](#)
- [Não modelado](#)
- [Ativos dinâmicos](#)

Modelado

Esta seção descreve o processo de seleção e visualização de ativos modelados.

Seleção de ativos

Os ativos podem ser consultados da seguinte forma:

- Pesquise o nome de um ativo. Use um curinga*. Por exemplo, Wind* retorna nomes de ativos que começam com o textoWind. Você deve [se integrar com AWS IoT TwinMaker](#) para aproveitar esse recurso.
- Todos os ativos são listados por padrão.

A partir dos ativos listados, filtre por nome, descrição, ID ou ID do modelo de ativo. Selecione um ativo para listar suas propriedades (fluxos de dados) e alarmes.

Seleção de fluxo de dados

Os fluxos de dados estão listados abaixo do menu Fluxos de dados. Filtre os fluxos de dados listados pelos metadados [da propriedade](#) no <https://docs.aws.amazon.com/iot-sitewise/último APIReference/>. Selecione um ou mais fluxos de dados, dependendo do widget selecionado.

- O KPI e o Gauge oferecem suporte apenas a um único fluxo de dados.
- Os widgets restantes oferecem suporte a vários fluxos de dados com seleção múltipla.

Seleção de alarme

AWS IoT SiteWise os alarmes estão listados abaixo do menu Alarm Data Streams. Filtre os fluxos de dados de alarme listados por metadados de alarme. nome, propriedade de entrada e ID do modelo composto são alguns metadados usados para filtragem. Selecione um ou mais fluxos de dados, dependendo do widget selecionado.

- O KPI e o Gauge suportam apenas um único alarme.
- Os widgets restantes suportam vários alarmes com seleção múltipla.

Visualização de ativos modelados

1. Arraste o widget até a tela. Selecione as propriedades de cada painel de widget para criar um painel.
2. A opção Filtro filtra os ativos para escolher o ativo a ser visualizado. A filtragem é feita por texto, propriedade ou valor. A filtragem é para ativos carregados no navegador e não para filtragem de back-end.
3. Pesquise para listar um ativo para adicionar ao seu widget.
4. Adicione o ativo ao widget na tela.

5. Escolha Redefinir para selecionar outro ativo ou fazer modificações no ativo escolhido.
6. Salve o painel. No modo de visualização, escolha ativos diferentes no menu suspenso para monitorar as propriedades em cada ativo sem reconstruir os painéis de dados.

 Note

A roda de configurações no lado direito exibe Preferências para o usuário escolher, como Tamanho da página, primeiras colunas fixas, últimas colunas fixas e Preferências de coluna. Personalize suas preferências e escolha Confirmar para aplicar as alterações.

Modeled

Unmodeled

Dynamic assets

Assets (1)

Browse through your asset hierarchy and select an asset to view its associated data streams.

Root

Search

Q

Search for resources

Search

Filter

Q

Filter assets by text, property, or value

< 1 > ⚙

Name

Description

Demo Wind Farm Asset

Asset properties (8)

Select a modeled datastream to add to a selected widget

Filter

Q

Filter asset properties by text, property, or value

< 1 > ⚙

☐	Name	Unit	Data ty...	Latest ...	Latest value time
☐	Total Aver...		DOUBLE	37478.2303	2024-10-01 09:50:00 p.m.
☐	Total Aver...		DOUBLE	6.0000	2022-10-26 03:42:43 p.m.
☐	Total Aver...		DOUBLE	555.0000	2022-10-13 11:59:49 p.m.
☐	Code		INTEGER	300.0000	2022-10-13 10:59:28 p.m.
☐	Reliability ...		STRING	Mary Major	2022-10-13 10:59:28 p.m.
☐	Location		STRING	Renton	2022-10-13 10:59:28 p.m.
☐	Total Over...		DOUBLE	900.0000	2024-10-01 09:50:00 p.m.
☐	recipient a...		STRING	54a88418-...	2022-10-26 03:42:43 p.m.

Não modelado

Esta seção descreve como pesquisar fluxos de dados não modelados e adicioná-los aos widgets para visualização.

Visualização de fluxos de dados não modelados

1. Arraste o widget até a tela. Selecione as propriedades de cada painel de widget para criar um painel.
2. Os fluxos de dados não modelados estão listados na seção Séries temporais. Eles têm propriedades que são personalizáveis.
3. A opção Filtro filtra os fluxos de dados a serem visualizados. A filtragem é para fluxos de dados carregados no navegador, e não para filtragem de back-end.
4. Adicione o fluxo de dados ao widget na tela.
5. Escolha Redefinir para desmarcar o fluxo de dados.
6. Salve o painel. No modo de visualização, escolha ativos diferentes no menu suspenso para monitorar as propriedades em cada ativo sem reconstruir os painéis de dados.

Note

A roda de configurações no lado direito exibe Preferências para o usuário escolher, como Tamanho da página, primeiras colunas fixas, últimas colunas fixas e Preferências de coluna. Personalize suas preferências e escolha Confirmar para aplicar as alterações.

Modeled | **Unmodeled** | Dynamic assets

Time series (1)
Select a unmodeled datastream to add to a selected widget

Filter < 1 > ⚙

☒	Alias ▾	ID ▾	Data type ▾	Latest val... ▾	Latest valu... ▾
☒	DemoDisass...	33e78bb9-39...	DOUBLE	3.0283	2024-10-01 0...

Ativos dinâmicos

O novo SiteWise Monitor permite que os clientes troquem dinamicamente os ativos por um modelo de ativo selecionado. Você pode visualizar propriedades de diferentes ativos selecionando em um menu suspenso.

Visualização dinâmica de ativos

1. Escolha a guia Ativos dinâmicos no explorador de recursos.
2. Selecione um modelo de ativo para listar ativos no menu suspenso.
3. Selecione o ativo padrão no menu suspenso.
4. Escolha Definir modelo de ativo para selecionar o modelo de ativo.
5. Salve o painel. No modo de visualização, escolha ativos diferentes no menu suspenso para monitorar as propriedades em cada ativo, sem reconstruir os painéis de dados.

Resource explorer

Modeled | **Unmodeled** | **Dynamic assets**

Dynamic asset visualizations allow you to build one visualization to represent any asset of a specified asset model. [Learn more](#)

Asset model
Select an asset model to add the associated properties into your dynamic display.

Demo Wind Farm Asset Model 2022-Oct-14 05:59:28

Q *Filter asset models*

Demo Turbine Asset Model 2022-Oct-14 05:59:12
This is an asset model used in the IoT SiteWise Demo for representing a turbine in a wind farm. It will be deleted at the end of the demo.

Demo Wind Farm A Demo Turbine Asset Model 2022-Oct-14 05:59:12
This is an asset model used in the IoT SiteWise Demo for representing a wind farm. It will be deleted at the end of the demo. ✓

Finished loading asset models.

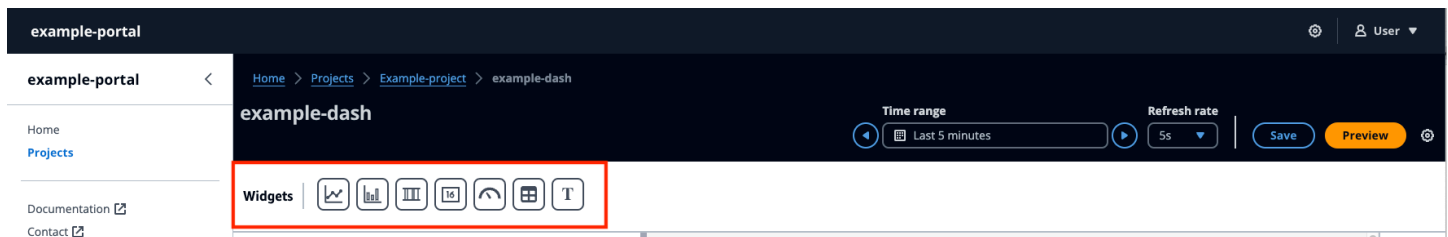
Set asset model

Widgets

Os widgets oferecem suporte a uma ampla variedade de recursos, incluindo alarmes, transmissão ao vivo de alto desempenho e sincronização suave com outros componentes do IoT App Kit. O painel é compatível com os seguintes widgets:

- **Linha** — O widget Linha é um widget de visualização que exibe tendências e mudanças ao longo do tempo. Ele consiste em uma série de pontos de dados, cada um representado por um ponto ou marcador, conectados por segmentos de linha reta para criar um gráfico de linha. Ele suporta uma ampla variedade de recursos, incluindo alarmes, limites, transmissão ao vivo de alto desempenho e sincronização suave com outros componentes do IoT App Kit. Esse widget é personalizável para comunicar dados complexos de forma clara e concisa.
- **Gráfico de barras** — O gráfico de barras é uma poderosa ferramenta de visualização que exibe dados de séries temporais. Ele suporta uma ampla variedade de recursos, incluindo alarmes, transmissão ao vivo de alto desempenho e sincronização suave com outros componentes do IoT App Kit.
- **Linha do tempo** — O widget Linha do tempo fornece uma maneira de visualizar e navegar pelos dados de séries temporais das fontes de dados. É exclusivo para exibir valores de fluxo de dados em cores distintas na linha do tempo. Ele suporta um rico conjunto de recursos, incluindo alarmes, transmissão ao vivo de alto desempenho e sincronização suave entre outros componentes do IoT App Kit. É melhor usado para exibir tipos de dados não numéricos/
- **KPI** — O componente Key Performance Indicator (KPI) fornece uma representação compacta de uma visão geral das propriedades de seus ativos. Ele suporta alarmes e limites. Essa visão geral fornece informações essenciais sobre o desempenho geral de seus dispositivos, equipamentos e processos. O KPI suporta apenas um único fluxo de dados ou alarme, e não vários fluxos de dados.
- **Medidor** — O componente Medidor fornece uma representação compacta de uma visão geral das propriedades de seus ativos. Ele é usado para visualizar informações críticas sobre o desempenho geral de seus dispositivos, equipamentos ou processos. É funcionalmente igual ao KPI, mas visualmente diferente. O medidor exibe o valor do fluxo de dados, o limite e a faixa de valores. Você pode interagir com AWS IoT dados de uma ou mais fontes de dados com o Gauge.
- **Tabela** — O componente Tabela fornece um formato compacto para visualizar um ou mais fluxos de dados de uma ou mais fontes de dados de séries temporais. Ele exibe ativos com Propriedade, Valor mais recente e Unidade em formato tabular. Suporta AWS IoT SiteWise alarmes.

- **Texto** — O widget de texto ajuda a escrever texto com várias cores e fontes. Você pode criar um link associando um texto a um URL. Os campos Propriedades e Limites não estão habilitados para esse widget.



Configurar widgets

Depois que o widget for adicionado ao painel, você poderá configurá-lo escolhendo o ícone Configuração no painel direito.

- **Estilo** — Adicione um título ao título do widget. Widgets diferentes têm configurações diferentes. Alguns exemplos estão listados abaixo.
 - **Widget de barra:**
 - **Resolução e agregação** — defina valores para resolução e agregação aqui.
 - **Formatar dados** — Defina casas decimais para o número de decimais a serem exibidos.
 - **Estilo de exibição** — Selecione os valores a serem exibidos.
 - **Eixo** — Escolha exibir o eixo.
 - **Widget de linha:**
 - **Resolução e agregação** — defina valores para resolução e agregação aqui.
 - **Formatar dados** — Defina casas decimais para o número de decimais a serem exibidos.
 - **Eixo Y** — Adicione um rótulo e valores mínimos e máximos.
 - **Estilo do widget** — Selecione o tipo de linha, o estilo da linha, a espessura da linha e os valores da forma do ponto de dados.
 - **Legenda** — Escolha Alinhamento e Exibição.
 - **Widget de medidor:**
 - **Resolução e agregação** — defina valores para resolução e agregação aqui.
 - **Formatar dados** — Defina casas decimais para o número de decimais a serem exibidos.
 - **Estilo de exibição** — Selecione os valores a serem exibidos.
 - **Eixo Y** — Adicione um rótulo e valores mínimos e máximos.

- Fontes — Selecione os valores de tamanho da fonte, Tamanho da fonte da unidade e Tamanho da fonte do rótulo.

Configuration for a Line widget

Configuration

Style | Properties | Thresholds

Widget title

Input title

▼ Resolution and Aggregation

Resolution

Autoselect

Aggregation

Average

▼ Format data

Decimal places

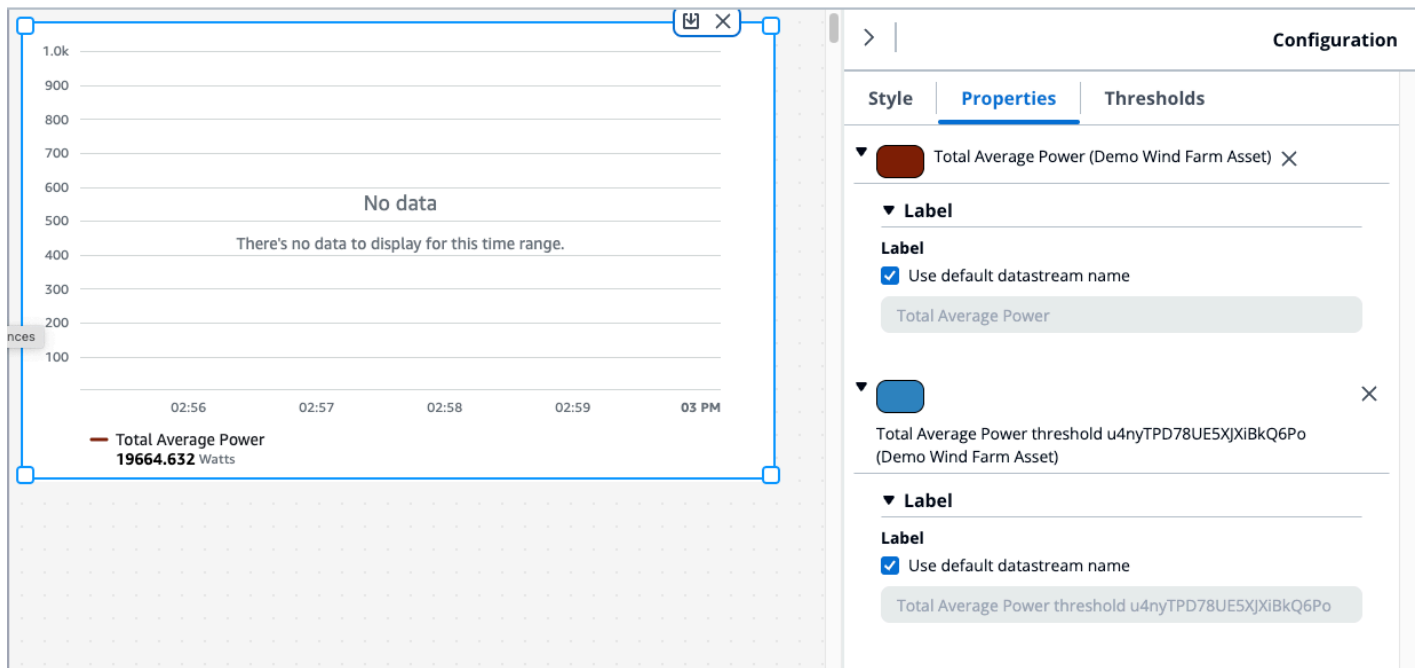
Must be between 0 and 100.

▼ Axis

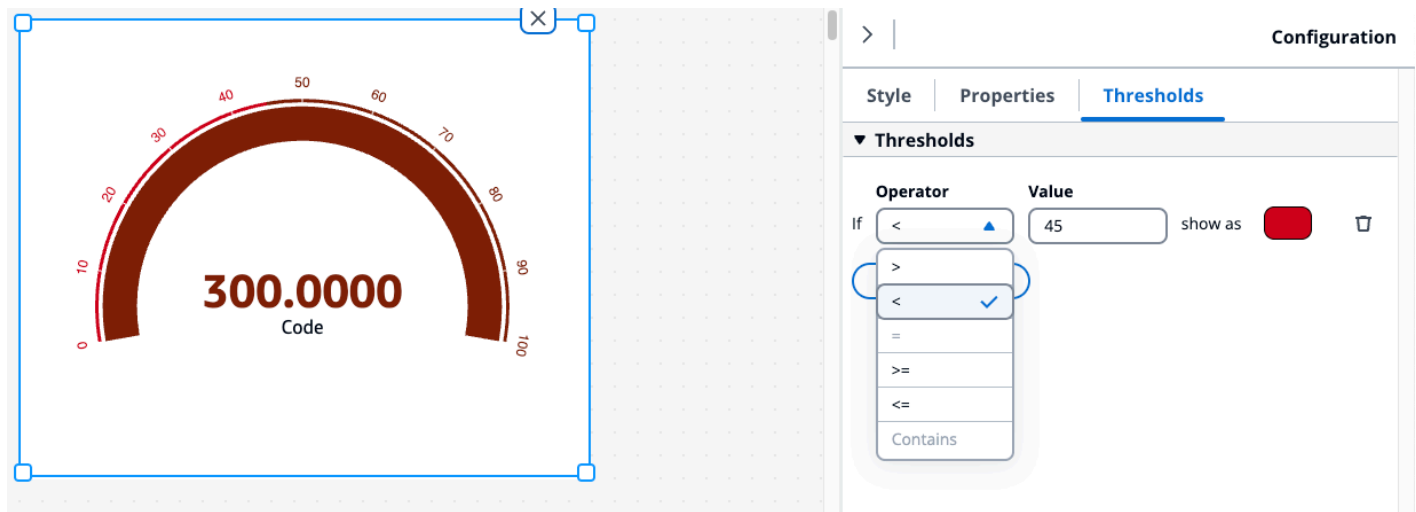
☒ View X axis ☒ View Y axis

Y axis Label

- Propriedades — Todas as propriedades dos widgets estão listadas nesta seção. Widgets diferentes têm propriedades diferentes. Alguns exemplos estão listados abaixo.
 - Widget de linha:
 - Rótulo — Escolha usar o nome padrão do fluxo de dados ou dar um novo nome.
 - Estilo — Defina o tipo de linha e o estilo da linha para o número de decimais a serem exibidos.
 - Eixo Y — Selecione valores para o estilo padrão, mostre os controles do eixo Y e defina os valores mínimo e máximo.
 - Widget de tabela:
 - Rótulo — Escolha usar o nome padrão do fluxo de dados ou dar um novo nome.
 - Widget de tabela:
 - Rótulo — Escolha usar o nome padrão do fluxo de dados ou dar um novo nome.



- Limites — Adicione um limite para um widget. Widgets diferentes têm configurações diferentes. Alguns exemplos estão listados abaixo.
 - Widget de gráfico de barras:
 - Escolha Adicionar um limite para adicionar ao widget.
 - Escolha Operador e forneça um valor para o limite. Personalize o limite com uma cor da paleta de cores.
 - Você pode optar por aplicar o limite em todos os dados.
 - Widget de linha:
 - Escolha Adicionar um limite para adicionar ao widget.
 - Escolha Operador e forneça um valor para o limite. Personalize o limite com uma cor da paleta de cores.
 - Escolha como Mostrar limites no menu suspenso.
 - Widget de medidor:
 - Escolha Adicionar um limite para adicionar ao widget.
 - Escolha Operador e forneça um valor para o limite. Personalize o limite com uma cor da paleta de cores.



Use widgets

Você pode usar widgets no painel individualmente ou selecionando-os várias vezes.

Edite widgets no painel

Escolha um único widget e edite-o. Para editar vários widgets no painel, clique com a tecla Shift + com o botão esquerdo do mouse e selecione todos os widgets no painel. Depois de selecionado, os usuários podem adicionar novos fluxos de dados e modificar o título do widget nas configurações de estilo. O título é alterado para todos os widgets no painel.

Clique com o botão direito na tela e faça o seguinte:

- Copiar — Adicione uma cópia do widget à tela.
- Excluir — Exclua o widget.
- Trazer para frente — Traga o widget selecionado para a frente da tela.
- Enviar para trás — Envie o widget selecionado para a parte de trás da tela.

Redimensionar widgets

Redimensione os widgets individualmente ou em um grupo selecionando vários widgets no painel.

Para alterar o tamanho dos widgets:

- Para alterar o tamanho de um único widget, selecione o widget e arraste-o por um canto para alterar seu tamanho.

- Para alterar o tamanho de vários widgets, selecione vários widgets com Shift + clique com o botão esquerdo e arraste-os por um canto para alterar seu tamanho.

Excluir widgets no painel

Exclua os widgets individualmente ou em um grupo selecionando vários widgets no painel.

Para excluir widgets:

- Para excluir um único widget, selecione o widget, clique com o botão direito do mouse e escolha Excluir. Você também pode selecionar e clicar em X no canto superior direito para excluir o widget.
- Para excluir vários widgets, selecione vários widgets com Shift + clique com o botão esquerdo, depois clique com o botão direito do mouse e escolha Excluir.

Alarmes em widgets

Os alarmes alertam você e sua equipe quando equipamentos ou processos apresentam desempenho abaixo do ideal. 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. Os alarmes permitem identificar problemas rapidamente e notificar os operadores para maximizar o desempenho de equipamentos e processos.

Você pode encontrar um alarme associado a um ativo na guia Modelado do Explorador de recursos.

- Pesquise e selecione um ativo.
- Desça até a tabela Data Streams até a seção Alarm Data Streams e expanda-a.
- Selecione um alarme na tabela Alarmes e escolha Adicionar.

Tópicos

- [Alarmes em diferentes widgets](#)

Alarmes em diferentes widgets

Para todos os widgets:

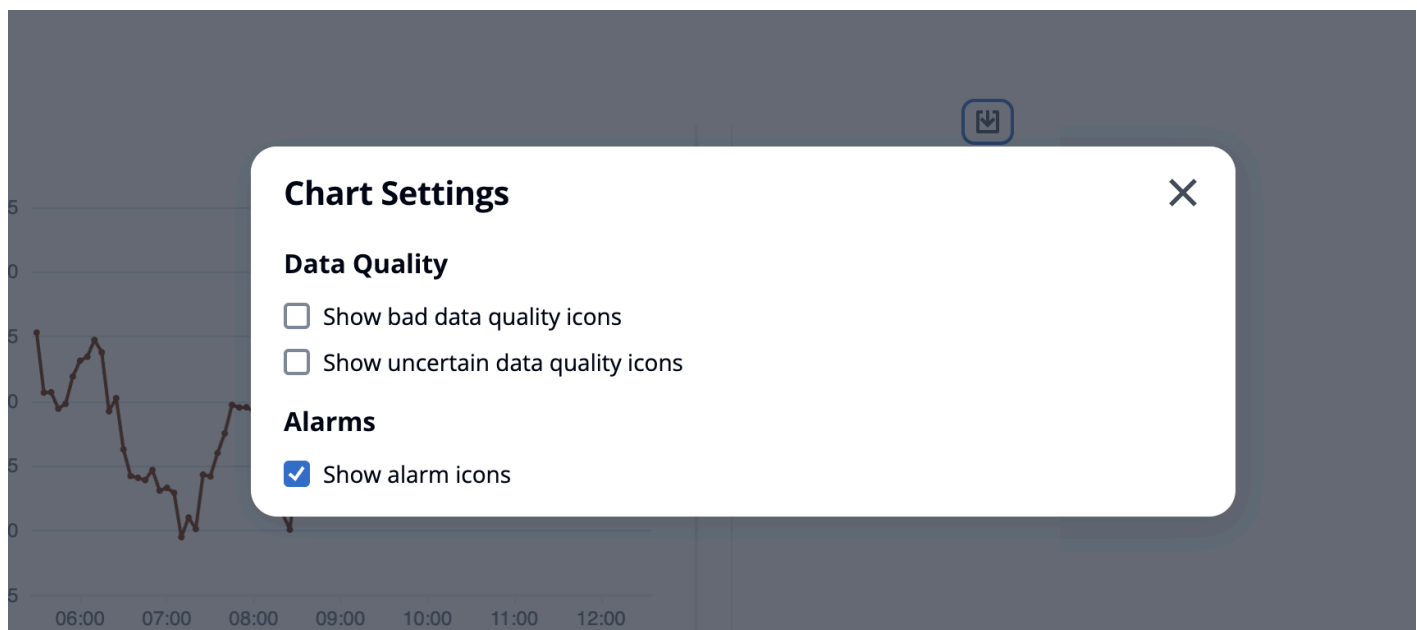
- As configurações da propriedade do fluxo de dados dependem do tipo de propriedade adicionada a um widget. As propriedades do fluxo de dados têm suporte total à configuração de propriedades,

enquanto as propriedades de alarme atualmente não permitem configurações de configuração de propriedades.

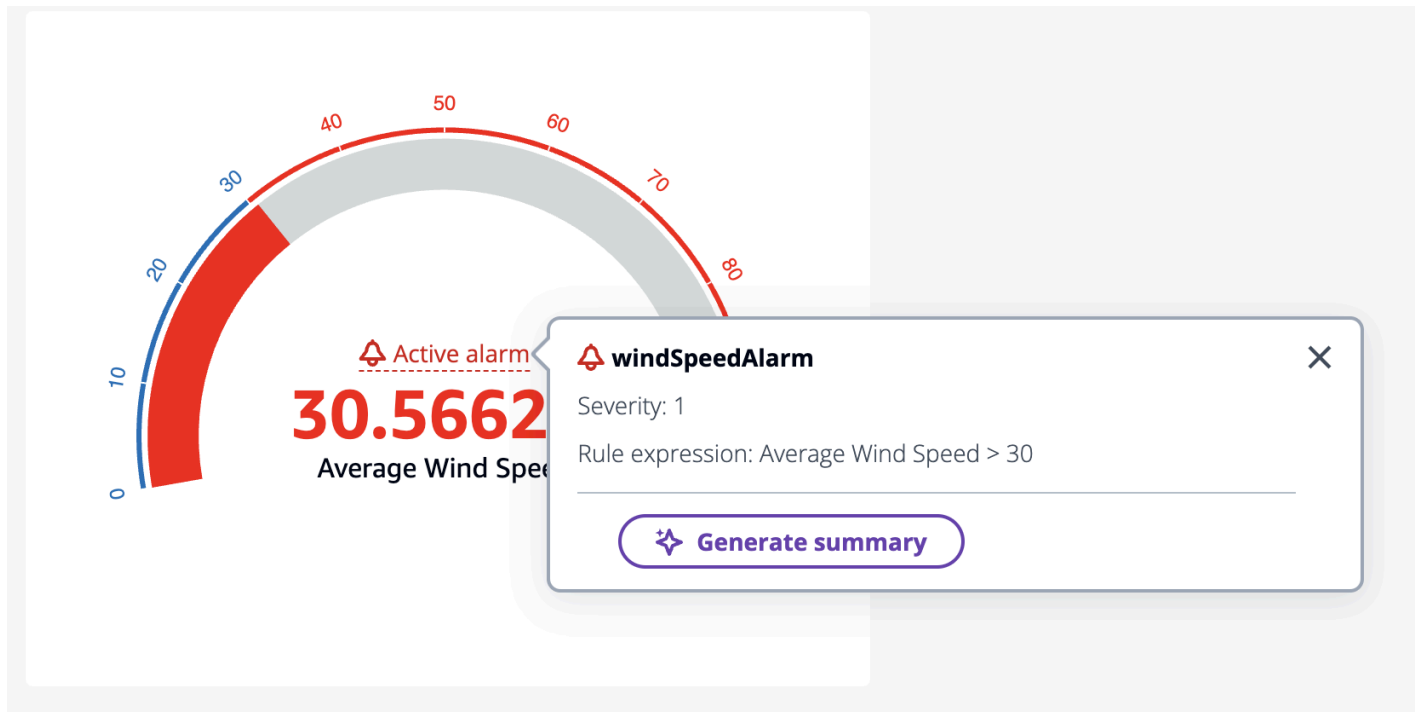
- Se você adicionar um fluxo de dados de alarme, seu fluxo de dados de propriedade de entrada associado também será adicionado ao gráfico. Se você remover o fluxo de dados do alarme, sua propriedade de entrada também será removida.
- Para controlar individualmente o fluxo de dados da propriedade de entrada de um alarme, você deve adicionar os dois separadamente.

Os exemplos abaixo mostram como alguns widgets usam alarmes.

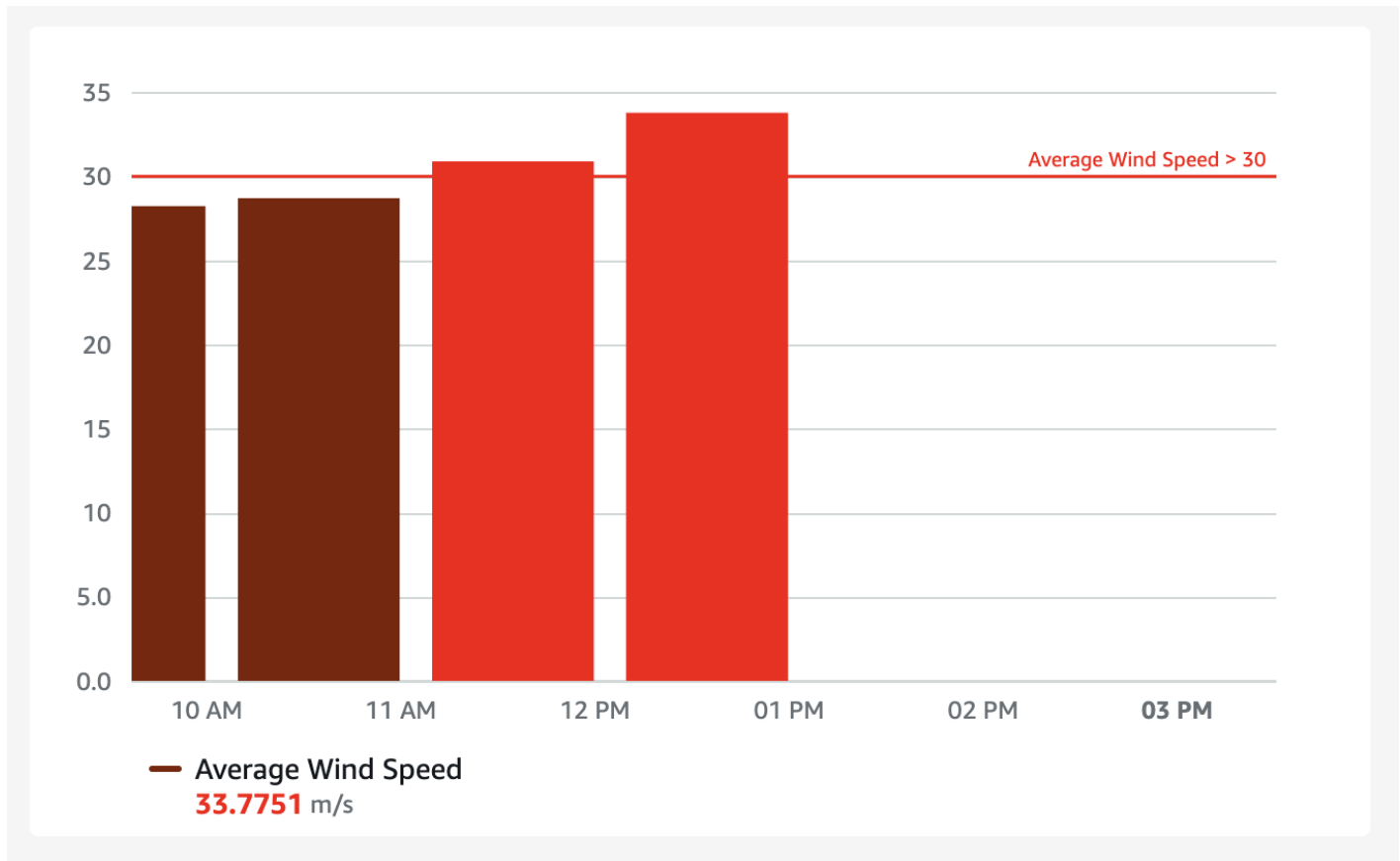
- Gráfico de linhas
 - O alarme e seu fluxo de dados de propriedades de entrada são adicionados ao gráfico.
 - Você pode ver o estado do alarme na legenda do gráfico e como ícones pairando sobre o fluxo de dados quando o alarme muda de estado.
 - Você pode desativar os ícones de alarme nas configurações do gráfico.



- KPI e medidor
 - O alarme e seu fluxo de dados de propriedades de entrada são adicionados ao widget escolhido.
 - O limite de alarme é adicionado ao widget, que muda de cor com base em sua configuração.
 - Você pode selecionar o estado do alarme no widget, ver os detalhes do alarme e clicar em Gerar resumo para chamar o e AWS IoT SiteWise obter um resumo do alarme.



- Tabela
 - O alarme e sua propriedade de entrada são adicionados como uma linha na tabela.
- Gráfico de barras
 - O alarme é adicionado como um limite ao gráfico, o que altera a cor de qualquer fluxo de dados que ultrapasse o limite.
 - Você pode adicionar qualquer fluxo de dados associado separadamente.
 - Você não pode interagir com o AWS IoT SiteWise Assistente a partir do widget.

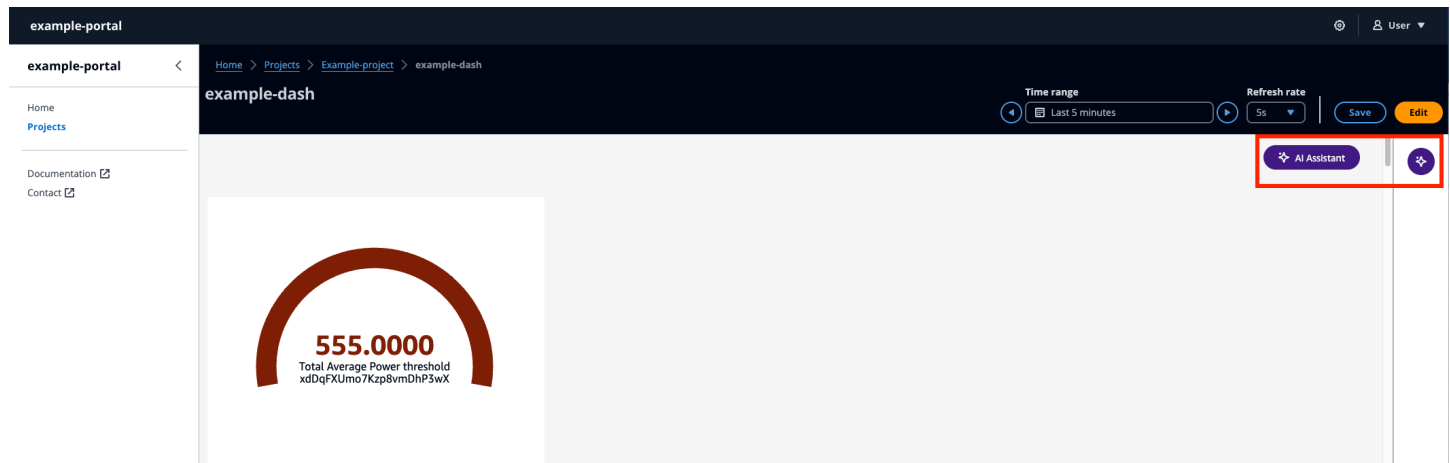


- Cronograma de status
 - O alarme é adicionado como um limite na linha do tempo.
 - Adicionar o estado do alarme e os dados de suas propriedades de entrada à linha do tempo é um trabalho em andamento.
 - Você não pode interagir com o AWS IoT SiteWise Assistente a partir do widget.

AWS IoT SiteWise Uso do assistente em widgets

O AWS IoT SiteWise Assistant é um assistente generativo alimentado por IA. Ele permite que usuários como gerentes de fábrica, engenheiros de qualidade e técnicos de manutenção obtenham insights, resolvam problemas e tomem medidas diretamente de seus dados operacionais e corporativos. O AWS IoT SiteWise Assistant consolida informações de AWS IoT dados, modelos de ativos, manuais e documentação em resumos compreensíveis de eventos críticos. Ele também permite sessões interativas de perguntas e respostas aprofundadas para facilitar o diagnóstico, explorar a causa raiz e fazer recomendações guiadas.

O botão AWS IoT SiteWise Assistente está no canto superior direito do painel. Clique nele para ativar o Assistente. Só pode ser usado com o modo de visualização do painel.



Use o AWS IoT SiteWise Assistente nos seguintes cenários:

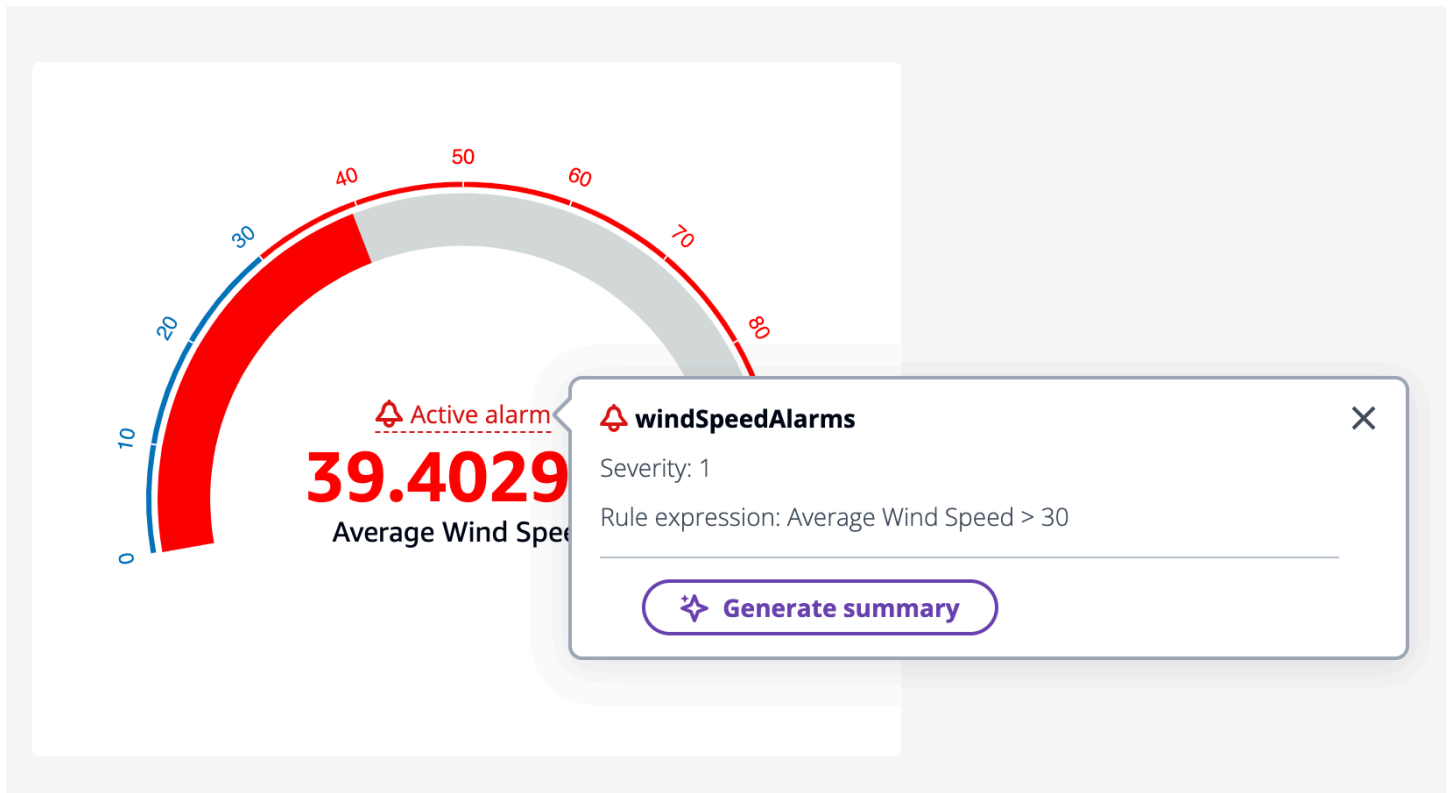
Tópicos

- [Caso de uso - Resumos de alarmes](#)
- [Caso de uso - Resumos situacionais](#)
- [Caso de uso - Resumos detalhados](#)

Caso de uso - Resumos de alarmes

Resuma o alarme atual de um painel selecionado no painel. Os alarmes são suportados pelos widgets Linha, KPI, Medidor e Tabela. Escolha um widget com um alarme e resuma-o.

- Selecione Alarme ativo no widget.
- A expressão Severidade e Regra é exibida para o alarme.
- Escolha Gerar resumo para gerar um resumo.



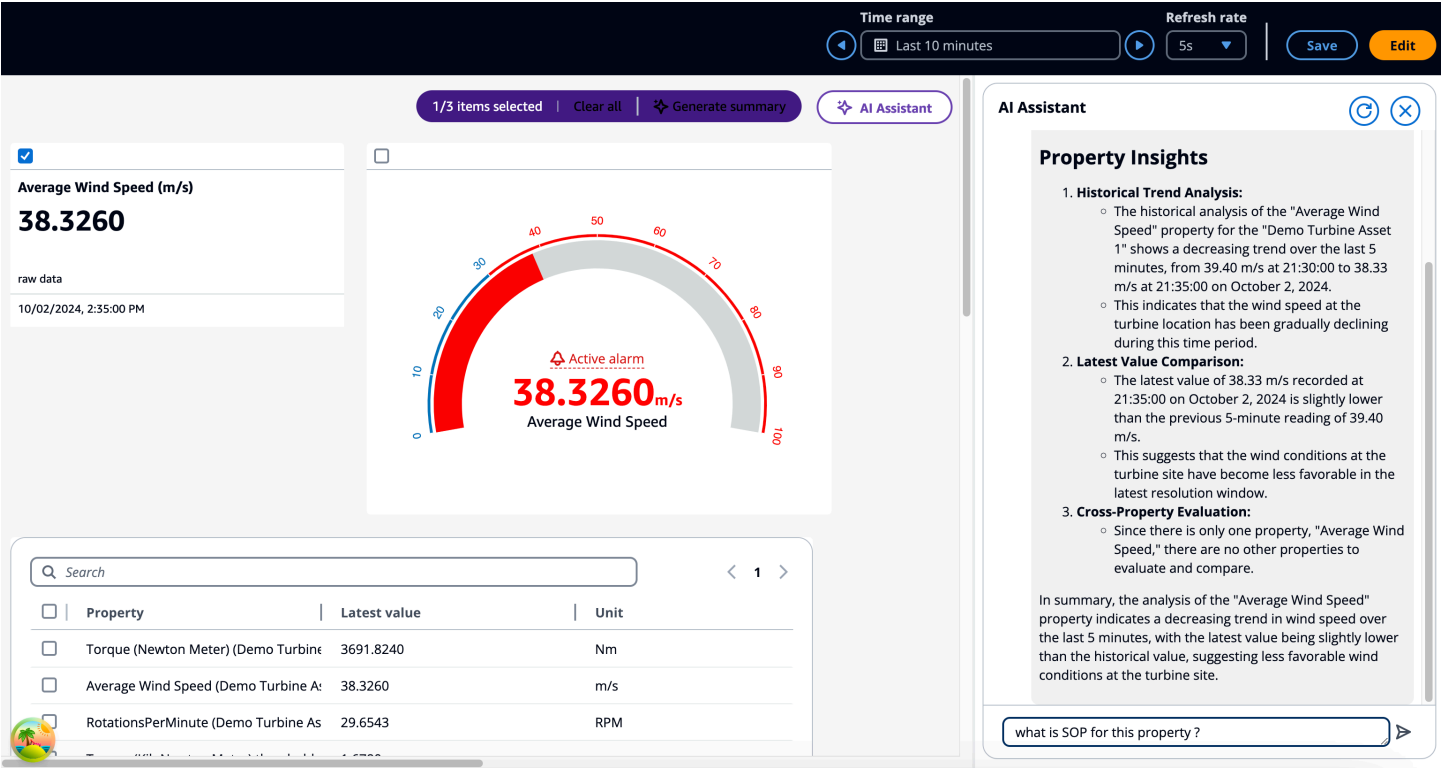
Caso de uso - Resumos situacionais

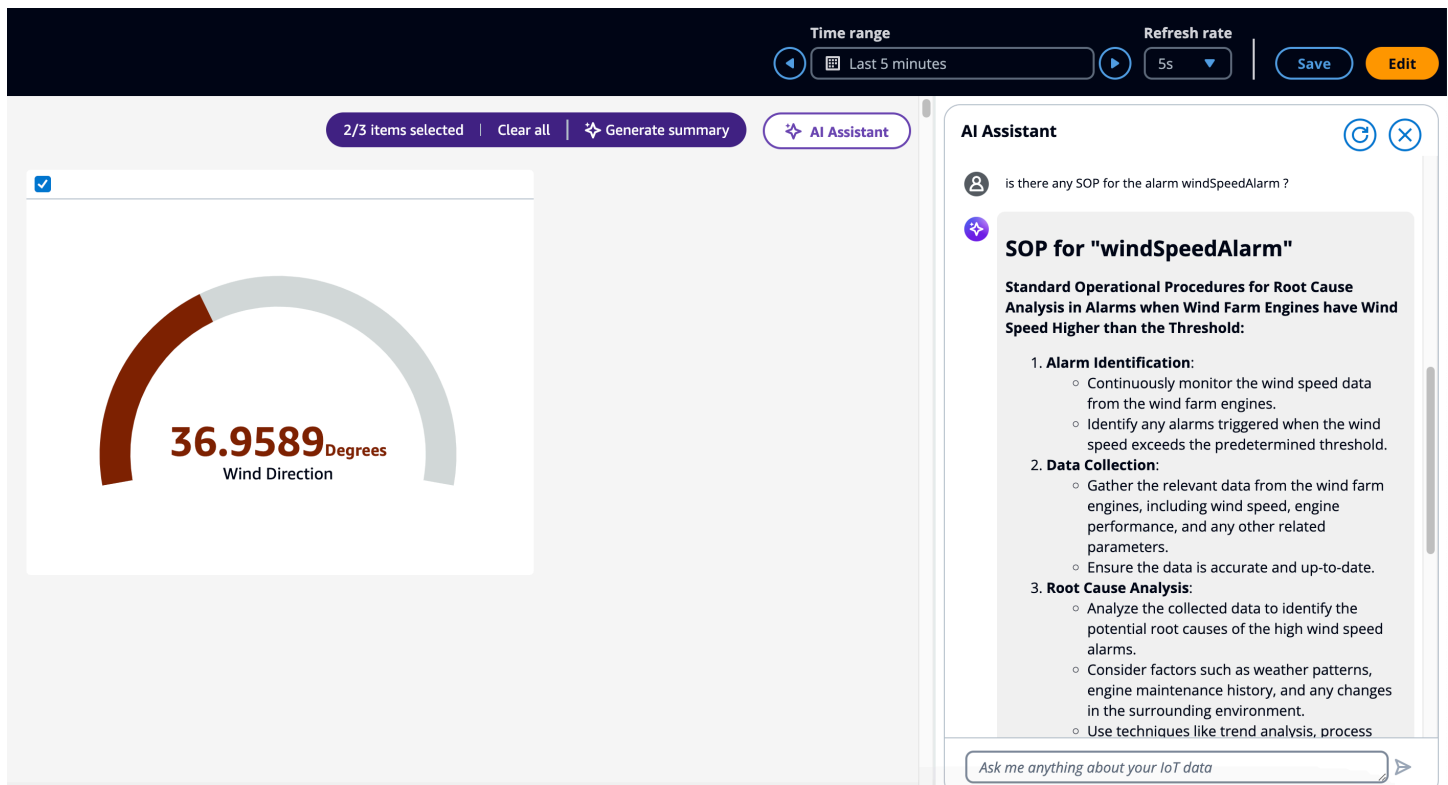
Selecione até três widgets para resumir. Eles podem ser uma combinação de widgets e propriedades. Se mais de três forem selecionados, o Assistente retornará um erro.

Gere um resumo da situação com o AWS IoT SiteWise Assistant

1. Clique em AI Assistant. Ele exibe um menu com três opções.
 - a. Itens selecionados — Selecione somente três. Você não pode selecionar mais de três.
 - b. Limpar tudo — Limpe sua seleção.
 - c. Gerar resumo — Gere um resumo sobre os itens selecionados.
2. Escolha Gerar resumo para gerar o resumo sobre os itens selecionados.

A imagem abaixo tem um widget selecionado e um resumo do AWS IoT SiteWise Assistente.





Exemplos de perguntas para fazer ao AWS IoT SiteWise Assistente

Note

- O AWS IoT SiteWise Assistente deve usar um conjunto de dados com um índice [Amazon Kendra](#) para obter conhecimento e orientação em nível empresarial. Se você não tiver um índice do Amazon Kendra, [consulte Criação de um índice para criar um](#). Adicionar um [conjunto de dados](#) melhora a qualidade da resposta do Assistente. Consulte [Criar um conjunto de dados](#) para saber mais.
- Algumas perguntas exigem AWS IoT TwinMaker integração. Consulte [Integrar AWS IoT TwinMaker e AWS IoT SiteWise](#) para obter detalhes.

Algumas perguntas complementares para fazer ao Assistente depois de receber um resumo do alarme no painel, como parte da mesma conversa.

- Mostrar os detalhes do ativo no resumo acima?
- Qual é o caminho hierárquico da raiz até o ativo mencionado?
- Quais são os ativos descendentes dependentes do ativo mencionado?

- Quais são os ativos dependentes do ativo mencionado que têm alarmes ativos?
- Encontre todos os ativos que têm alarmes ativos.

Algumas perguntas de acompanhamento para fazer ao Assistente depois de obter um resumo da propriedade no painel, como parte da mesma conversa.

- Faça a mesma análise nas últimas 24 horas.
- Encontre a documentação relacionada às propriedades mencionadas acima.
- Forneça os detalhes da ID do ativo 1da67d28-14f8-4f71-a06a-386f0425a21d/nome do ativo Demo Turbine Asset 1.

Invoque o AWS IoT SiteWise Assistente a partir da API.

- Gere um resumo do alarme para o nome do alarme windSpeedAlarm no ID do ativo d591e153-e5cf-4206-96bb-ce3c119d9d2d.
- Gere um resumo do alarme das últimas 12 horas/2 dias/1 semana para o nome windSpeedAlarm do alarme na ID do ativo. d591e153-e5cf-4206-96bb-ce3c119d9d2d
- Gerar resumo da propriedade para o ID da propriedade ab187fb7-d74b-44d9-bd9b-f2f19a9137cc no ID do ativo d591e153-e5cf-4206-96bb-ce3c119d9d2d
- Gere o resumo da propriedade nas últimas 12 horas/2 dias/1 semana para o ID da propriedade no ID do ab187fb7-d74b-44d9-bd9b-f2f19a9137cc ativo. d591e153-e5cf-4206-96bb-ce3c119d9d2d
- Encontre os ativos com o nome do ativo Turbine.
- Forneça os valores atuais da propriedade da ID da propriedade 5356168c-3390-456f-802c-9f6e047810d4 na ID do ativo d591e153-e5cf-4206-96bb-ce3c119d9d2d, 3cbb084e-1ded-4b08-9f21-1b47b2fb86fd.
- Qual é a relação entre o ID do ativo d591e153-e5cf-4206-96bb-ce3c119d9d2d e o ID do ativo 3cbb084e-1ded-4b08-9f21-1b47b2fb86fd.
- Encontre documentação sobre como corrigir o problema de baixa rotação da turbina eólica.
- Gere um resumo da propriedade para o alias WindSpeed da propriedade.
- Quais são as verificações pré-operatórias de acordo com minha base de conhecimento?

Consultar dados de AWS IoT SiteWise

Você pode usar 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.

Use esses recursos para ter informações sobre os dados. Por exemplo, descubra todos os ativos que têm determinado valor de propriedade ou crie uma representação personalizada dos 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, consulte [Monitore dados com AWS IoT SiteWise Monitor](#).

As operações descritas nesta seção retornam objetos de valor de propriedade que contêm estruturas de carimbos de data/hora, 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`
 - `nullValue`

Tópicos

- [Consulte os valores atuais da propriedade do ativo em AWS IoT SiteWise](#)
- [Consulte valores históricos de propriedades de ativos em AWS IoT SiteWise](#)
- [Consulte agregados de propriedades de ativos em AWS IoT SiteWise](#)
- [AWS IoT SiteWise linguagem de consulta](#)

Consulte os valores atuais da propriedade do ativo em AWS IoT SiteWise

Este tutorial mostra duas maneiras de obter o valor atual de uma propriedade de ativo. Você pode usar o AWS IoT SiteWise console ou usar a API no AWS Command Line Interface (AWS CLI).

Tópicos

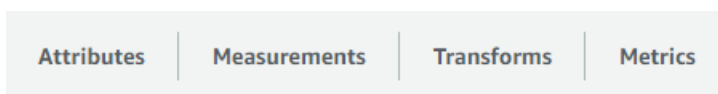
- [Consultar o valor atual de uma propriedade de ativo \(console\)](#)
- [Consultar o valor atual de uma propriedade de ativo \(AWS CLI\)](#)

Consultar o valor atual de uma propriedade de 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 o 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.

Consultar o valor atual de uma propriedade de 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 [GetAssetPropertyValue](#) operação para consultar o valor atual de uma propriedade do ativo.

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

- O `assetId` e `propertyId` da propriedade de 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 propriedade, consulte [Gerencie fluxos de dados para AWS IoT SiteWise](#).

Como obter o valor atual de uma propriedade de ativo (AWS CLI)

- Execute o seguinte comando para obter o valor atual da propriedade de ativo. *asset-id* Substitua 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",  
      "nullValue": {  
        "valueType": "String"  
      }  
    },  
  },  
  "timestamp": {  
    "timeInSeconds": Number,  
    "offsetInNanos": Number  
  },  
  "quality": "String"  
}
```

Consulte valores históricos de propriedades de ativos em AWS IoT SiteWise

Você pode usar a [GetAssetPropertyValueHistory](#) operação AWS IoT SiteWise da API para consultar os valores históricos de uma propriedade do ativo.

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

- O `assetId` e `propertyId` da propriedade de 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 propriedade, consulte [Gerencie fluxos de dados para AWS IoT SiteWise](#).

Envie os seguintes parâmetros para refinar os 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.

Como consultar o histórico de valores de uma propriedade de 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. *asset-id* Substitua 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 start-date \  
  --end-date end-date \  
  --max-results max-results \  
  --next-token next-token \  
  --time-ordering time-ordering \  
  --qualities qualities
```

```
--start-date 1575216000 \  
--end-date 1575216600
```

A operação retorna uma resposta que contém o histórico TQVs da propriedade no seguinte formato:

```
{  
  "assetPropertyValueHistory": [  
    {  
      "value": {  
        "booleanValue": Boolean,  
        "doubleValue": Number,  
        "integerValue": Number,  
        "stringValue": "String",  
        "nullValue": {  
          "valueType": "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 [GetAssetPropertyValueHistory](#) operação.

Consulte agregados de propriedades de ativos em AWS IoT SiteWise

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 de métrica, defina agregações específicas para a 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 obter mais informações, consulte [Agregar dados de propriedades e outros ativos \(métricas\)](#).

Tópicos

- [Agregados de uma propriedade de ativo \(API\)](#)
- [Agregados de uma propriedade de ativo \(AWS CLI\)](#)

Agregados de uma propriedade de ativo (API)

Use a AWS IoT SiteWise API para obter agregados para uma propriedade de ativo.

Use a [GetAssetPropertyAggregates](#) operação para consultar agregados de uma propriedade do ativo.

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

- O `assetId` e `propertyId` da propriedade de 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 propriedade, consulte [Gerencie fluxos de dados para AWS IoT SiteWise](#).

Você deve passar os seguintes parâmetros obrigatórios:

- `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 para recuperar a métrica: 1m (1 minuto), 15m (15 minutos), 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 [GetAssetPropertyAggregates](#) operação 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 de uma propriedade de ativo (AWS CLI)

Como consultar agregados de uma propriedade de 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. **asset-id** Substitua 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 que contém o histórico TQVs 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 [GetAssetPropertyAggregates](#) operação.

Note

Se seu intervalo de consulta contiver um `null` valor TQVs, consulte [AssetPropertyValueAPI](#). Todas as estatísticas, exceto a contagem, resultam em uma `null` resposta, semelhante às estatísticas de String TQVs. Se seu intervalo de consulta contiver `Double.NaN` para tipo duplo TQVs, todos os cálculos, exceto a contagem, resultarão em um `Double.NaN`.

AWS IoT SiteWise linguagem de consulta

Com a operação da [ExecuteQuery](#) API 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 da
- ativos
- medições
- métricas
- transformações
- 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 e AWS IoT TwinMaker estão disponíveis, exceto AWS GovCloud (Oeste dos EUA).

Tópicos

- [Pré-requisitos](#)
- [Referência da linguagem de consulta para AWS IoT SiteWise](#)

Pré-requisitos

AWS IoT SiteWise requer permissões de integração para que AWS IoT TwinMaker possa organizar e modelar dados industriais.

Para recuperar informações sobre modelos, ativos, medições, métricas, transformações e agregados, cumpra os seguintes pré-requisitos:

- Funções vinculadas ao serviço para ambas AWS IoT SiteWise e AWS IoT TwinMaker configuração em sua AWS conta. Para ter mais informações sobre os perfis vinculados ao serviço, consulte [Criar um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

- Uma AWS IoT SiteWise integração habilitada para sua função do IAM. Para obter mais informações, consulte [Integre AWS IoT SiteWise e 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 para AWS IoT SiteWise

AWS IoT SiteWise suporta uma linguagem de consulta avançada para trabalhar com seus dados. Os tipos de dados, operadores, funções e constructos disponíveis são descritos nos tópicos a seguir.

Consulte [Consultas de exemplo](#) para escrever consultas com a linguagem de AWS IoT SiteWise consulta.

Tópicos

- [Entenda as visualizações de referência da consulta](#)
- [Tipos de dados compatíveis](#)
- [Recupere dados com uma instrução SELECT](#)
- [Operadores lógicos](#)
- [Operadores de comparação](#)
- [Consultas de exemplo](#)

Entenda as visualizações de referência da consulta

Esta seção fornece informações para ajudá-lo a entender as visualizações AWS IoT SiteWise, como metadados do processo e dados de telemetria.

A tabela a seguir fornece os nomes e as descrições das visualizações.

Modelo de dados

Nome da visualização	Descrição da visualização
asset	Contém informações sobre o ativo e a derivação do modelo.
asset_property	Contém informações sobre a estrutura da propriedade do ativo.
raw_time_series	Contém os dados históricos da série temporal.
latest_value_time_series	Contém o valor mais recente da série temporal.
precomputed_aggregates	Contém os valores agregados de propriedades de ativo calculados automaticamente. Eles são um conjunto de métricas básicas calculadas com base em vários intervalos de tempo.

As visualizações a seguir listam os nomes das colunas para consultas e dados de amostra.

View:asset

asset_id	asset_name	asset_description	asset_model_id
88898498-0b8b-42b5-bf57-16180bc3d3a0	WindTurbine A	WindTurbine Ativo A	17847250-5bf0-4f74-b775-cc03f05e7cb8
17847250-5bf0-4f74-b775-cc03f05e7cb8	Modelo de Ativo da Turbina Eólica	Representa uma turbina em um parque eólico.	

View:asset_property

property_id	asset_id	property_name	property_alias	asset_composite_model_id	
b29be434-b000-4d74-b809-75287d83bcd6	88898498-0b8b-42b5-bf57-16180bc3d3a0	temperatura do motor	Rochester2/44///Line-5/Bus-2/Machine-5/Temperature		
3b458f00-24e7-458a-b4e8-c6026eff654a	88898498-0b8b-42b5-bf57-16180bc3d3a0	direção do vento	/company/windfarm/3/turbine/7/winddirection	2f458n00-56e7-458h-b4e8-c6026eff985g	

View:raw_time_series

asset_id	property_id	property_alias	event_timestamp	quality	boolean_value	int_value	double_value	string_value
888984980b8b-42b5-bf57-16180bc3d3a0	b29be434-b000-4d74-b809-75287d83bcd6	Rochester2/44///Line-5/Bus-2/Machine-5/Temperature	157521960	BOM			115,0	
888984980b8b-42b5-bf57-16180bc3d3a0	3b458f00-24e7-458a-b4e8-c6026eff654a	/company/windfarm/3/turbine/7/winddirection	157521937	BOM			348,75	

asset_id	property_id	property_alias	event_timestamp	quality	boolean_value	int_value	double_value	string_value
bf57-16180bc3d3a	c6026eff654a	windfarm3/ turbine /7/ winddirection						

Note

Você deve incluir uma cláusula de filtro na coluna `event_timestamp` para consultar a visualização `raw_time_series`. Esse filtro é obrigatório, e a consulta falhará sem ele.

Example consulta

```
SELECT event_timestamp, double_value FROM raw_time_series WHERE event_timestamp > 1234567890
```

View:latest_value_time_series

asset_id	property_id	property_alias	event_timestamp	quality	boolean_value	int_value	double_value	string_value
888984980b8b-42b1- bf57-16180bc3d3a	3b458f00- 24e7-458- b4e8-c6026eff654a	/ company, windfarm3/ turbine /7/ winddirection	15752196	BOM			355,39	

 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 será arredondado se a precisão de um número de entrada for muito alta.

Recupere dados com uma instrução SELECT

A instrução SELECT é usada para recuperar dados de uma ou mais visualizações. O AWS IoT SiteWise oferece suporte a uma JOIN implícita das visualizações. Você pode listar as visualizações a serem unidas (na cláusula FROM da instrução SELECT) usando vírgulas para separá-las.

Example

Use a seguinte instrução SELECT:

```
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 procurar um ativo:

```
SELECT asset_name, asset_description FROM asset WHERE asset_name LIKE 'Wind%'
```

Example para procurar 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 operador AND 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. Todas as operações de comparação estão disponíveis para tipos de dados incorporados e são avaliadas como um booleano.

Operadores lógicos

Operador	Descrição
<	Menor que
>	Maior que
<=	Menor ou igual a
>=	Maior ou igual a
=	Igual
!=	Not equal

Tabela verdadeira da operação de comparação para valores não numéricos

Tipo	Digite >= x	Tipo <= x	Tipo > x	Tipo < x	Tipo = x	Digite! = x
NaN	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE
NULL	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE

Existem alguns predicados que se comportam como operadores, mas têm uma sintaxe especial. Veja abaixo os exemplos.

Predicados de comparação

Operador	Descrição
IS NULL	Testa se um valor éNULL.
IS NOT NULL	Testa se um valor não éNULL.
IS NaN	Testa se um valor éNaN.
IS NOT NaN	Testa se um valor não éNaN.

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 valor

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
```

Interaja com outros AWS serviços

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 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 obter mais informações, consulte [Publicar atualizações de valores 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, consulte [Ingerir dados para AWS IoT SiteWise usar regras AWS IoT Core](#).

Tópicos

- [Noções básicas sobre as propriedades de ativo em tópicos MQTT](#)
- [Ative as notificações de propriedades de ativos em AWS IoT SiteWise](#)
- [Consulte notificações de propriedades de ativos em AWS IoT SiteWise](#)
- [Exportar dados para o Amazon S3 com notificações de propriedades de ativo](#)
- [Integre AWS IoT SiteWise com a Grafana](#)
- [Integre AWS IoT SiteWise e AWS IoT TwinMaker](#)
- [Detectar anomalias com o Lookout for Equipment](#)

Noções básicas sobre as propriedades de ativo em tópicos MQTT

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 .

Ative as notificações de propriedades de ativos em AWS IoT SiteWise

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

- [Ativar notificações de propriedades de ativo \(console\)](#)
- [Ativar notificações de propriedades de ativo \(AWS CLI\)](#)

Ativar notificações de propriedades de ativo (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.

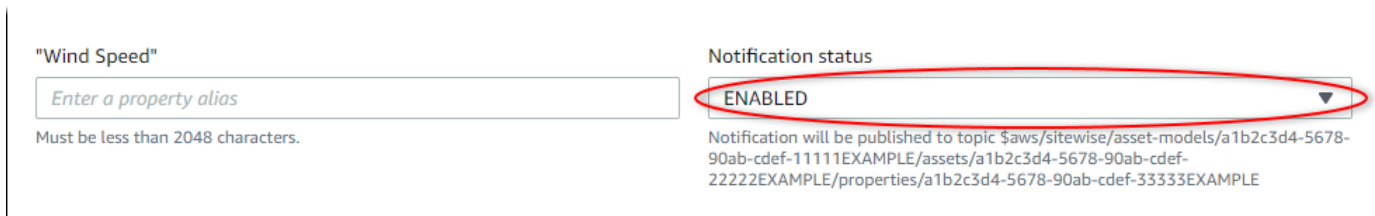
Como habilitar ou desabilitar notificações de propriedade de um ativo (console)

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 Editar.
5. Para o Status da notificação da propriedade de ativo, escolha HABILITADO.



The screenshot shows the AWS IoT SiteWise console interface. On the left, there is a text input field labeled '"Wind Speed"' with a placeholder text 'Enter a property alias' and a note 'Must be less than 2048 characters.' To the right of this field is a dropdown menu titled 'Notification status'. The dropdown menu is open, showing the option 'ENABLED' selected. Below the dropdown menu, there is a text block stating: 'Notification will be published to topic \$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/assets/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE/properties/a1b2c3d4-5678-90ab-cdef-33333EXAMPLE'.

Você também pode escolher DESABILITADO para desabilitar notificações para a propriedade do ativo.

6. Escolha Salvar.

Ativar notificações de propriedades de ativo (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 `conneceassetId`, use a [ListAssets](#) API para listar todos os ativos de um modelo específico. Use a [DescribeAsset](#) operação para visualizar as propriedades do seu ativo, incluindo propriedades IDs.

Use a [UpdateAssetProperty](#) operação 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. *asset-id* Substitua 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-2222EXAMPLE",  
  "assetName": "Wind Turbine 7",  
  "assetModelId": "a1b2c3d4-5678-90ab-cdef-1111EXAMPLE",  
  "assetProperty": {  
    "id": "a1b2c3d4-5678-90ab-cdef-3333EXAMPLE",  
    "name": "Wind Speed",  
    "alias": "/company/windfarm/3/turbine/7/windspeed",  
    "notification": {  
      "topic": "$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-1111EXAMPLE/  
assets/a1b2c3d4-5678-90ab-cdef-2222EXAMPLE/properties/a1b2c3d4-5678-90ab-  
cdef-3333EXAMPLE",  
      "state": "DISABLED"  
    }  
  }  
}
```

```

    },
    "dataType": "DOUBLE",
    "unit": "m/s",
    "type": {
      "measurement": {}
    }
  }
}

```

2. Execute o seguinte comando para habilitar notificações para a propriedade de ativo. *property-alias* Substitua pelo alias da propriedade da resposta do comando anterior ou omita --property-alias a atualização da 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.

Consulte notificações de propriedades de ativos em AWS IoT SiteWise

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",
        "nullValue": {
            "valueType": "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`
 - `nullValue`

`nullValue`— Uma estrutura com o campo a seguir indicando o tipo do valor da propriedade com valor Nulo e qualidade de `BAD` ou `UNCERTAIN`

- `valueType`— Enumeração de {"B", "D", "S", "I"}

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 valores 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.

Exportar dados para o Amazon S3 com notificações de propriedades de ativo

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.

Para exportar dados de séries temporais de AWS IoT SiteWise, habilite o recurso de camada fria para que os dados sejam armazenados em um bucket do Amazon S3. Consulte [Gerenciar armazenamento de dados em AWS IoT SiteWise](#) para obter detalhes.

Para exportar modelos de ativos e metadados de ativos AWS IoT SiteWise, use o recurso de operações em massa para exportar metadados para um bucket do Amazon S3. Consulte [Operações em massa com ativos e modelos](#) para obter detalhes.

Integre AWS IoT SiteWise com a Grafana

Grafana é uma plataforma de visualização de dados usada para visualizar e monitorar dados em painéis. Na versão 10.4.0 e posterior do Grafana, use o AWS IoT SiteWise plug-in para visualizar seus AWS IoT SiteWise dados de ativos nos painéis do Grafana. Os usuários podem 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 AWS IoT SiteWise plug-in:

- Servidores locais do Grafana

Você pode configurar o AWS IoT SiteWise plug-in 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 Serviço gerenciado para Grafana

Você pode usar o AWS IoT SiteWise plug-in 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 AWS Guia do usuário do Managed Service for Grafana:

- [O que é o Amazon Managed Service for Grafana \(AMG\)?](#)
- [Usando a fonte AWS IoT SiteWise de dados](#)

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](#).



Integre AWS IoT SiteWise e AWS IoT TwinMaker

A integração com AWS IoT TwinMaker concede acesso a funcionalidades robustas AWS 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](#)
- [Integrando e AWS IoT SiteWiseAWS IoT TwinMaker](#)

Habilitar a integração

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 podem ser usadas para permitir ou negar acesso em uma política. Para obter mais informações sobre as ações AWS IoT SiteWise suportadas, consulte [Ações definidas por 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 e AWS 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 ao perfil do IAM:

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

Integrando e AWS IoT SiteWise AWS IoT TwinMaker

Para integrar AWS IoT SiteWise e AWS IoT TwinMaker, você deve ter o seguinte:

- AWS IoT SiteWise função vinculada ao serviço configurada em sua conta

- AWS IoT TwinMaker função vinculada ao serviço configurada em sua conta
- AWS IoT TwinMaker espaço de trabalho com ID `IoTSiteWiseDefaultWorkspace` em sua conta na região.

Para integrar usando o AWS IoT SiteWise console

Ao ver o banner Integração com o AWS IoT TwinMaker no console, escolha Conceder permissão. Os pré-requisitos são criados na conta.

Para integrar usando o AWS CLI

Para integrar AWS IoT SiteWise e AWS IoT TwinMaker usar o AWS CLI, digite os seguintes comandos:

1. Chame `CreateServiceLinkedRole` com um `AWSServiceName` de `iotsitewise.amazonaws.com`.

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

2. Chame `CreateServiceLinkedRole` com um `AWSServiceName` de `iottwinmaker.amazonaws.com`.

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

3. Chame `CreateWorkspace` com um ID de `IoTSiteWiseDefaultWorkspace`.

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

Detectar anomalias com o Lookout for Equipment

Note

A detecção de anomalias só está disponível nas regiões onde 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 machine learning (ML) para monitoramento de equipamentos industriais que detecta comportamento anormal dos equipamentos 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 ter mais informações sobre o Lookout for Equipment, consulte [What is 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 estabelecer uma definição de previsão em um modelo de ativo, especifique os perfis do IAM necessários para que o Lookout for Equipment acesse os dados e as propriedades para enviar ao Lookout for Equipment e envie dados processados ao Amazon S3. Para obter mais informações, consulte [Crie modelos de ativos em AWS IoT SiteWise](#).

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 dos 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 do Lookout for Equipment monitora os dados que recebe dos equipamentos e procura anomalias no comportamento dos equipamentos. 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. Também é possível criar alarmes usando detectores de alarme do modelo de ativo para alertar você sobre o comportamento anormal dos equipamentos.

Tópicos

- [Adicionar uma definição de previsão \(console\)](#)
- [Treinar uma previsão \(console\)](#)
- [Iniciar ou interromper a inferência em uma previsão \(console\)](#)
- [Adicionar uma definição de previsão \(CLI\)](#)

- [Treinar uma previsão e iniciar a inferência \(CLI\)](#)
- [Treinar uma previsão \(CLI\)](#)
- [Iniciar ou interromper a inferência em uma previsão \(CLI\)](#)

Adicionar 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, selecione Modelos e escolha o modelo de ativo para o qual você deseja adicionar a definição de previsão.
3. Escolha Previsões.
4. Escolha Adicionar definição de previsão.
5. Defina detalhes sobre a definição de previsão.
 - a. Insira um Nome exclusivo e uma Descrição para a definição de previsão. Escolha o nome com cuidado, pois depois de criada a definição de previsão, você não poderá mudar o nome.
 - b. Crie ou selecione um Perfil de permissões do IAM que permita que o AWS IoT SiteWise compartilhe os dados de ativos com o Amazon Lookout for Equipment. O perfil deve ter as políticas do IAM e de confiança a seguir. Se precisar de ajuda para criar o perfil, consulte [Criar um perfil do IAM 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. Escolha Próximo.
6. Selecione os atributos de dados (medições, transformações e métricas) que você deseja enviar para o Lookout for Equipment.
 - a. (Opcional) Selecione as medições.
 - b. (Opcional) Selecione as transformações.
 - c. (Opcional) Selecione as métricas.
 - d. Escolha 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 previsão existente que tenha previsões ativas anexadas.

Treinar uma previsão (console)

Depois de adicionar uma definição de previsão a um modelo de ativo, você poderá treinar as previsões que estão nos ativos.

Para treinar uma previsão em AWS IoT SiteWise

1. Navegue até o [console do AWS IoT SiteWise](#).
2. No painel de navegação, selecione Ativos e selecione o ativo que deseja monitorar.
3. Escolha Previsões.
4. Selecione as previsões que deseja treinar.
5. Em Ações, escolha Começar o 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 precisar criar um novo perfil, escolha Criar um novo perfil.
 - b. Em Configurações de dados de treinamento, insira um Intervalo de tempo dos 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 os dados de rotulagem. Para ter mais informações sobre rotulagem de dados, consulte [Labeling your data](#) no Guia do usuário do Amazon Lookout for Equipment.
 - e. Escolha 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 a frequência de upload dos dados e, em Tempo de atraso de compensação, defina a quantidade de buffer a ser usada.
 - b. Escolha Próximo.
7. Revise os detalhes da previsão e escolha Salvar e iniciar.

Iniciar ou interromper a inferência em 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 ter mais informações, consulte [Amazon Lookout for Equipment pricing](#).

Se você adicionou a previsão `lookoutequipment:CreateDataset`, mas não optou por ativá-la após o treinamento, deverá ativá-la para começar a monitorar os ativos.

Como 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 deseja ativar.
5. Em Ações, escolha Iniciar inferência e faça o seguinte:

- a. Em Dados de entrada, em Frequência de upload de dados, defina a frequência de upload dos dados e, em Tempo de atraso de compensação, defina a quantidade de buffer a ser usada.
- b. Escolha Salvar e iniciar.

Como 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 deseja interromper.
5. Em Ações, escolha Interromper inferência.

Adicionar 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 ter mais informações, consulte [Criar um modelo de ativo \(AWS CLI\)](#) e [Criar 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 obter mais informações, consulte [Criar um trabalho de importação AWS IoT SiteWise em massa \(AWS CLI\)](#).

Como 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 ter mais informações sobre como criar um modelo de ativo, consulte [Criar um modelo de ativo \(AWS CLI\)](#).
 - Para ter mais informações sobre como atualizar um modelo de ativo existente, consulte [Atualizar um modelo de ativo ou de componente \(AWS CLI\)](#).
2. Adicione um modelo composto do Lookout for Equipment (`assetModelCompositeModels`) ao modelo de ativo adicionando o código a seguir.
- Substitua *Property* pelo ID das propriedades que deseja incluir. Para obtê-los IDs, 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. Substitua *asset-model-id* pelo 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.

Treinar uma previsão e iniciar a inferência (CLI)

Agora que a definição de previsão está estabelecida, você pode treinar ativos com base nela e iniciar a inferência. Se você quiser treinar a previsão, mas não iniciar a inferência, vá para [Treinar uma previsão \(CLI\)](#). Para treinar a previsão e iniciar a inferência no ativo, você precisará do `assetId` do recurso de destino.

Como treinar e iniciar a inferência da previsão

1. Execute o comando a seguir para encontrar `assetModelCompositeModelId` em `assetModelCompositeModelSummaries`. Substitua *asset-model-id* pelo ID do modelo de ativo criado em [Atualizar um modelo de ativo ou de componente \(AWS CLI\)](#).

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

2. Execute o seguinte comando para encontrar `actionDefinitionId` da ação `TrainingWithInference`. Substitua *asset-model-id* pelo ID usado na etapa anterior e substitua *asset-model-composite-model-id* pelo ID retornado 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* pelo ID do ativo de destino.
- *action-definition-id* com o ID da `TrainingWithInference` ação
- *StartTime* pelo início dos dados de treinamento, fornecido em segundos epoch.
- *EndTime* pelo fim dos dados de treinamento, fornecido em segundos epoch.
- *TargetSamplingRate* pela taxa de amostragem dos dados após o pós-processamento pelo 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
```

Treinar uma previsão (CLI)

Agora que a definição de previsão está estabelecida, você pode treinar ativos com base nela. Para treinar a previsão no ativo, você precisará do `assetId` do recurso de destino.

Como treinar a previsão

1. Execute o comando a seguir para encontrar `assetModelCompositeModelId` em `assetModelCompositeModelSummaries`. Substitua *asset-model-id* pelo ID do modelo de ativo criado em [Atualizar um modelo de ativo ou de componente \(AWS CLI\)](#).

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

2. Execute o seguinte comando para encontrar `actionDefinitionId` da ação Training. Substitua *asset-model-id* pelo ID usado na etapa anterior e substitua *asset-model-composite-model-id* pelo ID retornado 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* pelo ID do ativo de destino.
 - *action-definition-id* pelo ID da ação de treinamento.
 - *StartTime* pelo início dos dados de treinamento, fornecido em segundos epoch.
 - *EndTime* pelo fim dos dados de treinamento, fornecido em segundos epoch.
 - (Opcional) *BucketName* pelo nome do bucket do Amazon S3 que contém os dados de rótulo.
 - (Opcional) *Prefix* pelo prefixo associado ao bucket do Amazon S3.

- *TargetSamplingRate* pela taxa de amostragem dos dados após o pós-processamento pelo 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 seguinte comando 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 um dos seguintes procedimentos:

- 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.

Iniciar ou interromper a inferência em uma previsão (CLI)

Depois que a previsão for treinada, você poderá iniciar a inferência para fazer com que o Lookout for Equipment comece a monitorar os ativos. Para iniciar ou interromper a inferência, você precisará de `assetId` do recurso de destino.

Como iniciar a inferência

1. Execute o comando a seguir para encontrar `assetModelCompositeModelId` em `assetModelCompositeModelSummaries`. Substitua *asset-model-id* pelo ID do modelo de ativo criado em [Atualizar um modelo de ativo ou de componente \(AWS CLI\)](#).

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

2. Execute o seguinte comando para encontrar `actionDefinitionId` da ação Inference. Substitua *asset-model-id* pelo ID usado na etapa anterior e substitua *asset-model-composite-model-id* pelo ID retornado 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* pelo ID do ativo de destino.
- *action-definition-id* pelo ID da ação que dá início à inferência.
- *Offset* pela quantidade de buffer a ser usada.
- *Frequency* pela frequência de upload dos dados.

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

4. Execute o seguinte comando para iniciar a inferência:

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

Como interromper a inferência

1. Execute o comando a seguir para encontrar `assetModelCompositeModelId` em `assetModelCompositeModelSummaries`. Substitua *asset-model-id* pelo ID do modelo de ativo criado em [Atualizar um modelo de ativo ou de componente \(AWS CLI\)](#).

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

2. Execute o seguinte comando para encontrar `actionDefinitionId` da ação Inference. Substitua *asset-model-id* pelo ID usado na etapa anterior e substitua *asset-model-composite-model-id* pelo ID retornado 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* pelo ID do ativo de destino.
- *action-definition-id* pelo ID da ação que dá início à inferência.

```
{  
  "targetResource": {  
    "assetId": "asset-id"  
  },  
  "actionDefinitionId": "action-definition-id",  
  "actionPayload": { "stringValue": "{\"l4EIInference\":{\"inferenceMode\":\"STOP\"}}"  
}
```

4. Execute o seguinte comando para interromper a inferência:

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


Gerencie o armazenamento de dados em AWS IoT SiteWise

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 no nível quente são usados por aplicações industriais que precisam de acesso rápido aos valores mais recentes das medições nos equipamentos. Isso inclui aplicações que visualizam métricas em tempo real com um painel interativo ou aplicações que monitoram operações e acionam 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 maximizar o desempenho e o custo-benefício, defina o período de retenção do nível quente de modo que seja 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 estiver definido, os dados serão armazenados indefinidamente no nível quente.

Nível morno

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 o nível morno para armazenar dados históricos necessários para grandes workloads. Por exemplo, ele é usado para recuperação de dados para analytics, aplicações de business intelligence (BI), ferramentas de relatórios e treinamento de modelos de machine learning (ML). Se habilitar o nível de armazenamento frio, você poderá definir um período de retenção do nível morno. 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 frio usa um bucket do Amazon S3 para armazenar dados que raramente são usados. Com o nível frio habilitado, o AWS IoT SiteWise replica a série temporal, inclusive medições, métricas, transformações, agregados e definições de modelos de ativo a

cada 6 horas. O nível frio é usado para armazenar dados que toleram alta latência de leitura para relatórios e backups históricos.

Tópicos

- [Defina as configurações de armazenamento em AWS IoT SiteWise](#)
- [Solucionar problemas de configurações de armazenamento para AWS IoT SiteWise](#)
- [Caminhos de arquivo e esquemas de dados salvos na camada fria](#)

Defina as configurações de armazenamento em AWS IoT SiteWise

Você pode definir configurações de armazenamento para aceitar o armazenamento do nível morno gerenciado pelo serviço, além de replicar os dados para o nível frio. Para saber mais sobre o período de retenção para os níveis morno e quente, consulte [Impacto 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, os dados serão armazenados indefinidamente no nível quente.
- 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 estiver definido, os dados serão armazenados indefinidamente no nível morno.

Note

Para melhorar o desempenho de consulta, defina um período de retenção do nível quente com armazenamento de nível morno.

Impacto da retenção de dados no armazenamento dos níveis quente e morno

- Quando você diminui o período de retenção do armazenamento do nível quente, os dados são movidos permanentemente do nível quente para o nível morno ou frio. Quando você diminui o período de retenção do nível morno, os dados são movidos para o nível frio e excluídos permanentemente do nível morno.
- 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 nível quente for inicialmente definido para 30 dias, depois for aumentado para 60 dias, serão necessários 30 dias para que o armazenamento de nível quente contenha dados equivalentes a 60 dias.

Tópicos

- [Definir configurações de armazenamento para nível morno \(console\)](#)
- [Definir configurações de armazenamento para nível morno \(AWS CLI\)](#)
- [Definir configurações de armazenamento para nível frio \(console\)](#)
- [Definir configurações de armazenamento para nível frio \(AWS CLI\)](#)

Definir configurações de armazenamento para nível morno (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 nível quente, faça o seguinte:

- Se quiser definir um período de retenção para armazenamento dos dados no nível quente antes que eles sejam excluídos e movidos para o armazenamento do nível morno gerenciado pelo serviço, escolha Habilitar 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 do nível morno, faça o seguinte:

- Para aceitar o armazenamento de nível morno, selecione Confirmo a opção de armazenamento de nível morno para aceitar o armazenamento de nível morno.
- (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 aceita o nível morno, a configuração só é exibida uma vez.
- Para definir a retenção do nível quente, você deve ter um armazenamento de nível morno 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 morno, você deve ter um armazenamento de nível frio.

7. Escolha Salvar para salvar as configurações de armazenamento.

Na seção Armazenamento do AWS IoT SiteWise , o Armazenamento de nível morno está em um destes estados:

- **Habilitado:** se os dados existiam antes do período de retenção do nível quente, o AWS IoT SiteWise move os dados para o nível morno.
- **Desabilitado:** o armazenamento de nível morno está desabilitado.

Definir configurações de armazenamento para nível morno (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 da configuração de armazenamento atual executando o seguinte comando:

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

Exemplo resposta sem a configuração de nível frio existente

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

Exemplo resposta com a configuração de nível frio existente

```
{
  "storageType": "MULTI_LAYER_STORAGE",
  "multiLayerStorage": {
    "customerManagedS3Storage": {
      "s3ResourceArn": "arn:aws:s3:::amzn-s3-demo-bucket/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
  }
}
```

O trecho `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 o armazenamento de nível frio estiver habilitado, consulte [Definir configurações de armazenamento com a AWS CLI e um nível frio existente](#).

Definir configurações de armazenamento com a AWS CLI e um nível frio 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 que contém a configuração de armazenamento do AWS IoT SiteWise .

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

Example AWS IoT SiteWise configuração de armazenamento

- Substitua *amzn-s3-demo-bucket* pelo nome do bucket do Amazon S3.
- *prefix* Substitua pelo prefixo do Amazon S3.
- *aws-account-id* Substitua pelo ID AWS da sua conta.
- *role-name* Substitua pelo nome da função de acesso do Amazon S3 que permite enviar dados AWS IoT SiteWise para o Amazon S3.
- *hot-tier-retention-in-days* Substitua por um número inteiro maior ou igual a 30 dias.
- *warm-tier-retention-in-days* Substitua 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:::amzn-s3-demo-bucket/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 configurações de armazenamento para 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:::amzn-s3-demo-bucket",
```

```

    "arn:aws:s3:::amzn-s3-demo-bucket/*"
  ]
}
]
}

```

Substitua amzn-s3-demo-bucket pelo nome do bucket do Amazon S3.

- Se o bucket do Amazon S3 for criptografado usando uma chave KMS gerenciada pelo cliente, a chave KMS deverá ter uma política de acesso com uma função do IAM para operações. kms:Decrypt kms:GenerateDataKey

- Para configurar o nível quente, consulte a etapa 5 em [Definir configurações de armazenamento para nível morno \(console\)](#).
- (Opcional) Para Integração AWS IoT Analytics , faça o seguinte:

Note

Aviso de fim do suporte: em 15 de dezembro de 2025, AWS encerrará o suporte para AWS IoT Analytics. Depois de 15 de dezembro de 2025, você não poderá mais acessar o AWS IoT Analytics console ou AWS IoT Analytics os recursos. Para obter mais informações, consulte [AWS IoT Analytics Fim do suporte](#).

- Se você quiser usar AWS IoT Analytics para consultar seus dados, escolha Armazenamento de AWS IoT Analytics dados ativado.
- 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.

- Escolha 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 obter mais informações, consulte [Monitore com Amazon CloudWatch Logs](#).
- **Desabilitado** — O armazenamento em camada fria está desabilitado.

Definir configurações de armazenamento para 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: *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 de armazenamento

- Substitua *amzn-s3-demo-bucket* pelo nome do bucket do Amazon S3.
- *prefix* Substitua pelo prefixo do Amazon S3.
- *aws-account-id* Substitua pelo ID AWS da sua conta.
- *role-name* Substitua pelo nome da função de acesso do Amazon S3 que permite enviar dados AWS IoT SiteWise 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:::amzn-s3-demo-bucket/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:

Exemplo 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:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ]
    }
  ]
}

```

Substitua amzn-s3-demo-bucket pelo nome do bucket do Amazon S3.

- Se o bucket do Amazon S3 for criptografado usando uma chave KMS gerenciada pelo cliente, a chave KMS deverá ter uma política de acesso com uma função do IAM para operações. `kms:Decrypt` `kms:GenerateDataKey`

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:::amzn-s3-demo-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)

Note

Aviso de fim do suporte: em 15 de dezembro de 2025, AWS encerrará o suporte para AWS IoT Analytics. Depois de 15 de dezembro de 2025, você não poderá mais acessar o AWS IoT Analytics console ou AWS IoT Analytics os recursos. Para obter mais informações, consulte [AWS IoT Analytics Fim do suporte](#).

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 AWS IoT Analytics APIs 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 do 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: *file-name* Substitua pelo nome do arquivo que contém a configuração do 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 do 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 *amzn-s3-demo-bucket* 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": "amzn-s3-demo-bucket"
      }
    }
  },
  "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 para AWS IoT SiteWise

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 do Amazon S3 entre regiões](#)

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:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ]
    }
  ]
}
```

Substitua amzn-s3-demo-bucket 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 do Amazon S3 entre regiões

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 especifica 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. 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:

Componente do caminho	Descrição
	• O prefixo <code>raw</code>. • O valor <code>timeSeriesId</code> . • 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: <code>GOOD</code>, <code>BAD</code> e <code>UNCERTAIN</code> . Para obter mais informações, consulte AssetPropertyValue na Referência de APIs do AWS IoT SiteWise . O arquivo é salvo no formato <code>.avro</code> usando a compressão Rápida.

Exemplo 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:

AWS IoT SiteWise aconselha os clientes a implementarem o suporte para a evolução do esquema em sistemas que leem dados brutos do nível frio, pois podem ser introduzidos campos adicionais no futuro.

Os dados nulos são representados como todos os campos de valor sendo nulos. No entanto, os clientes ainda receberão o tipo de dados correto ao fazer consultas com AWS IoT SiteWise APIs.

Nome do campo	Tipos suportados	Tipo padrão	Descrição
<code>seriesId</code>	<code>string</code>	N/A	A ID que identifica os dados de

Nome do campo	Tipos suportados	Tipo padrão	Descrição
			série temporais do equipamento (medições). Você pode usar esse campo para unir dados brutos e metadados de ativos em consultas.
<code>timeInSeconds</code>	<code>long</code>	N/D	O carimbo de data e hora, em segundos, no formato de época do Unix. Os dados fracionários de nanossegundos são fornecidos por <code>offsetInNanos</code> .
<code>offsetInNanos</code>	<code>long</code>	N/D	O deslocamento em nanossegundos de <code>timeInSeconds</code> .
<code>quality</code>	<code>string</code>	N/D	A qualidade do valor de série temporal.
<code>doubleValue</code>	<code>double</code> ou <code>null</code>	<code>null</code>	Dados de séries temporais tipo duplo (número de ponto flutuante).
<code>stringValue</code>	<code>string</code> ou <code>null</code>	<code>null</code>	Dados de séries temporais tipo string (sequência de caracteres).

Nome do campo	Tipos suportados	Tipo padrão	Descrição
<code>integerValue</code>	<code>int</code> ou <code>null</code>	<code>null</code>	Dados de séries temporais tipo inteiro (número inteiro).
<code>booleanValue</code>	<code>boolean</code> ou <code>null</code>	<code>null</code>	Dados de séries temporais tipo Booleanos (verdadeiro ou falso).
<code>jsonValue</code>	<code>string</code> ou <code>null</code>	<code>null</code>	Dados de séries temporais do tipo JSON (tipos de dados complexos armazenados como string).
<code>recordVersion</code>	<code>long</code> ou <code>null</code>	<code>null</code>	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.

Exemplo 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,
  "recordVersion": 1
},
{
  "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,
  "recordVersion": 2
}
```

```
{
  "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": null
  }
},
{
  "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": null
  }
},
{
  "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": null
  }
}
```

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 especifica 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.
seriesBucket	Um número hexadecimal entre 00 e ff. Esse número é derivado de timeSeriesId . Essa

Componente do caminho	Descrição
	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. <code>seriesBucket</code> e <code>timeSeriesBucket</code> nos metadados do ativo são o mesmo número.
<code>startYear</code>	O ano do horário de início exclusivo associado aos dados de séries temporais.
<code>startMonth</code>	O mês do horário de início exclusivo associado aos dados de séries temporais.
<code>startDay</code>	O dia do mês do horário de início exclusivo associado aos dados de séries temporais.
<code>fileName</code>	O nome do arquivo usa o caractere sublinhado (<code>_</code>) como delimitador para separar: • O prefixo <code>raw</code>. • O valor <code>timeSeriesId</code> . • 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: <code>GOOD</code>, <code>BAD</code> e <code>UNCERTAIN</code> . Para obter mais informações, consulte AssetPropertyValue na Referência de APIs do AWS IoT SiteWise . O arquivo é salvo no formato <code>.avro</code> usando a compressão Rápida.

Exemplo caminho do arquivo para métricas na camada fria

```
keyPrefix/agg/startYear=2021/startMonth=1/startDay=2/seriesBucket=a2/  
agg_7020c8e2-e6db-40fa-9845-ed0ddddd4c77d_95e63da7-d34e-43e1-  
bc6f-1b490154b07a_1609577700_G00D.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 identifique dados de séries temporais de equipamentos, métricas ou transformações. 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 <code>offsetInNanos</code> .
offsetInNanos	long	N/D	O deslocamento em nanossegundos de <code>timeInSeconds</code> .

Nome do campo	Tipos suportados	Tipo padrão	Descrição
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.
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.

Nome do campo	Tipos suportados	Tipo padrão	Descrição
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": "1s",
  "value": 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": "1s",
  "value": 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": "1s",
  "value": 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": "1s",
  "value": 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": "1s",
  "value": 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 de ativo são salvos no nível frio 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.

Exemplo 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
<code>assetId</code>	ID do ativo.
<code>assetName</code>	O nome do ativo.
<code>assetExternalId</code>	O ID externo do ativo.
<code>assetModelId</code>	ID do modelo de ativo usada para criá-lo.
<code>assetModelName</code>	O nome do modelo do ativo.
<code>assetModelExternalId</code>	O ID externo do modelo de ativo.
<code>assetPropertyId</code>	A ID da propriedade do ativo.
<code>assetPropertyName</code>	O nome da propriedade do ativo.
<code>assetPropertyExternalId</code>	O ID externo da propriedade de ativo.
<code>assetPropertyDataType</code>	O tipo de dados da propriedade do ativo.
<code>assetPropertyUnit</code>	A unidade da propriedade do ativo (por exemplo, Newtons e RPM).
<code>assetPropertyAlias</code>	O alias que identifica a propriedade de ativo, como um caminho de fluxo de dados do servidor OPC UA (por exemplo, <code>/company/windfarm/3/turbine/7/temperature</code>).
<code>timeSeriesId</code>	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.
<code>timeSeriesBucket</code>	Um número hexadecimal entre 00 e ff. Esse número é derivado de <code>timeSeriesId</code> . Essa partição é usada para aumentar a taxa de transferência ao AWS IoT SiteWise gravar

Nome do campo	Descrição
	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. <code>timeSeriesBucket</code> e <code>seriesBucket</code> no caminho do arquivo para os dados brutos são o mesmo número.
<code>assetCompositeModelId</code>	O ID do modelo composto.
<code>assetCompositeModelExternalId</code>	O ID externo do modelo composto.
<code>assetCompositeModelDescription</code>	A descrição do modelo composto.
<code>assetCompositeModelName</code>	O nome do modelo composto.
<code>assetCompositeModelType</code>	O tipo do modelo composto. Para modelos compostos de alarme, este tipo é <code>AWS/ALARM</code> .
<code>assetCreationDate</code>	A data na qual o ativo foi criado, no horário de época do Unix.
<code>assetLastUpdateDate</code>	A data na qual o ativo foi atualizado pela última vez, no horário de época do Unix.
<code>assetStatusErrorCode</code>	O código do erro.
<code>assetStatusErrorMessage</code>	A mensagem de erro.
<code>assetStatusState</code>	O status atual do ativo.

Exemplo 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 no nível frio 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 [DescribeAsset](#) API.

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 especifica 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_hierarchy_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.

Exemplo 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-cdcccfc9747a0.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.
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
```

Exemplo caminho do arquivo para o arquivo de índice de armazenamento de dados

```
keyPrefix/index/series=7020c8e2-e6db-40fa-9845-ed0ddddd4c77d_95e63da7-  
d34e-43e1-bc6f-1b490154b07a/startYear=2022/startMonth=02/startDay=03/  
index_7020c8e2-e6db-40fa-9845-ed0ddddd4c77d_95e63da7-d34e-43e1-  
bc6f-1b490154b07a_1643846400_G00D
```

Exemplos de código para AWS IoT SiteWise usar AWS SDKs

Os exemplos de código a seguir mostram como usar AWS IoT SiteWise com um kit AWS de desenvolvimento de software (SDK).

As noções básicas são exemplos de código que mostram como realizar as operações essenciais em um serviço.

Ações são trechos de código de programas maiores e devem ser executadas em contexto. Embora as ações mostrem como chamar perfis de serviço individuais, você pode ver as ações no contexto em seus cenários relacionados.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando esse serviço com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Conceitos básicos

Olá AWS IoT SiteWise

O exemplo de código a seguir mostra como começar a usar o AWS IoT SiteWise.

Java

SDK para Java 2.x

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
public class HelloSitewise {
    private static final Logger logger =
        LoggerFactory.getLogger(HelloSitewise.class);
    public static void main(String[] args) {
        fetchAssetModels();
    }
}
```

```

/**
 * Fetches asset models using the provided {@link IoTSiteWiseAsyncClient}.
 */
public static void fetchAssetModels() {
    IoTSiteWiseAsyncClient siteWiseAsyncClient =
IoTSiteWiseAsyncClient.create();
    ListAssetModelsRequest assetModelsRequest =
ListAssetModelsRequest.builder()
        .assetModelTypes(AssetModelType.ASSET_MODEL)
        .build();

    // Asynchronous paginator - process paginated results.
    ListAssetModelsPublisher listModelsPaginator =
siteWiseAsyncClient.listAssetModelsPaginator(assetModelsRequest);
    CompletableFuture<Void> future = listModelsPaginator.subscribe(response -
> {
        response.assetModelSummaries().forEach(assetSummary ->
            logger.info("Asset Model Name: {} ", assetSummary.name())
        );
    });

    // Wait for the asynchronous operation to complete
    future.join();
}
}

```

- Para obter detalhes da API, consulte [ListAssetModels](#) na Referência AWS SDK for Java 2.x da API.

JavaScript

SDK para JavaScript (v3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
import {
```

```
paginateListAssetModels,
IoTSiteWiseClient,
} from "@aws-sdk/client-iotsitewise";

// Call ListDocuments and display the result.
export const main = async () => {
  const client = new IoTSiteWiseClient();
  const listAssetModelsPaginated = [];
  console.log(
    "Hello, AWS Systems Manager! Let's list some of your documents:\n",
  );
  try {
    // The paginate function is a wrapper around the base command.
    const paginator = paginateListAssetModels({ client }, { maxResults: 5 });
    for await (const page of paginator) {
      listAssetModelsPaginated.push(...page.assetModelSummaries);
    }
  } catch (caught) {
    console.error(`There was a problem saying hello: ${caught.message}`);
    throw caught;
  }
  for (const { name, creationDate } of listAssetModelsPaginated) {
    console.log(`${name} - ${creationDate}`);
  }
};

// Call function if run directly.
import { fileURLToPath } from "node:url";
if (process.argv[1] === fileURLToPath(import.meta.url)) {
  main();
}
```

- Para obter detalhes da API, consulte [ListAssetModels](#) a Referência AWS SDK para JavaScript da API.

Python

SDK para Python (Boto3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
import boto3

def hello_iot_sitewise(iot_sitewise_client):
    """
    Use the AWS SDK for Python (Boto3) to create an AWS IoT SiteWise
    client and list the asset models in your account.
    This example uses the default settings specified in your shared credentials
    and config files.

    :param iot_sitewise_client: A Boto3 AWS IoT SiteWise Client object. This
    object wraps
                                the low-level AWS IoT SiteWise service API.
    """
    print("Hello, AWS IoT SiteWise! Let's list some of your asset models:\n")
    paginator = iot_sitewise_client.get_paginator("list_asset_models")
    page_iterator = paginator.paginate(PaginationConfig={"MaxItems": 10})

    asset_model_names: [str] = []
    for page in page_iterator:
        for asset_model in page["assetModelSummaries"]:
            asset_model_names.append(asset_model["name"])

    print(f"{len(asset_model_names)} asset model(s) retrieved.")
    for asset_model_name in asset_model_names:
        print(f"\t{asset_model_name}")

if __name__ == "__main__":
    hello_iot_sitewise(boto3.client("iotsitewise"))
```

- Para obter detalhes da API, consulte a [ListAssetModels](#)Referência da API AWS SDK for Python (Boto3).

Exemplos de código

- [Exemplos básicos de AWS IoT SiteWise uso AWS SDKs](#)
 - [Olá AWS IoT SiteWise](#)
 - [Aprenda o básico AWS IoT SiteWise com um SDK AWS](#)
 - [Ações para AWS IoT SiteWise usar AWS SDKs](#)
 - [Use BatchPutAssetPropertyValue com um AWS SDK ou CLI](#)
 - [Use CreateAsset com um AWS SDK ou CLI](#)
 - [Use CreateAssetModel com um AWS SDK ou CLI](#)
 - [Use CreateGateway com um AWS SDK ou CLI](#)
 - [Use CreatePortal com um AWS SDK ou CLI](#)
 - [Use DeleteAsset com um AWS SDK ou CLI](#)
 - [Use DeleteAssetModel com um AWS SDK ou CLI](#)
 - [Use DeleteGateway com um AWS SDK ou CLI](#)
 - [Use DeletePortal com um AWS SDK ou CLI](#)
 - [Use DescribeAssetModel com um AWS SDK ou CLI](#)
 - [Use DescribeGateway com um AWS SDK ou CLI](#)
 - [Use DescribePortal com um AWS SDK ou CLI](#)
 - [Use GetAssetPropertyValue com um AWS SDK ou CLI](#)
 - [Use ListAssetModels com um AWS SDK ou CLI](#)

Exemplos básicos de AWS IoT SiteWise uso AWS SDKs

Os exemplos de código a seguir mostram como usar o básico do AWS IoT SiteWise with AWS SDKs.

Exemplos

- [Olá AWS IoT SiteWise](#)
- [Aprenda o básico AWS IoT SiteWise com um SDK AWS](#)
- [Ações para AWS IoT SiteWise usar AWS SDKs](#)
 - [Use BatchPutAssetPropertyValue com um AWS SDK ou CLI](#)

- [Use CreateAsset com um AWS SDK ou CLI](#)
- [Use CreateAssetModel com um AWS SDK ou CLI](#)
- [Use CreateGateway com um AWS SDK ou CLI](#)
- [Use CreatePortal com um AWS SDK ou CLI](#)
- [Use DeleteAsset com um AWS SDK ou CLI](#)
- [Use DeleteAssetModel com um AWS SDK ou CLI](#)
- [Use DeleteGateway com um AWS SDK ou CLI](#)
- [Use DeletePortal com um AWS SDK ou CLI](#)
- [Use DescribeAssetModel com um AWS SDK ou CLI](#)
- [Use DescribeGateway com um AWS SDK ou CLI](#)
- [Use DescribePortal com um AWS SDK ou CLI](#)
- [Use GetAssetPropertyValue com um AWS SDK ou CLI](#)
- [Use ListAssetModels com um AWS SDK ou CLI](#)

Olá AWS IoT SiteWise

O exemplo de código a seguir mostra como começar a usar o AWS IoT SiteWise.

Java

SDK para Java 2.x

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
public class HelloSitewise {
    private static final Logger logger =
        LoggerFactory.getLogger(HelloSitewise.class);
    public static void main(String[] args) {
        fetchAssetModels();
    }

    /**
```



```

    * Fetches asset models using the provided {@link IoTSiteWiseAsyncClient}.
    */
    public static void fetchAssetModels() {
        IoTSiteWiseAsyncClient siteWiseAsyncClient =
        IoTSiteWiseAsyncClient.create();
        ListAssetModelsRequest assetModelsRequest =
        ListAssetModelsRequest.builder()
            .assetModelTypes(AssetModelType.ASSET_MODEL)
            .build();

        // Asynchronous paginator - process paginated results.
        ListAssetModelsPublisher listModelsPaginator =
        siteWiseAsyncClient.listAssetModelsPaginator(assetModelsRequest);
        CompletableFuture<Void> future = listModelsPaginator.subscribe(response -
> {
            response.assetModelSummaries().forEach(assetSummary ->
                logger.info("Asset Model Name: {} ", assetSummary.name())
            );
        });

        // Wait for the asynchronous operation to complete
        future.join();
    }
}

```

- Para obter detalhes da API, consulte [ListAssetModels](#) na Referência AWS SDK for Java 2.x da API.

JavaScript

SDK para JavaScript (v3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```

import {
    paginateListAssetModels,

```

```
IoTSiteWiseClient,
} from "@aws-sdk/client-iotsitewise";

// Call ListDocuments and display the result.
export const main = async () => {
  const client = new IoTSiteWiseClient();
  const listAssetModelsPaginated = [];
  console.log(
    "Hello, AWS Systems Manager! Let's list some of your documents:\n",
  );
  try {
    // The paginate function is a wrapper around the base command.
    const paginator = paginateListAssetModels({ client }, { maxResults: 5 });
    for await (const page of paginator) {
      listAssetModelsPaginated.push(...page.assetModelSummaries);
    }
  } catch (caught) {
    console.error(`There was a problem saying hello: ${caught.message}`);
    throw caught;
  }
  for (const { name, creationDate } of listAssetModelsPaginated) {
    console.log(`${name} - ${creationDate}`);
  }
};

// Call function if run directly.
import { fileURLToPath } from "node:url";
if (process.argv[1] === fileURLToPath(import.meta.url)) {
  main();
}
```

- Para obter detalhes da API, consulte [ListAssetModels](#) na Referência AWS SDK para JavaScript da API.

Python

SDK para Python (Boto3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
import boto3

def hello_iot_sitewise(iot_sitewise_client):
    """
    Use the AWS SDK for Python (Boto3) to create an AWS IoT SiteWise
    client and list the asset models in your account.
    This example uses the default settings specified in your shared credentials
    and config files.

    :param iot_sitewise_client: A Boto3 AWS IoT SiteWise Client object. This
    object wraps
                                the low-level AWS IoT SiteWise service API.
    """
    print("Hello, AWS IoT SiteWise! Let's list some of your asset models:\n")
    paginator = iot_sitewise_client.get_paginator("list_asset_models")
    page_iterator = paginator.paginate(PaginationConfig={"MaxItems": 10})

    asset_model_names: [str] = []
    for page in page_iterator:
        for asset_model in page["assetModelSummaries"]:
            asset_model_names.append(asset_model["name"])

    print(f"{len(asset_model_names)} asset model(s) retrieved.")
    for asset_model_name in asset_model_names:
        print(f"\t{asset_model_name}")

if __name__ == "__main__":
    hello_iot_sitewise(boto3.client("iotsitewise"))
```

- Para obter detalhes da API, consulte a [ListAssetModels](#) Referência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando esse serviço com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Aprenda o básico AWS IoT SiteWise com um SDK AWS

Os exemplos de código a seguir mostram como:

- Crie um modelo AWS IoT SiteWise de ativo.
- Crie um AWS IoT SiteWise ativo.
- Recupere os valores da ID da propriedade.
- Envie dados para um AWS IoT SiteWise ativo.
- Recupere o valor da propriedade do AWS IoT SiteWise ativo.
- Crie um AWS IoT SiteWise portal.
- Crie um AWS IoT SiteWise gateway.
- Descreva o AWS IoT SiteWise Gateway.
- Exclua os AWS IoT SiteWise ativos.

Java

SDK para Java 2.x

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

Execute um cenário interativo demonstrando AWS IoT SiteWise recursos.

```
public class SitewiseScenario {  
  
    public static final String DASHES = new String(new char[80]).replace("\0",  
        "-");  
}
```

```
private static final Logger logger =
LoggerFactory.getLogger(SitewiseScenario.class);
static Scanner scanner = new Scanner(System.in);

private static final String ROLES_STACK = "RoleSitewise";

static SitewiseActions sitewiseActions = new SitewiseActions();

public static void main(String[] args) throws Throwable {
    Scanner scanner = new Scanner(System.in);
    String contactEmail = "user@mydomain.com"; // Change email address.
    String assetModelName = "MyAssetModel1";
    String assetName = "MyAsset1" ;
    String portalName = "MyPortal1" ;
    String gatewayName = "MyGateway1" ;
    String myThing = "MyThing1" ;

    logger.info("""
        AWS IoT SiteWise is a fully managed software-as-a-service (SaaS)
that
        makes it easy to collect, store, organize, and monitor data from
industrial equipment and processes.
        It is designed to help industrial and manufacturing organizations
collect data from their equipment and
        processes, and use that data to make informed decisions about their
operations.

        One of the key features of AWS IoT SiteWise is its ability to connect
to a wide range of industrial
        equipment and systems, including programmable logic controllers
(PLCs), sensors, and other
        industrial devices. It can collect data from these devices and
organize it into a unified data model,
        making it easier to analyze and gain insights from the data. AWS IoT
SiteWise also provides tools for
        visualizing the data, setting up alarms and alerts, and generating
reports.

        Another key feature of AWS IoT SiteWise is its ability to scale to
handle large volumes of data.
        It can collect and store data from thousands of devices and process
millions of data points per second,
```

making it suitable for large-scale industrial operations. Additionally, AWS IoT SiteWise is designed to be secure and compliant, with features like role-based access controls, data encryption, and integration with other AWS services for additional security and compliance features.

Let's get started...
 """);

```
waitForInputToContinue(scanner);
logger.info(DASHES);

try {
    runScenario(assetModelName, assetName, portalName, contactEmail,
gatewayName, myThing);
} catch (RuntimeException e) {
    logger.info(e.getMessage());
}
}
```

```
public static void runScenario(String assetModelName, String assetName,
String portalName, String contactEmail, String gatewayName, String myThing)
throws Throwable {
    logger.info("Use AWS CloudFormation to create an IAM role that is
required for this scenario.");
    CloudFormationHelper.deployCloudFormationStack(ROLES_STACK);
    Map<String, String> stackOutputs =
CloudFormationHelper.getStackOutputsAsync(ROLES_STACK).join();
    String iamRole = stackOutputs.get("SitewiseRoleArn");
    logger.info("The ARN of the IAM role is {}",iamRole);
    logger.info(DASHES);

    logger.info(DASHES);
    logger.info("1. Create an AWS SiteWise Asset Model");
    logger.info("""
        An AWS IoT SiteWise Asset Model is a way to represent the physical
assets, such as equipment,
        processes, and systems, that exist in an industrial environment.
This model provides a structured and
        hierarchical representation of these assets, allowing users to
define the relationships and properties
        of each asset.
```

```

        This scenario creates two asset model properties: temperature and
        humidity.

        """);
        waitForInputToContinue(scanner);
        String assetModelId = null;
        try {
            CreateAssetModelResponse response =
sitewiseActions.createAssetModelAsync(assetModelName).join();
            assetModelId = response.assetModelId();
            logger.info("Asset Model successfully created. Asset Model ID: {}. ",
assetModelId);
        } catch (CompletionException ce) {
            Throwable cause = ce.getCause();
            if (cause instanceof ResourceAlreadyExistsException) {
                try {
                    assetModelId =
sitewiseActions.getAssetModelIdAsync(assetModelName).join();
                    logger.info("The Asset Model {} already exists. The id of the
existing model is {}. Moving on...", assetModelName, assetModelId);
                } catch (CompletionException cex) {
                    logger.error("Exception thrown acquiring the asset model id:
{}", cex.getCause().getCause(), cex);
                    return;
                }
            } else {
                logger.info("An unexpected error occurred: " +
cause.getMessage(), cause);
                return;
            }
        }
        waitForInputToContinue(scanner);

        logger.info(DASHES);
        logger.info("2. Create an AWS IoT SiteWise Asset");
        logger.info("""
            The IoT SiteWise model that we just created defines the structure
            and metadata for your physical assets.
            Now we create an asset from the asset model.

            """);
        logger.info("Let's wait 30 seconds for the asset to be ready.");
        countdown(30);
        waitForInputToContinue(scanner);
        String assetId;

```

```

        try {
            CreateAssetResponse response =
sitewiseActions.createAssetAsync(assetName, assetModelId).join();
            assetId = response.assetId();
            logger.info("Asset created with ID: {}", assetId);
        } catch (CompletionException ce) {
            Throwable cause = ce.getCause();
            if (cause instanceof ResourceNotFoundException) {
                logger.info("The asset model id was not found: {}",
cause.getMessage(), cause);
            } else {
                logger.info("An unexpected error occurred: {}",
cause.getMessage(), cause);
            }
            return;
        }
        waitForInputToContinue(scanner);
        logger.info(DASHES);

        logger.info(DASHES);
        logger.info("3. Retrieve the property ID values");
        logger.info("""
            To send data to an asset, we need to get the property ID values. In
this scenario, we access the
            temperature and humidity property ID values.
            """);
        waitForInputToContinue(scanner);
        Map<String, String> propertyIds = null;
        try {
            propertyIds = sitewiseActions.getPropertyIds(assetModelId).join();
        } catch (CompletionException ce) {
            Throwable cause = ce.getCause();
            if (cause instanceof IoTSiteWiseException) {
                logger.error("IoTSiteWiseException occurred: {}",
cause.getMessage(), ce);
            } else {
                logger.error("An unexpected error occurred: {}",
cause.getMessage(), ce);
            }
            return;
        }
        String humPropId = propertyIds.get("Humidity");
        logger.info("The Humidity property Id is {}", humPropId);
        String tempPropId = propertyIds.get("Temperature");

```



```

logger.info("The Temperature property Id is {}", tempPropId);

waitForInputToContinue(scanner);
logger.info(DASHES);

logger.info(DASHES);
logger.info("4. Send data to an AWS IoT SiteWise Asset");
logger.info("
    By sending data to an IoT SiteWise Asset, you can aggregate data
from
    multiple sources, normalize the data into a standard format, and
store it in a
    centralized location. This makes it easier to analyze and gain
insights from the data.

    In this example, we generate sample temperature and humidity data and
send it to the AWS IoT SiteWise asset.

    ");
waitForInputToContinue(scanner);
try {
    sitewiseActions.sendDataToSiteWiseAsync(assetId, tempPropId,
humPropId).join();
    logger.info("Data sent successfully.");
} catch (CompletionException ce) {
    Throwable cause = ce.getCause();
    if (cause instanceof ResourceNotFoundException) {
        logger.error("The AWS resource was not found: {}",
cause.getMessage(), cause);
    } else {
        logger.error("An unexpected error occurred: {}",
cause.getMessage(), cause);
    }
    return;
}
waitForInputToContinue(scanner);
logger.info(DASHES);

logger.info(DASHES);
logger.info("5. Retrieve the value of the IoT SiteWise Asset property");
logger.info("
    IoT SiteWise is an AWS service that allows you to collect, process,
and analyze industrial data

```

```

        from connected equipment and sensors. One of the key benefits of
        reading an IoT SiteWise property
        is the ability to gain valuable insights from your industrial data.

        """);
        waitForInputToContinue(scanner);
        try {
            Double assetVal = sitewiseActions.getAssetPropValueAsync(tempPropId,
assetId).join();
            logger.info("The property name is: {}", "Temperature");
            logger.info("The value of this property is: {}", assetVal);

            waitForInputToContinue(scanner);

            assetVal = sitewiseActions.getAssetPropValueAsync(humPropId,
assetId).join();
            logger.info("The property name is: {}", "Humidity");
            logger.info("The value of this property is: {}", assetVal);
        } catch (CompletionException ce) {
            Throwable cause = ce.getCause();
            if (cause instanceof ResourceNotFoundException) {
                logger.info("The AWS resource was not found: {}",
cause.getMessage(), cause);
            } else {
                logger.info("An unexpected error occurred: {}",
cause.getMessage(), cause);
            }
            return;
        }
        waitForInputToContinue(scanner);
        logger.info(DASHES);

        logger.info(DASHES);
        logger.info("6. Create an IoT SiteWise Portal");
        logger.info("""
            An IoT SiteWise Portal allows you to aggregate data from multiple
            industrial sources,
            such as sensors, equipment, and control systems, into a centralized
            platform.

            """);
        waitForInputToContinue(scanner);
        String portalId;
        try {

```

```

        portalId = sitewiseActions.createPortalAsync(portalName, iamRole,
contactEmail).join();
        logger.info("Portal created successfully. Portal ID {}", portalId);
    } catch (CompletionException ce) {
        Throwable cause = ce.getCause();
        if (cause instanceof IoTSiteWiseException siteWiseEx) {
            logger.error("IoT SiteWise error occurred: Error message: {},
Error code {}",
                        siteWiseEx.getMessage(),
siteWiseEx.awsErrorDetails().errorCode(), siteWiseEx);
        } else {
            logger.error("An unexpected error occurred: {}",
cause.getMessage());
        }
        return;
    }
    waitForInputToContinue(scanner);
    logger.info(DASHES);

    logger.info(DASHES);
    logger.info("7. Describe the Portal");
    logger.info(""""
        In this step, we get a description of the portal and display the
portal URL.
        """);
    waitForInputToContinue(scanner);
    try {
        String portalUrl =
sitewiseActions.describePortalAsync(portalId).join();
        logger.info("Portal URL: {}", portalUrl);
    } catch (CompletionException ce) {
        Throwable cause = ce.getCause();
        if (cause instanceof ResourceNotFoundException notFoundException) {
            logger.error("A ResourceNotFoundException occurred: Error
message: {}, Error code {}",
                        notFoundException.getMessage(),
notFoundException.awsErrorDetails().errorCode(), notFoundException);
        } else {
            logger.error("An unexpected error occurred: {}",
cause.getMessage());
        }
        return;
    }
    waitForInputToContinue(scanner);

```

```

        logger.info(DASHES);

        logger.info(DASHES);
        logger.info("8. Create an IoT SiteWise Gateway");
        logger.info(
            ""
            IoT SiteWise Gateway serves as the bridge between industrial
equipment, sensors, and the
            cloud-based IoT SiteWise service. It is responsible for securely
collecting, processing, and
            transmitting data from various industrial assets to the IoT
SiteWise platform,
            enabling real-time monitoring, analysis, and optimization of
industrial operations.

            "");
        waitForInputToContinue(scanner);
        String gatewayId = "";
        try {
            gatewayId = sitewiseActions.createGatewayAsync(gatewayName,
myThing).join();
            logger.info("Gateway creation completed successfully. id is {}",
gatewayId );
        } catch (CompletionException ce) {
            Throwable cause = ce.getCause();
            if (cause instanceof IoTSiteWiseException siteWiseEx) {
                logger.error("IoT SiteWise error occurred: Error message: {},
Error code {}",
                    siteWiseEx.getMessage(),
siteWiseEx.awsErrorDetails().errorCode(), siteWiseEx);
            } else {
                logger.error("An unexpected error occurred: {}",
cause.getMessage());
            }
            return;
        }
        logger.info(DASHES);
        logger.info(DASHES);

        logger.info("9. Describe the IoT SiteWise Gateway");
        waitForInputToContinue(scanner);
        try {
            sitewiseActions.describeGatewayAsync(gatewayId)
                .thenAccept(response -> {

```

```

        logger.info("Gateway Name: {}", response.gatewayName());
        logger.info("Gateway ARN: {}", response.gatewayArn());
        logger.info("Gateway Platform: {}",
response.gatewayPlatform());
        logger.info("Gateway Creation Date: {}",
response.creationDate());
    }).join();
    } catch (CompletionException ce) {
        Throwable cause = ce.getCause();
        if (cause instanceof ResourceNotFoundException notFoundException) {
            logger.error("A ResourceNotFoundException occurred: Error
message: {}, Error code {}",
                notFoundException.getMessage(),
notFoundException.awsErrorDetails().errorCode(), notFoundException);
        } else {
            logger.error("An unexpected error occurred: {}",
cause.getMessage(), cause);
        }
        return;
    }
    logger.info(DASHES);

    logger.info(DASHES);
    logger.info("10. Delete the AWS IoT SiteWise Assets");
    logger.info(
        ""
        Before you can delete the Asset Model, you must delete the assets.

        "");
    logger.info("Would you like to delete the IoT SiteWise Assets? (y/n)");
    String delAns = scanner.nextLine().trim();
    if (delAns.equalsIgnoreCase("y")) {
        logger.info("You selected to delete the SiteWise assets.");
        waitForInputToContinue(scanner);
        try {
            sitewiseActions.deletePortalAsync(portalId).join();
            logger.info("Portal {} was deleted successfully.", portalId);

        } catch (CompletionException ce) {
            Throwable cause = ce.getCause();
            if (cause instanceof ResourceNotFoundException notFoundException)
{
                logger.error("A ResourceNotFoundException occurred: Error
message: {}, Error code {}",

```

```

        notFoundException.getMessage(),
notFoundException.awsErrorDetails().errorCode(), notFoundException);
    } else {
        logger.error("An unexpected error occurred: {}",
cause.getMessage());
    }
}

try {
    sitewiseActions.deleteGatewayAsync(gatewayId).join();
    logger.info("Gateway {} was deleted successfully.", gatewayId);
} catch (CompletionException ce) {
    Throwable cause = ce.getCause();
    if (cause instanceof ResourceNotFoundException notFoundException)
{
        logger.error("A ResourceNotFoundException occurred: Error
message: {}, Error code {}",
            notFoundException.getMessage(),
notFoundException.awsErrorDetails().errorCode(), notFoundException);
    } else {
        logger.error("An unexpected error occurred: {}",
cause.getMessage());
    }
}

try {
    sitewiseActions.deleteAssetAsync(assetId).join();
    logger.info("Request to delete asset {} sent successfully",
assetId);
} catch (CompletionException ce) {
    Throwable cause = ce.getCause();
    if (cause instanceof ResourceNotFoundException notFoundException)
{
        logger.error("A ResourceNotFoundException occurred: Error
message: {}, Error code {}",
            notFoundException.getMessage(),
notFoundException.awsErrorDetails().errorCode(), notFoundException);
    } else {
        logger.error("An unexpected error occurred: {}",
cause.getMessage());
    }
}
logger.info("Let's wait 1 minute for the asset to be deleted.");
countdown(60);

```

```

        waitForInputToContinue(scanner);
        logger.info("Delete the AWS IoT SiteWise Asset Model");
        try {
            sitewiseActions.deleteAssetModelAsync(assetModelId).join();
            logger.info("Asset model deleted successfully.");
        } catch (CompletionException ce) {
            Throwable cause = ce.getCause();
            if (cause instanceof ResourceNotFoundException notFoundException)
        {
            logger.error("A ResourceNotFoundException occurred: Error
message: {}, Error code {}",
                        notFoundException.getMessage(),
notFoundException.awsErrorDetails().errorCode(), notFoundException);
            } else {
                logger.error("An unexpected error occurred: {}",
cause.getMessage());
            }
        }
        waitForInputToContinue(scanner);

    } else {
        logger.info("The resources will not be deleted.");
    }
    logger.info(DASHES);

    logger.info(DASHES);
    CloudFormationHelper.destroyCloudFormationStack(ROLES_STACK);
    logger.info("This concludes the AWS IoT SiteWise Scenario");
    logger.info(DASHES);
}

private static void waitForInputToContinue(Scanner scanner) {
    while (true) {
        logger.info("");
        logger.info("Enter 'c' followed by <ENTER> to continue:");
        String input = scanner.nextLine();

        if (input.trim().equalsIgnoreCase("c")) {
            logger.info("Continuing with the program...");
            logger.info("");
            break;
        } else {
            logger.info("Invalid input. Please try again.");
        }
    }
}

```

```

    }
}

public static void countdown(int totalSeconds) throws InterruptedException {
    for (int i = totalSeconds; i >= 0; i--) {
        int displayMinutes = i / 60;
        int displaySeconds = i % 60;
        System.out.printf("\r%02d:%02d", displayMinutes, displaySeconds);
        Thread.sleep(1000); // Wait for 1 second
    }
    System.out.println(); // Move to the next line after countdown
    logger.info("Countdown complete!");
}
}

```

Uma classe wrapper para métodos do AWS IoT SiteWise SDK.

```

public class SitewiseActions {

    private static final Logger logger =
        LoggerFactory.getLogger(SitewiseActions.class);

    private static IoTSiteWiseAsyncClient ioTSiteWiseAsyncClient;

    private static IoTSiteWiseAsyncClient getAsyncClient() {
        if (ioTSiteWiseAsyncClient == null) {
            SdkAsyncHttpClient httpClient = NettyNioAsyncHttpClient.builder()
                .maxConcurrency(100)
                .connectionTimeout(Duration.ofSeconds(60))
                .readTimeout(Duration.ofSeconds(60))
                .writeTimeout(Duration.ofSeconds(60))
                .build();

            ClientOverrideConfiguration overrideConfig =
                ClientOverrideConfiguration.builder()
                    .apiCallTimeout(Duration.ofMinutes(2))
                    .apiCallAttemptTimeout(Duration.ofSeconds(90))
                    .retryStrategy(RetryMode.STANDARD)
                    .build();

            ioTSiteWiseAsyncClient = IoTSiteWiseAsyncClient.builder()
                .httpClient(httpClient)

```



```

        .overrideConfiguration(overrideConfig)
        .build();
    }
    return ioTSiteWiseAsyncClient;
}

/**
 * Creates an asset model.
 *
 * @param name the name of the asset model to create.
 * @return a {@link CompletableFuture} that represents a {@link
CreateAssetModelResponse} result. The calling code
 *         can attach callbacks, then handle the result or exception by
calling {@link CompletableFuture#join()} or
 *         {@link CompletableFuture#get()}.
 *         <p>
 *         If any completion stage in this method throws an exception, the
method logs the exception cause and keeps it
 *         available to the calling code as a {@link CompletionException}. By
calling
 *         {@link CompletionException#getCause()}, the calling code can
access the original exception.
 */
public CompletableFuture<CreateAssetModelResponse>
createAssetModelAsync(String name) {
    PropertyType humidity = PropertyType.builder()
        .measurement(Measurement.builder().build())
        .build();

    PropertyType temperaturePropertyType = PropertyType.builder()
        .measurement(Measurement.builder().build())
        .build();

    AssetModelPropertyDefinition temperatureProperty =
AssetModelPropertyDefinition.builder()
        .name("Temperature")
        .dataType(PropertyDataType.DOUBLE)
        .type(temperaturePropertyType)
        .build();

    AssetModelPropertyDefinition humidityProperty =
AssetModelPropertyDefinition.builder()
        .name("Humidity")

```

```

        .dataType(PropertyDataType.DOUBLE)
        .type(humidity)
        .build();

    CreateAssetModelRequest createAssetModelRequest =
CreateAssetModelRequest.builder()
        .assetModelName(name)
        .assetModelDescription("This is my asset model")
        .assetModelProperties(temperatureProperty, humidityProperty)
        .build();

    return getAsyncClient().createAssetModel(createAssetModelRequest)
        .whenComplete((response, exception) -> {
            if (exception != null) {
                logger.error("Failed to create asset model: {} ",
exception.getCause().getMessage());
            }
        });
    }

/**
 * Creates an asset with the specified name and asset model Id.
 *
 * @param assetName the name of the asset to create.
 * @param assetModelId the Id of the asset model to associate with the asset.
 * @return a {@link CompletableFuture} that represents a {@link
CreateAssetResponse} result. The calling code can
 *      attach callbacks, then handle the result or exception by calling
{@link CompletableFuture#join()} or
 *      {@link CompletableFuture#get()}.
 *      <p>
 *      If any completion stage in this method throws an exception, the
method logs the exception cause and keeps it
 *      available to the calling code as a {@link CompletionException}. By
calling
 *      {@link CompletionException#getCause()}, the calling code can
access the original exception.
 */
    public CompletableFuture<CreateAssetResponse> createAssetAsync(String
assetName, String assetModelId) {
        CreateAssetRequest createAssetRequest = CreateAssetRequest.builder()
            .assetModelId(assetModelId)
            .assetDescription("Created using the AWS SDK for Java")

```

```

        .assetName(assetName)
        .build();

    return getAsyncClient().createAsset(createAssetRequest)
        .whenComplete((response, exception) -> {
            if (exception != null) {
                logger.error("Failed to create asset: {}",
exception.getCause().getMessage());
            }
        });
}

/**
 * Sends data to the SiteWise service.
 *
 * @param assetId the ID of the asset to which the data will be sent.
 * @param tempPropertyId the ID of the temperature property.
 * @param humidityPropId the ID of the humidity property.
 * @return a {@link CompletableFuture} that represents a {@link
BatchPutAssetPropertyValueResponse} result. The
 * calling code can attach callbacks, then handle the result or
exception by calling
 * {@link CompletableFuture#join()} or {@link
CompletableFuture#get()}.
 * <p>
 * If any completion stage in this method throws an exception, the
method logs the exception cause and keeps it
 * available to the calling code as a {@link CompletionException}. By
calling
 * {@link CompletionException#getCause()}, the calling code can
access the original exception.
 */
public CompletableFuture<BatchPutAssetPropertyValueResponse>
sendDataToSiteWiseAsync(String assetId, String tempPropertyId, String
humidityPropId) {
    Map<String, Double> sampleData = generateSampleData();
    long timestamp = Instant.now().toEpochMilli();

    TimeInNanos time = TimeInNanos.builder()
        .timeInSeconds(timestamp / 1000)
        .offsetInNanos((int) ((timestamp % 1000) * 1000000))
        .build();

```

```

        BatchPutAssetPropertyValueRequest request =
BatchPutAssetPropertyValueRequest.builder()
    .entries(Arrays.asList(
        PutAssetPropertyValueEntry.builder()
            .entryId("entry-3")
            .assetId(assetId)
            .propertyId(tempPropertyId)
            .propertyValues(Arrays.asList(
                AssetPropertyValue.builder()
                    .value(Variant.builder()
                        .doubleValue(sampleData.get("Temperature"))
                        .build())
                    .timestamp(time)
                    .build()
            ))
            .build(),
        PutAssetPropertyValueEntry.builder()
            .entryId("entry-4")
            .assetId(assetId)
            .propertyId(humidityPropId)
            .propertyValues(Arrays.asList(
                AssetPropertyValue.builder()
                    .value(Variant.builder()
                        .doubleValue(sampleData.get("Humidity"))
                        .build())
                    .timestamp(time)
                    .build()
            ))
            .build()
    ))
    .build();

return getAsyncClient().batchPutAssetPropertyValue(request)
    .whenComplete((response, exception) -> {
        if (exception != null) {
            logger.error("An exception occurred: {}",
exception.getCause().getMessage());
        }
    });
}

/**
 * Fetches the value of an asset property.
 *

```

```

    * @param propId the ID of the asset property to fetch.
    * @param assetId the ID of the asset to fetch the property value for.
    * @return a {@link CompletableFuture} that represents a {@link Double}
result. The calling code can attach
    *     callbacks, then handle the result or exception by calling {@link
CompletableFuture#join()} or
    *     {@link CompletableFuture#get()}.
    *
    * <p>
    *     If any completion stage in this method throws an exception, the
method logs the exception cause and keeps
    *     it available to the calling code as a {@link CompletionException}.
By calling
    *     {@link CompletionException#getCause()}, the calling code can
access the original exception.
    */
    public CompletableFuture<Double> getAssetPropValueAsync(String propId, String
assetId) {
        GetAssetPropertyValueRequest assetPropertyValueRequest =
GetAssetPropertyValueRequest.builder()
            .propertyId(propId)
            .assetId(assetId)
            .build();

        return getAsyncClient().getAssetPropertyValue(assetPropertyValueRequest)
            .handle((response, exception) -> {
                if (exception != null) {
                    logger.error("Error occurred while fetching property
value: {}.", exception.getCause().getMessage());
                    throw (CompletionException) exception;
                }
                return response.propertyValue().value().doubleValue();
            });
    }

    /**
    * Retrieves the property IDs associated with a specific asset model.
    *
    * @param assetModelId the ID of the asset model that defines the properties.
    * @return a {@link CompletableFuture} that represents a {@link Map} result
that associates the property name to the
    *     propert ID. The calling code can attach callbacks, then handle the
result or exception by calling
    *     {@link CompletableFuture#join()} or {@link
CompletableFuture#get()}.

```

```

    *      <p>
    *      If any completion stage in this method throws an exception, the
method logs the exception cause and keeps
    *      it available to the calling code as a {@link CompletionException}.
By calling
    *      {@link CompletionException#getCause()}, the calling code can
access the original exception.
    */
    public CompletableFuture<Map<String, String>> getPropertyIds(String
assetModelId) {
        ListAssetModelPropertiesRequest modelPropertiesRequest =
ListAssetModelPropertiesRequest.builder().assetModelId(assetModelId).build();
        return getAsyncClient().listAssetModelProperties(modelPropertiesRequest)
            .handle((response, throwable) -> {
                if (response != null) {
                    return response.assetModelPropertySummaries().stream()
                        .collect(Collectors
                            .toMap(AssetModelPropertySummary::name,
AssetModelPropertySummary::id));
                } else {
                    logger.error("Error occurred while fetching property IDs:
{}.\"", throwable.getCause().getMessage());
                    throw (CompletionException) throwable;
                }
            });
    }

    /**
    * Deletes an asset.
    *
    * @param assetId the ID of the asset to be deleted.
    * @return a {@link CompletableFuture} that represents a {@link
DeleteAssetResponse} result. The calling code can
    *      attach callbacks, then handle the result or exception by calling
{@link CompletableFuture#join()} or
    *      {@link CompletableFuture#get()}.
    *      <p>
    *      If any completion stage in this method throws an exception, the
method logs the exception cause and keeps
    *      it available to the calling code as a {@link CompletionException}.
By calling
    *      {@link CompletionException#getCause()}, the calling code can
access the original exception.
    */

```

```

    public CompletableFuture<DeleteAssetResponse> deleteAssetAsync(String
assetId) {
        DeleteAssetRequest deleteAssetRequest = DeleteAssetRequest.builder()
            .assetId(assetId)
            .build();

        return getAsyncClient().deleteAsset(deleteAssetRequest)
            .whenComplete((response, exception) -> {
                if (exception != null) {
                    logger.error("An error occurred deleting asset with id: {}",
assetId);
                }
            });
    }

    /**
     * Deletes an Asset Model with the specified ID.
     *
     * @param assetModelId the ID of the Asset Model to delete.
     * @return a {@link CompletableFuture} that represents a {@link
DeleteAssetModelResponse} result. The calling code
     *         can attach callbacks, then handle the result or exception by
calling {@link CompletableFuture#join()} or
     *         {@link CompletableFuture#get()}.
     *
     * <p>
     *         If any completion stage in this method throws an exception, the
method logs the exception cause and keeps
     *         it available to the calling code as a {@link CompletionException}.
By calling
     *         {@link CompletionException#getCause()}, the calling code can
access the original exception.
     */
    public CompletableFuture<DeleteAssetModelResponse>
deleteAssetModelAsync(String assetModelId) {
        DeleteAssetModelRequest deleteAssetModelRequest =
DeleteAssetModelRequest.builder()
            .assetModelId(assetModelId)
            .build();

        return getAsyncClient().deleteAssetModel(deleteAssetModelRequest)
            .whenComplete((response, exception) -> {
                if (exception != null) {
                    logger.error("Failed to delete asset model with ID:{}",
exception.getMessage());

```

```

        }
    });
}

/**
 * Creates a new IoT SiteWise portal.
 *
 * @param portalName the name of the portal to create.
 * @param iamRole the IAM role ARN to use for the portal.
 * @param contactEmail the email address of the portal contact.
 * @return a {@link CompletableFuture} that represents a {@link String}
result of the portal ID. The calling code
 * can attach callbacks, then handle the result or exception by
calling {@link CompletableFuture#join()} or
 * {@link CompletableFuture#get()}.
 *
 * <p>
 * If any completion stage in this method throws an exception, the
method logs the exception cause and keeps
 * it available to the calling code as a {@link CompletionException}.
By calling
 * {@link CompletionException#getCause()}, the calling code can
access the original exception.
 */
public CompletableFuture<String> createPortalAsync(String portalName, String
iamRole, String contactEmail) {
    CreatePortalRequest createPortalRequest = CreatePortalRequest.builder()
        .portalName(portalName)
        .portalDescription("This is my custom IoT SiteWise portal.")
        .portalContactEmail(contactEmail)
        .roleArn(iamRole)
        .build();

    return getAsyncClient().createPortal(createPortalRequest)
        .handle((response, exception) -> {
            if (exception != null) {
                logger.error("Failed to create portal: {} ",
exception.getCause().getMessage());
                throw (CompletionException) exception;
            }
            return response.portalId();
        });
}

/**

```



```

    * Deletes a portal.
    *
    * @param portalId the ID of the portal to be deleted.
    * @return a {@link CompletableFuture} that represents a {@link
DeletePortalResponse}. The calling code can attach
    *     callbacks, then handle the result or exception by calling {@link
CompletableFuture#join()} or
    *     {@link CompletableFuture#get()}.
    *     <p>
    *     If any completion stage in this method throws an exception, the
method logs the exception cause and keeps
    *     it available to the calling code as a {@link CompletionException}.
By calling
    *     {@link CompletionException#getCause()}, the calling code can
access the original exception.
    */
    public CompletableFuture<DeletePortalResponse> deletePortalAsync(String
portalId) {
        DeletePortalRequest deletePortalRequest = DeletePortalRequest.builder()
            .portalId(portalId)
            .build();

        return getAsyncClient().deletePortal(deletePortalRequest)
            .whenComplete((response, exception) -> {
                if (exception != null) {
                    logger.error("Failed to delete portal with ID: {}. Error:
{}", portalId, exception.getCause().getMessage());
                }
            });
    }

    /**
    * Retrieves the asset model ID for the given asset model name.
    *
    * @param assetModelName the name of the asset model for the ID.
    * @return a {@link CompletableFuture} that represents a {@link String}
result of the asset model ID or null if the
    *     asset model cannot be found. The calling code can attach
callbacks, then handle the result or exception
    *     by calling {@link CompletableFuture#join()} or {@link
CompletableFuture#get()}.
    *     <p>
    *     If any completion stage in this method throws an exception, the
method logs the exception cause and keeps

```

```

        *           it available to the calling code as a {@link CompletionException}.
By calling
        *           {@link CompletionException#getCause()}, the calling code can
access the original exception.
        */
    public CompletableFuture<String> getAssetModelIdAsync(String assetModelName)
    {
        ListAssetModelsRequest listAssetModelsRequest =
ListAssetModelsRequest.builder().build();
        return getAsyncClient().listAssetModels(listAssetModelsRequest)
            .handle((listAssetModelsResponse, exception) -> {
                if (exception != null) {
                    logger.error("Failed to retrieve Asset Model ID: {}",
exception.getCause().getMessage());
                    throw (CompletionException) exception;
                }
                for (AssetModelSummary assetModelSummary :
listAssetModelsResponse.assetModelSummaries()) {
                    if (assetModelSummary.name().equals(assetModelName)) {
                        return assetModelSummary.id();
                    }
                }
                return null;
            });
    }

    /**
     * Retrieves a portal's description.
     *
     * @param portalId the ID of the portal to describe.
     * @return a {@link CompletableFuture} that represents a {@link String}
result of the portal's start URL
     * (see: {@link DescribePortalResponse#portalStartUrl()}). The
calling code can attach callbacks, then handle the
     * result or exception by calling {@link CompletableFuture#join()} or
{@link CompletableFuture#get()}.
     *
     * <p>
     * If any completion stage in this method throws an exception, the
method logs the exception cause and keeps
     * it available to the calling code as a {@link CompletionException}.
By calling
     * {@link CompletionException#getCause()}, the calling code can
access the original exception.
     */

```

```

public CompletableFuture<String> describePortalAsync(String portalId) {
    DescribePortalRequest request = DescribePortalRequest.builder()
        .portalId(portalId)
        .build();

    return getAsyncClient().describePortal(request)
        .handle((response, exception) -> {
            if (exception != null) {
                logger.error("An exception occurred retrieving the portal
description: {}", exception.getCause().getMessage());
                throw (CompletionException) exception;
            }
            return response.portalStartUrl();
        });
}

/**
 * Creates a new IoT SiteWise gateway.
 *
 * @param gatewayName The name of the gateway to create.
 * @param myThing      The name of the core device thing to associate with the
gateway.
 * @return a {@link CompletableFuture} that represents a {@link String}
result of the gateways ID. The calling code
 *         can attach callbacks, then handle the result or exception by
calling {@link CompletableFuture#join()} or
 *         {@link CompletableFuture#get()}.
 *         <p>
 *         If any completion stage in this method throws an exception, the
method logs the exception cause and keeps
 *         it available to the calling code as a {@link CompletionException}.
By calling
 *         {@link CompletionException#getCause()}, the calling code can
access the original exception.
 */
public CompletableFuture<String> createGatewayAsync(String gatewayName,
String myThing) {
    GreengrassV2 gg = GreengrassV2.builder()
        .coreDeviceThingName(myThing)
        .build();

    GatewayPlatform platform = GatewayPlatform.builder()
        .greengrassV2(gg)

```

```

        .build();

        Map<String, String> tag = new HashMap<>();
        tag.put("Environment", "Production");

        CreateGatewayRequest createGatewayRequest =
        CreateGatewayRequest.builder()
            .gatewayName(gatewayName)
            .gatewayPlatform(platform)
            .tags(tag)
            .build();

        return getAsyncClient().createGateway(createGatewayRequest)
            .handle((response, exception) -> {
                if (exception != null) {
                    logger.error("Error creating the gateway.");
                    throw (CompletionException) exception;
                }
                logger.info("The ARN of the gateway is {}" ,
response.gatewayArn());
                return response.gatewayId();
            });
    }

    /**
     * Deletes the specified gateway.
     *
     * @param gatewayId the ID of the gateway to delete.
     * @return a {@link CompletableFuture} that represents a {@link
DeleteGatewayResponse} result.. The calling code
     *         can attach callbacks, then handle the result or exception by
calling {@link CompletableFuture#join()} or
     *         {@link CompletableFuture#get()}.
     *
     * <p>
     *         If any completion stage in this method throws an exception, the
method logs the exception cause and keeps
     *         it available to the calling code as a {@link CompletionException}.
By calling
     *         {@link CompletionException#getCause()}, the calling code can
access the original exception.
     */
    public CompletableFuture<DeleteGatewayResponse> deleteGatewayAsync(String
gatewayId) {

```

```

        DeleteGatewayRequest deleteGatewayRequest =
DeleteGatewayRequest.builder()
        .gatewayId(gatewayId)
        .build();

        return getAsyncClient().deleteGateway(deleteGatewayRequest)
            .whenComplete((response, exception) -> {
                if (exception != null) {
                    logger.error("Failed to delete gateway: {}",
exception.getCause().getMessage());
                }
            });
    }

    /**
     * Describes the specified gateway.
     *
     * @param gatewayId the ID of the gateway to describe.
     * @return a {@link CompletableFuture} that represents a {@link
DescribeGatewayResponse} result. The calling code
     *         can attach callbacks, then handle the result or exception by
calling {@link CompletableFuture#join()} or
     *         {@link CompletableFuture#get()}.
     *
     * <p>
     *         If any completion stage in this method throws an exception, the
method logs the exception cause and keeps
     *         it available to the calling code as a {@link CompletionException}.
By calling
     *         {@link CompletionException#getCause()}, the calling code can
access the original exception.
     */
    public CompletableFuture<DescribeGatewayResponse> describeGatewayAsync(String
gatewayId) {
        DescribeGatewayRequest request = DescribeGatewayRequest.builder()
            .gatewayId(gatewayId)
            .build();

        return getAsyncClient().describeGateway(request)
            .whenComplete((response, exception) -> {
                if (exception != null) {
                    logger.error("An error occurred during the describeGateway
method: {}", exception.getCause().getMessage());
                }
            });
    }

```

```
}

private static Map<String, Double> generateSampleData() {
    Map<String, Double> data = new HashMap<>();
    data.put("Temperature", 23.5);
    data.put("Humidity", 65.0);
    return data;
}
}
```

JavaScript

SDK para JavaScript (v3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
import {
    Scenario,
    ScenarioAction,
    ScenarioInput,
    ScenarioOutput,
    //} from "@aws-doc-sdk-examples/lib/scenario/index.js";
} from "../../libs/scenario/index.js";
import {
    IoTSiteWiseClient,
    CreateAssetModelCommand,
    CreateAssetCommand,
    ListAssetModelPropertiesCommand,
    BatchPutAssetPropertyValueCommand,
    GetAssetPropertyValueCommand,
    CreatePortalCommand,
    DescribePortalCommand,
    CreateGatewayCommand,
    DescribeGatewayCommand,
    DeletePortalCommand,
    DeleteGatewayCommand,
```

```

    DeleteAssetCommand,
    DeleteAssetModelCommand,
    DescribeAssetModelCommand,
} from "@aws-sdk/client-iotsitewise";
import {
    CloudFormationClient,
    CreateStackCommand,
    DeleteStackCommand,
    DescribeStacksCommand,
    waitUntilStackExists,
    waitUntilStackCreateComplete,
    waitUntilStackDeleteComplete,
} from "@aws-sdk/client-cloudformation";
import { wait } from "@aws-doc-sdk-examples/lib/utils/util-timers.js";
import { parseArgs } from "node:util";
import { readFileSync } from "node:fs";
import { fileURLToPath } from "node:url";
import { dirname } from "node:path";

const __filename = fileURLToPath(import.meta.url);
const __dirname = dirname(__filename);
const stackName = "SiteWiseBasicsStack";

/**
 * @typedef {{
 *   iotSiteWiseClient: import('@aws-sdk/client-iotsitewise').IotSiteWiseClient,
 *   cloudFormationClient: import('@aws-sdk/client-
cloudformation').CloudFormationClient,
 *   stackName,
 *   stack,
 *   askToDeleteResources: true,
 *   asset: {assetName: "MyAsset1"},
 *   assetModel: {assetModelName: "MyAssetModel1"},
 *   portal: {portalName: "MyPortal1"},
 *   gateway: {gatewayName: "MyGateway1"},
 *   propertyIds: [],
 *   contactEmail: "user@mydomain.com",
 *   thing: "MyThing1",
 *   sampleData: { temperature: 23.5, humidity: 65.0}
 * }} State
 */

/**
 * Used repeatedly to have the user press enter.

```

```

* @type {ScenarioInput}
*/
const pressEnter = new ScenarioInput("continue", "Press Enter to continue", {
  type: "confirm",
});

const greet = new ScenarioOutput(
  "greet",
  `AWS IoT SiteWise is a fully managed industrial software-as-a-service (SaaS)
  that makes it easy to collect, store, organize, and monitor data from industrial
  equipment and processes. It is designed to help industrial and manufacturing
  organizations collect data from their equipment and processes, and use that data
  to make informed decisions about their operations.
  One of the key features of AWS IoT SiteWise is its ability to connect to a
  wide range of industrial equipment and systems, including programmable logic
  controllers (PLCs), sensors, and other industrial devices. It can collect data
  from these devices and organize it into a unified data model, making it easier
  to analyze and gain insights from the data. AWS IoT SiteWise also provides tools
  for visualizing the data, setting up alarms and alerts, and generating reports.
  Another key feature of AWS IoT SiteWise is its ability to scale to handle large
  volumes of data. It can collect and store data from thousands of devices and
  process millions of data points per second, making it suitable for large-scale
  industrial operations. Additionally, AWS IoT SiteWise is designed to be secure
  and compliant, with features like role-based access controls, data encryption,
  and integration with other AWS services for additional security and compliance
  features.

  Let's get started...`,
  { header: true },
);

const displayBuildCloudFormationStack = new ScenarioOutput(
  "displayBuildCloudFormationStack",
  "This scenario uses AWS CloudFormation to create an IAM role that is required
  for this scenario. The stack will now be deployed.",
);

const sdkBuildCloudFormationStack = new ScenarioAction(
  "sdkBuildCloudFormationStack",
  async (** @type {State} */ state) => {
    try {
      const data = readFileSync(
        `${__dirname}/../../../../resources/cfn/iotsitewise_basics/SitewiseRoles-
        template.yml`,

```



```

    "utf8",
  );
  await state.cloudFormationClient.send(
    new CreateStackCommand({
      StackName: stackName,
      TemplateBody: data,
      Capabilities: ["CAPABILITY_IAM"],
    }),
  );
  await waitUntilStackExists(
    { client: state.cloudFormationClient },
    { StackName: stackName },
  );
  await waitUntilStackCreateComplete(
    { client: state.cloudFormationClient },
    { StackName: stackName },
  );
  const stack = await state.cloudFormationClient.send(
    new DescribeStacksCommand({
      StackName: stackName,
    }),
  );
  state.stack = stack.Stacks[0].Outputs[0];
  console.log(`The ARN of the IAM role is ${state.stack.OutputValue}`);
} catch (caught) {
  console.error(caught.message);
  throw caught;
}
},
);

```

```

const displayCreateAWSSiteWiseAssetModel = new ScenarioOutput(
  "displayCreateAWSSiteWiseAssetModel",
  `1. Create an AWS SiteWise Asset Model

```

An AWS IoT SiteWise Asset Model is a way to represent the physical assets, such as equipment, processes, and systems, that exist in an industrial environment. This model provides a structured and hierarchical representation of these assets, allowing users to define the relationships and properties of each asset.

This scenario creates two asset model properties: temperature and humidity.`,

```

);

```

```

const sdkCreateAWSSiteWiseAssetModel = new ScenarioAction(
  "sdkCreateAWSSiteWiseAssetModel",

```

```

async (/** @type {State} */ state) => {
  let assetModelResponse;
  try {
    assetModelResponse = await state.iotSiteWiseClient.send(
      new CreateAssetModelCommand({
        assetModelName: state.assetModel.assetModelName,
        assetModelProperties: [
          {
            name: "Temperature",
            dataType: "DOUBLE",
            type: {
              measurement: {},
            },
          },
          {
            name: "Humidity",
            dataType: "DOUBLE",
            type: {
              measurement: {},
            },
          },
        ],
      })),
    );
    state.assetModel.assetModelId = assetModelResponse.assetModelId;
    console.log(
      `Asset Model successfully created. Asset Model ID:
    ${state.assetModel.assetModelId}`,
    );
  } catch (caught) {
    if (caught.name === "ResourceAlreadyExistsException") {
      console.log(
        `The Asset Model ${state.assetModel.assetModelName} already exists.`,
      );
      throw caught;
    }
    console.error(`${caught.message}`);
    throw caught;
  }
},
);

const displayCreateAWSIoTSiteWiseAssetModel = new ScenarioOutput(
  "displayCreateAWSIoTSiteWiseAssetModel",

```

`2. Create an AWS IoT SiteWise Asset

The IoT SiteWise model that we just created defines the structure and metadata for your physical assets. Now we create an asset from the asset model.

Let's wait 30 seconds for the asset to be ready.`,
);

```
const waitThirtySeconds = new ScenarioAction("waitThirtySeconds", async () => {
  await wait(30); // wait 30 seconds
  console.log("Time's up! Let's check the asset's status.");
});
```

```
const sdkCreateAWSIoTSiteWiseAssetModel = new ScenarioAction(
  "sdkCreateAWSIoTSiteWiseAssetModel",
  async (/** @type {State} */ state) => {
    try {
      const assetResponse = await state.iotSiteWiseClient.send(
        new CreateAssetCommand({
          assetModelId: state.assetModel.assetModelId,
          assetName: state.asset.assetName,
        })),
      );
      state.asset.assetId = assetResponse.assetId;
      console.log(`Asset created with ID: ${state.asset.assetId}`);
    } catch (caught) {
      if (caught.name === "ResourceNotFoundException") {
        console.log(
          `The Asset ${state.assetModel.assetModelName} was not found.`
        );
        throw caught;
      }
      console.error(`${caught.message}`);
      throw caught;
    }
  },
);
```

```
const displayRetrievePropertyId = new ScenarioOutput(
  "displayRetrievePropertyId",
  `3. Retrieve the property ID values
```

To send data to an asset, we need to get the property ID values. In this scenario, we access the temperature and humidity property ID values.`,
);

```
const sdkRetrievePropertyId = new ScenarioAction(
  "sdkRetrievePropertyId",
  async (state) => {
    try {
      const retrieveResponse = await state.iotSiteWiseClient.send(
        new ListAssetModelPropertiesCommand({
          assetModelId: state.assetModel.assetModelId,
        }),
      );
      for (const retrieveResponseKey in
retrieveResponse.assetModelPropertySummaries) {
        if (
          retrieveResponse.assetModelPropertySummaries[retrieveResponseKey]
            .name === "Humidity"
        ) {
          state.propertyIds.Humidity =
            retrieveResponse.assetModelPropertySummaries[
              retrieveResponseKey
            ].id;
        }
        if (
          retrieveResponse.assetModelPropertySummaries[retrieveResponseKey]
            .name === "Temperature"
        ) {
          state.propertyIds.Temperature =
            retrieveResponse.assetModelPropertySummaries[
              retrieveResponseKey
            ].id;
        }
      }
      console.log(`The Humidity propertyId is ${state.propertyIds.Humidity}`);
      console.log(
        `The Temperature propertyId is ${state.propertyIds.Temperature}`,
      );
    } catch (caught) {
      if (caught.name === "IoTSiteWiseException") {
        console.log(
          `There was a problem retrieving the properties: ${caught.message}`,
        );
        throw caught;
      }
      console.error(`${caught.message}`);
      throw caught;
    }
  }
);
```

```

    }
  },
);

const displaySendDataToIoTSiteWiseAsset = new ScenarioOutput(
  "displaySendDataToIoTSiteWiseAsset",
  `4. Send data to an AWS IoT SiteWise Asset

```

By sending data to an IoT SiteWise Asset, you can aggregate data from multiple sources, normalize the data into a standard format, and store it in a centralized location. This makes it easier to analyze and gain insights from the data.

In this example, we generate sample temperature and humidity data and send it to the AWS IoT SiteWise asset.`,

```

);

```

```

const sdkSendDataToIoTSiteWiseAsset = new ScenarioAction(
  "sdkSendDataToIoTSiteWiseAsset",
  async (state) => {
    try {
      const sendResponse = await state.iotSiteWiseClient.send(
        new BatchPutAssetPropertyValueCommand({
          entries: [
            {
              entryId: "entry-3",
              assetId: state.asset.assetId,
              propertyId: state.propertyIds.Humidity,
              propertyValues: [
                {
                  value: {
                    doubleValue: state.sampleData.humidity,
                  },
                  timestamp: {
                    timeInSeconds: Math.floor(Date.now() / 1000),
                  },
                },
              ],
            },
            {
              entryId: "entry-4",
              assetId: state.asset.assetId,
              propertyId: state.propertyIds.Temperature,
              propertyValues: [

```

```

        {
            value: {
                doubleValue: state.sampleData.temperature,
            },
            timestamp: {
                timeInSeconds: Math.floor(Date.now() / 1000),
            },
        },
    ],
},
],
)),
);
console.log("The data was sent successfully.");
} catch (caught) {
    if (caught.name === "ResourceNotFoundException") {
        console.log(`The Asset ${state.asset.assetName} was not found.`);
        throw caught;
    }
    console.error(`${caught.message}`);
    throw caught;
}
},
);

const displayRetrieveValueOfIoTSiteWiseAsset = new ScenarioOutput(
    "displayRetrieveValueOfIoTSiteWiseAsset",
    `5. Retrieve the value of the IoT SiteWise Asset property

IoT SiteWise is an AWS service that allows you to collect, process, and analyze
industrial data from connected equipment and sensors. One of the key benefits of
reading an IoT SiteWise property is the ability to gain valuable insights from
your industrial data.`,
);

const sdkRetrieveValueOfIoTSiteWiseAsset = new ScenarioAction(
    "sdkRetrieveValueOfIoTSiteWiseAsset",
    async (/** @type {State} */ state) => {
        try {
            const temperatureResponse = await state.iotSiteWiseClient.send(
                new GetAssetPropertyValueCommand({
                    assetId: state.asset.assetId,
                    propertyId: state.propertyIds.Temperature,
                }),
            );

```

```

    );
    const humidityResponse = await state.iotSiteWiseClient.send(
      new GetAssetPropertyValueCommand({
        assetId: state.asset.assetId,
        propertyId: state.propertyIds.Humidity,
      }),
    );
    console.log(
      `The property value for Temperature is
    ${temperatureResponse.propertyValue.value.doubleValue}`,
    );
    console.log(
      `The property value for Humidity is
    ${humidityResponse.propertyValue.value.doubleValue}`,
    );
  } catch (caught) {
    if (caught.name === "ResourceNotFoundException") {
      console.log(`The Asset ${state.asset.assetName} was not found.`);
      throw caught;
    }
    console.error(`${caught.message}`);
    throw caught;
  }
},
);

const displayCreateIoTSiteWisePortal = new ScenarioOutput(
  "displayCreateIoTSiteWisePortal",
  `6. Create an IoT SiteWise Portal

An IoT SiteWise Portal allows you to aggregate data from multiple industrial
sources, such as sensors, equipment, and control systems, into a centralized
platform.`
);

const sdkCreateIoTSiteWisePortal = new ScenarioAction(
  "sdkCreateIoTSiteWisePortal",
  async (** @type {State} */ state) => {
    try {
      const createPortalResponse = await state.iotSiteWiseClient.send(
        new CreatePortalCommand({
          portalName: state.portal.portalName,
          portalContactEmail: state.contactEmail,
          roleArn: state.stack.OutputValue,

```

```

    })),
  );
  state.portal = { ...state.portal, ...createPortalResponse };
  await wait(5); // Allow the portal to properly propagate.
  console.log(
    `Portal created successfully. Portal ID
    ${createPortalResponse.portalId}`,
  );
} catch (caught) {
  if (caught.name === "IoTSiteWiseException") {
    console.log(
      `There was a problem creating the Portal: ${caught.message}.`,
    );
    throw caught;
  }
  console.error(`${caught.message}`);
  throw caught;
}
},
);

```

```

const displayDescribePortal = new ScenarioOutput(
  "displayDescribePortal",
  `7. Describe the Portal

```

In this step, we get a description of the portal and display the portal URL.`,

```

);

```

```

const sdkDescribePortal = new ScenarioAction(
  "sdkDescribePortal",
  async (/** @type {State} */ state) => {
    try {
      const describePortalResponse = await state.iotSiteWiseClient.send(
        new DescribePortalCommand({
          portalId: state.portal.portalId,
        }),
      );
      console.log(`Portal URL: ${describePortalResponse.portalStartUrl}`);
    } catch (caught) {
      if (caught.name === "ResourceNotFoundException") {
        console.log(`The Portal ${state.portal.portalName} was not found.`);
        throw caught;
      }
      console.error(`${caught.message}`);
    }
  }
);

```



```

        throw caught;
    }
},
);

```

```

const displayCreateIoTSiteWiseGateway = new ScenarioOutput(
  "displayCreateIoTSiteWiseGateway",
  `8. Create an IoT SiteWise Gateway

```

IoT SiteWise Gateway serves as the bridge between industrial equipment, sensors, and the cloud-based IoT SiteWise service. It is responsible for securely collecting, processing, and transmitting data from various industrial assets to the IoT SiteWise platform, enabling real-time monitoring, analysis, and optimization of industrial operations.`,

```

);

```

```

const sdkCreateIoTSiteWiseGateway = new ScenarioAction(
  "sdkCreateIoTSiteWiseGateway",
  async (/** @type {State} */ state) => {
    try {
      const createGatewayResponse = await state.iotSiteWiseClient.send(
        new CreateGatewayCommand({
          gatewayName: state.gateway.gatewayName,
          gatewayPlatform: {
            greengrassV2: {
              coreDeviceThingName: state.thing,
            },
          },
        }),
      );
      console.log(
        `Gateway creation completed successfully. ID is
        ${createGatewayResponse.gatewayId}`,
      );
      state.gateway.gatewayId = createGatewayResponse.gatewayId;
    } catch (caught) {
      if (caught.name === "IoTSiteWiseException") {
        console.log(
          `There was a problem creating the gateway: ${caught.message}.`,
        );
        throw caught;
      }
      console.error(`${caught.message}`);
      throw caught;
    }
  }
);

```

```

    }
  },
);

const displayDescribeIoTSiteWiseGateway = new ScenarioOutput(
  "displayDescribeIoTSiteWiseGateway",
  "9. Describe the IoT SiteWise Gateway",
);

const sdkDescribeIoTSiteWiseGateway = new ScenarioAction(
  "sdkDescribeIoTSiteWiseGateway",
  async (** @type {State} */ state) => {
    try {
      const describeGatewayResponse = await state.iotSiteWiseClient.send(
        new DescribeGatewayCommand({
          gatewayId: state.gateway.gatewayId,
        }),
      );
      console.log("Gateway creation completed successfully.");
      console.log(`Gateway Name: ${describeGatewayResponse.gatewayName}`);
      console.log(`Gateway ARN: ${describeGatewayResponse.gatewayArn}`);
      console.log(
        `Gateway Platform:
${Object.keys(describeGatewayResponse.gatewayPlatform)}`,
      );
      console.log(
        `Gateway Creation Date: ${describeGatewayResponse.creationDate}`,
      );
    } catch (caught) {
      if (caught.name === "ResourceNotFoundException") {
        console.log(`The Gateway ${state.gateway.gatewayId} was not found.`);
        throw caught;
      }
      console.error(`${caught.message}`);
      throw caught;
    }
  },
);

const askToDeleteResources = new ScenarioInput(
  "askToDeleteResources",
  `10. Delete the AWS IoT SiteWise Assets

Before you can delete the Asset Model, you must delete the assets.`

```

```
    { type: "confirm" },
  );

const displayConfirmDeleteResources = new ScenarioAction(
  "displayConfirmDeleteResources",
  async (** @type {State} */ state) => {
    if (state.askToDeleteResources) {
      return "You selected to delete the SiteWise assets.";
    }
    return "The resources will not be deleted. Please delete them manually to avoid charges.";
  },
);

const sdkDeleteResources = new ScenarioAction(
  "sdkDeleteResources",
  async (** @type {State} */ state) => {
    await wait(10); // Give the portal status time to catch up.
    try {
      await state.iotSiteWiseClient.send(
        new DeletePortalCommand({
          portalId: state.portal.portalId,
        }),
      );
      console.log(
        `Portal ${state.portal.portalName} was deleted successfully.`,
      );
    } catch (caught) {
      if (caught.name === "ResourceNotFoundException") {
        console.log(`The Portal ${state.portal.portalName} was not found.`);
      } else {
        console.log(`When trying to delete the portal: ${caught.message}`);
      }
    }

    try {
      await state.iotSiteWiseClient.send(
        new DeleteGatewayCommand({
          gatewayId: state.gateway.gatewayId,
        }),
      );
      console.log(
        `Gateway ${state.gateway.gatewayName} was deleted successfully.`,
      );
    }
  }
);
```

```
    } catch (caught) {
      if (caught.name === "ResourceNotFoundException") {
        console.log(`The Gateway ${state.gateway.gatewayId} was not found.`);
      } else {
        console.log(`When trying to delete the gateway: ${caught.message}`);
      }
    }
  }

  try {
    await state.iotSiteWiseClient.send(
      new DeleteAssetCommand({
        assetId: state.asset.assetId,
      }),
    );
    await wait(5); // Allow the delete to finish.
    console.log(`Asset ${state.asset.assetName} was deleted successfully.`);
  } catch (caught) {
    if (caught.name === "ResourceNotFoundException") {
      console.log(`The Asset ${state.asset.assetName} was not found.`);
    } else {
      console.log(`When deleting the asset: ${caught.message}`);
    }
  }
}

await wait(30); // Allow asset deletion to finish.
try {
  await state.iotSiteWiseClient.send(
    new DeleteAssetModelCommand({
      assetModelId: state.assetModel.assetModelId,
    }),
  );
  console.log(
    `Asset Model ${state.assetModel.assetModelName} was deleted
successfully.`,
  );
} catch (caught) {
  if (caught.name === "ResourceNotFoundException") {
    console.log(
      `The Asset Model ${state.assetModel.assetModelName} was not found.`,
    );
  } else {
    console.log(`When deleting the asset model: ${caught.message}`);
  }
}
```

```
try {
  await state.cloudFormationClient.send(
    new DeleteStackCommand({
      StackName: stackName,
    }),
  );
  await waitUntilStackDeleteComplete(
    { client: state.cloudFormationClient },
    { StackName: stackName },
  );
  console.log("The stack was deleted successfully.");
} catch (caught) {
  console.log(
    `${caught.message}. The stack was NOT deleted. Please clean up the
resources manually.`
  );
}
},
{ skipWhen: (/** @type {} */ state) => !state.askToDeleteResources },
);

const goodbye = new ScenarioOutput(
  "goodbye",
  "This concludes the IoT SiteWise Basics scenario for the AWS Javascript SDK v3.
Thank you!",
);

const myScenario = new Scenario(
  "IoTSiteWise Basics",
  [
    greet,
    pressEnter,
    displayBuildCloudFormationStack,
    sdkBuildCloudFormationStack,
    pressEnter,
    displayCreateAWSSiteWiseAssetModel,
    sdkCreateAWSSiteWiseAssetModel,
    displayCreateAWSIoTSiteWiseAssetModel,
    pressEnter,
    waitThirtySeconds,
    sdkCreateAWSIoTSiteWiseAssetModel,
    pressEnter,
    displayRetrievePropertyId,
```

```

    sdkRetrievePropertyId,
    pressEnter,
    displaySendDataToIoTSiteWiseAsset,
    sdkSendDataToIoTSiteWiseAsset,
    pressEnter,
    displayRetrieveValueOfIoTSiteWiseAsset,
    sdkRetrieveValueOfIoTSiteWiseAsset,
    pressEnter,
    displayCreateIoTSiteWisePortal,
    sdkCreateIoTSiteWisePortal,
    pressEnter,
    displayDescribePortal,
    sdkDescribePortal,
    pressEnter,
    displayCreateIoTSiteWiseGateway,
    sdkCreateIoTSiteWiseGateway,
    pressEnter,
    displayDescribeIoTSiteWiseGateway,
    sdkDescribeIoTSiteWiseGateway,
    pressEnter,
    askToDeleteResources,
    displayConfirmDeleteResources,
    sdkDeleteResources,
    goodbye,
  ],
  {
    iotSiteWiseClient: new IoTSiteWiseClient({}),
    cloudFormationClient: new CloudFormationClient({}),
    asset: { assetName: "MyAsset1" },
    assetModel: { assetModelName: "MyAssetModel1" },
    portal: { portalName: "MyPortal1" },
    gateway: { gatewayName: "MyGateway1" },
    propertyIds: [],
    contactEmail: "user@mydomain.com",
    thing: "MyThing1",
    sampleData: { temperature: 23.5, humidity: 65.0 },
  },
);

/** @type {{ stepHandlerOptions: StepHandlerOptions }} */
export const main = async (stepHandlerOptions) => {
  await myScenario.run(stepHandlerOptions);
};

```

```
// Invoke main function if this file was run directly.
if (process.argv[1] === fileURLToPath(import.meta.url)) {
  const { values } = parseArgs({
    options: {
      yes: {
        type: "boolean",
        short: "y",
      },
    },
  });
  main({ confirmAll: values.yes });
}
```

Python

SDK para Python (Boto3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

Execute um cenário interativo em um prompt de comando.

```
class IoTSiteWiseGettingStarted:
    """
    A scenario that demonstrates how to use Boto3 to manage IoT physical assets
    using
    the AWS IoT SiteWise.
    """

    def __init__(
        self,
        iot_siteWise_wrapper: IoTSiteWiseWrapper,
        cloud_formation_resource: ServiceResource,
    ):
        self.iot_siteWise_wrapper = iot_siteWise_wrapper
        self.cloud_formation_resource = cloud_formation_resource
        self.stack = None
```

```

        self.asset_model_id = None
        self.asset_id = None
        self.portal_id = None
        self.gateway_id = None

```

```

def run(self) -> None:
    """
    Runs the scenario.
    """
    print(
        """

```

AWS IoT SiteWise is a fully managed software-as-a-service (SaaS) that makes it easy to collect, store, organize, and monitor data from industrial equipment and processes.

It is designed to help industrial and manufacturing organizations collect data from their equipment and processes, and use that data to make informed decisions about their operations.

One of the key features of AWS IoT SiteWise is its ability to connect to a wide range of industrial equipment and systems, including programmable logic controllers (PLCs), sensors, and other industrial devices. It can collect data from these devices and organize it into a unified data model, making it easier to analyze and gain insights from the data. AWS IoT SiteWise also provides tools for visualizing the data, setting up alarms and alerts, and generating reports.

Another key feature of AWS IoT SiteWise is its ability to scale to handle large volumes of data.

It can collect and store data from thousands of devices and process millions of data points per second, making it suitable for large-scale industrial operations. Additionally, AWS IoT SiteWise is designed to be secure and compliant, with features like role-based access controls, data encryption, and integration with other AWS services for additional security and compliance features.

Let's get started...

```

    """
)
    press_enter_to_continue()
    print_dashes()

```



```

        print(f'')
        print(
            f'Use AWS CloudFormation to create an IAM role that is required for
this scenario.'
        )
        template_file = IoTSitewiseGettingStarted.get_template_as_string()

        self.stack = self.deploy_cloudformation_stack(
            "python-iot-sitewise-basics", template_file
        )
        outputs = self.stack.outputs
        iam_role = None

        for output in outputs:
            if output.get("OutputKey") == "SitewiseRoleArn":
                iam_role = output.get("OutputValue")

        if iam_role is None:
            error_string = f'Failed to retrieve iam_role from CloudFormation
stack.'
            logger.error(error_string)
            raise ValueError(error_string)

        print(f'The ARN of the IAM role is {iam_role}')
        print_dashes()
        print_dashes()
        print(f'1. Create an AWS SiteWise Asset Model')
        print(
            """

```

An AWS IoT SiteWise Asset Model is a way to represent the physical assets, such as equipment, processes, and systems, that exist in an industrial environment. This model provides a structured and hierarchical representation of these assets, allowing users to define the relationships and values of each asset.

This scenario creates two asset model values: temperature and humidity.

```

        """
    )
    press_enter_to_continue()
    asset_model_name = "MyAssetModel1"
    temperature_property_name = "temperature"
    humidity_property_name = "humidity"

```

```

try:
    properties = [
        {
            "name": temperature_property_name,
            "dataType": "DOUBLE",
            "type": {
                "measurement": {},
            },
        },
        {
            "name": humidity_property_name,
            "dataType": "DOUBLE",
            "type": {
                "measurement": {},
            },
        },
    ]
    self.asset_model_id = self.iot_sitewise_wrapper.create_asset_model(
        asset_model_name, properties
    )
    print(
        f"Asset Model successfully created. Asset Model ID:
{self.asset_model_id}. "
    )
except ClientError as err:
    if err.response["Error"]["Code"] == "ResourceAlreadyExistsException":
        self.asset_model_id =
self.get_model_id_for_model_name(asset_model_name)
        print(
            f"Asset Model {asset_model_name} already exists. Asset Model
ID: {self.asset_model_id}. "
        )
    else:
        raise

    press_enter_to_continue()
    print_dashes()
    print(f"2. Create an AWS IoT SiteWise Asset")
    print(
        """

```

The IoT SiteWise model that we just created defines the structure and metadata for your physical assets.

Now we create an asset from the asset model.

```

"""
)
press_enter_to_continue()

self.asset_id = self.iot_sitewise_wrapper.create_asset(
    "MyAsset1", self.asset_model_id
)

print(f"Asset created with ID: {self.asset_id}")
press_enter_to_continue()
print_dashes()
print_dashes()
print(f"3. Retrieve the property ID values")
print(
    """

```

To send data to an asset, we need to get the property ID values. In this scenario, we access the temperature and humidity property ID values.

```

"""
)
press_enter_to_continue()
property_ids = self.iot_sitewise_wrapper.list_asset_model_properties(
    self.asset_model_id
)
humidity_property_id = None
temperature_property_id = None
for property_id in property_ids:
    if property_id.get("name") == humidity_property_name:
        humidity_property_id = property_id.get("id")
    elif property_id.get("name") == temperature_property_name:
        temperature_property_id = property_id.get("id")
if humidity_property_id is None or temperature_property_id is None:
    error_string = f"Failed to retrieve property IDs from Asset Model."
    logger.error(error_string)
    raise ValueError(error_string)

print(f"The Humidity property Id is {humidity_property_id}")
print(f"The Temperature property Id is {temperature_property_id}")
press_enter_to_continue()
print_dashes()
print_dashes()

print(f"4. Send data to an AWS IoT SiteWise Asset")
print(

```

```
"""
```

By sending data to an IoT SiteWise Asset, you can aggregate data from multiple sources, normalize the data into a standard format, and store it in a centralized location. This makes it easier to analyze and gain insights from the data.

In this example, we generate sample temperature and humidity data and send it to the AWS IoT SiteWise asset.

```

"""
)
press_enter_to_continue()

values = [
    {
        "propertyId": humidity_property_id,
        "valueType": "doubleValue",
        "value": 65.0,
    },
    {
        "propertyId": temperature_property_id,
        "valueType": "doubleValue",
        "value": 23.5,
    },
]
self.iot_sitewise_wrapper.batch_put_asset_property_value(self.asset_id,
values)
print(f"Data sent successfully.")

press_enter_to_continue()
print_dashes()
print_dashes()

print(f"5. Retrieve the value of the IoT SiteWise Asset property")
print(
    """

```

IoT SiteWise is an AWS service that allows you to collect, process, and analyze industrial data from connected equipment and sensors. One of the key benefits of reading an IoT SiteWise property is the ability to gain valuable insights from your industrial data.

```
"""
```

```
)
```

```

        press_enter_to_continue()

        property_value = self.iot_sitewise_wrapper.get_asset_property_value(
            self.asset_id, temperature_property_id
        )
        print(f"The property name is '{temperature_property_name}'.")

        print(
            f"The value of this property is: {property_value['value']}
['doubleValue']}"
        )
        press_enter_to_continue()

        property_value = self.iot_sitewise_wrapper.get_asset_property_value(
            self.asset_id, humidity_property_id
        )
        print(f"The property name is '{humidity_property_name}'.")
        print(
            f"The value of this property is: {property_value['value']}
['doubleValue']}"
        )
        press_enter_to_continue()
        print_dashes()
        print_dashes()

        print(f"6. Create an IoT SiteWise Portal")
        print(
            """
An IoT SiteWise Portal allows you to aggregate data from multiple industrial
sources,
such as sensors, equipment, and control systems, into a centralized platform.
            """
        )

        press_enter_to_continue()
        contact_email = q.ask("Enter a contact email for the portal:",
q.non_empty)
        print("Creating the portal. The portal may take a while to become
active.")
        self.portal_id = self.iot_sitewise_wrapper.create_portal(
            "MyPortal1", iam_role, contact_email
        )
        print(f"Portal created successfully. Portal ID {self.portal_id}")
        press_enter_to_continue()

```

```

        print_dashes()
        print_dashes()

        print(f"7. Describe the Portal")
        print(
            """
In this step, we get a description of the portal and display the portal URL.
            """
        )
        press_enter_to_continue()
        portal_description =
self.iot_sitewise_wrapper.describe_portal(self.portal_id)
        print(f"Portal URL: {portal_description['portalStartUrl']}")
        press_enter_to_continue()
        print_dashes()
        print_dashes()

        print(f"8. Create an IoT SiteWise Gateway")
        press_enter_to_continue()
        self.gateway_id = self.iot_sitewise_wrapper.create_gateway(
            "MyGateway1", "MyThing1"
        )
        print(f"Gateway creation completed successfully. id is
{self.gateway_id}")
        print_dashes()
        print_dashes()
        print(f"9. Describe the IoT SiteWise Gateway")
        press_enter_to_continue()

        gateway_description = self.iot_sitewise_wrapper.describe_gateway(
            self.gateway_id
        )
        print(f"Gateway Name: {gateway_description['gatewayName']}")
        print(f"Gateway ARN: {gateway_description['gatewayArn']}")
        print(f"Gateway Platform:\n{gateway_description['gatewayPlatform']}")
        print(f"Gateway Creation Date: {gateway_description['gatewayArn']}")
        print_dashes()
        print_dashes()

        print(f"10. Delete the AWS IoT SiteWise Assets")
        if q.ask("Would you like to delete the IoT SiteWise Assets? (y/n)",
q.is_yesno):
            self.cleanup()
        else:

```

```

        print(f"The resources will not be deleted.")
    print_dashes()
    print_dashes()
    print(f"This concludes the AWS IoT SiteWise Scenario")

def cleanup(self) -> None:
    """
    Deletes the CloudFormation stack and the resources created for the demo.
    """

    if self.gateway_id is not None:
        self.iot_sitewise_wrapper.delete_gateway(self.gateway_id)
        print(f"Deleted gateway with id {self.gateway_id}.")
        self.gateway_id = None
    if self.portal_id is not None:
        self.iot_sitewise_wrapper.delete_portal(self.portal_id)
        print(f"Deleted portal with id {self.portal_id}.")
        self.portal_id = None
    if self.asset_id is not None:
        self.iot_sitewise_wrapper.delete_asset(self.asset_id)
        print(f"Deleted asset with id {self.asset_id}.")
        self.iot_sitewise_wrapper.wait_asset_deleted(self.asset_id)
        self.asset_id = None
    if self.asset_model_id is not None:
        self.iot_sitewise_wrapper.delete_asset_model(self.asset_model_id)
        print(f"Deleted asset model with id {self.asset_model_id}.")
        self.asset_model_id = None
    if self.stack is not None:
        stack = self.stack
        self.stack = None
        self.destroy_cloudformation_stack(stack)

def deploy_cloudformation_stack(
    self, stack_name: str, cfn_template: str
) -> ServiceResource:
    """
    Deploys prerequisite resources used by the scenario. The resources are
    defined in the associated `SitewiseRoles-template.yaml` AWS
    CloudFormation script and are deployed
    as a CloudFormation stack, so they can be easily managed and destroyed.

    :param stack_name: The name of the CloudFormation stack.
    :param cfn_template: The CloudFormation template as a string.
    :return: The CloudFormation stack resource.

```

```

    """
    print(f"Deploying CloudFormation stack: {stack_name}.")
    stack = self.cloud_formation_resource.create_stack(
        StackName=stack_name,
        TemplateBody=cfn_template,
        Capabilities=["CAPABILITY_NAMED_IAM"],
    )
    print(f"CloudFormation stack creation started: {stack_name}")
    print("Waiting for CloudFormation stack creation to complete...")
    waiter = self.cloud_formation_resource.meta.client.get_waiter(
        "stack_create_complete"
    )
    waiter.wait(StackName=stack.name)
    stack.load()
    print("CloudFormation stack creation complete.")

    return stack

def destroy_cloudformation_stack(self, stack: ServiceResource) -> None:
    """
    Destroys the resources managed by the CloudFormation stack, and the
    CloudFormation
    stack itself.

    :param stack: The CloudFormation stack that manages the example
    resources.
    """
    print(
        f"CloudFormation stack '{stack.name}' is being deleted. This may take
    a few minutes."
    )
    stack.delete()
    waiter = self.cloud_formation_resource.meta.client.get_waiter(
        "stack_delete_complete"
    )
    waiter.wait(StackName=stack.name)
    print(f"CloudFormation stack '{stack.name}' has been deleted.")

    @staticmethod
    def get_template_as_string() -> str:
        """
        Returns a string containing this scenario's CloudFormation template.
        """

```



```

        template_file_path = os.path.join(script_dir, "SitewiseRoles-
template.yaml")
        file = open(template_file_path, "r")
        return file.read()

def get_model_id_for_model_name(self, model_name: str) -> str:
    """
    Returns the model ID for the given model name.

    :param model_name: The name of the model.
    :return: The model ID.
    """
    model_id = None
    asset_models = self.iot_sitewise_wrapper.list_asset_models()
    for asset_model in asset_models:
        if asset_model["name"] == model_name:
            model_id = asset_model["id"]
            break
    return model_id

```

Classe IoTSitewise Wrapper que agrupa ações. AWS IoT SiteWise

```

class IoTSitewiseWrapper:
    """Encapsulates AWS IoT SiteWise actions using the client interface."""

    def __init__(self, iotsitewise_client: client) -> None:
        """
        Initializes the IoTSitewiseWrapper with an AWS IoT SiteWise client.

        :param iotsitewise_client: A Boto3 AWS IoT SiteWise client. This client
        provides low-level
                                access to AWS IoT SiteWise services.
        """
        self.iotsitewise_client = iotsitewise_client
        self.entry_id = 0 # Incremented to generate unique entry IDs for
        batch_put_asset_property_value.

    @classmethod
    def from_client(cls) -> "IoTSitewiseWrapper":
        """

```

```

        Creates an IoTSiteWiseWrapper instance with a default AWS IoT SiteWise
        client.

        :return: An instance of IoTSiteWiseWrapper initialized with the default
        AWS IoT SiteWise client.
        """
        iotsitewise_client = boto3.client("iotsitewise")
        return cls(iotsitewise_client)

def create_asset_model(
    self, asset_model_name: str, properties: List[Dict[str, Any]]
) -> str:
    """
    Creates an AWS IoT SiteWise Asset Model.

    :param asset_model_name: The name of the asset model to create.
    :param properties: The property definitions of the asset model.
    :return: The ID of the created asset model.
    """
    try:
        response = self.iotsitewise_client.create_asset_model(
            assetModelName=asset_model_name,
            assetModelDescription="This is a sample asset model
description.",
            assetModelProperties=properties,
        )
        asset_model_id = response["assetModelId"]
        waiter = self.iotsitewise_client.get_waiter("asset_model_active")
        waiter.wait(assetModelId=asset_model_id)
        return asset_model_id
    except ClientError as err:
        if err.response["Error"]["Code"] == "ResourceAlreadyExistsException":
            logger.error("Asset model %s already exists.", asset_model_name)
        else:
            logger.error(
                "Error creating asset model %s. Here's why %s",
                asset_model_name,
                err.response["Error"]["Message"],
            )
        raise

def create_asset(self, asset_name: str, asset_model_id: str) -> str:

```

```

"""
Creates an AWS IoT SiteWise Asset.

:param asset_name: The name of the asset to create.
:param asset_model_id: The ID of the asset model to associate with the
asset.
:return: The ID of the created asset.
"""
try:
    response = self.iotsitewise_client.create_asset(
        assetName=asset_name, assetModelId=asset_model_id
    )
    asset_id = response["assetId"]
    waiter = self.iotsitewise_client.get_waiter("asset_active")
    waiter.wait(assetId=asset_id)
    return asset_id
except ClientError as err:
    if err.response["Error"] == "ResourceNotFoundException":
        logger.error("Asset model %s does not exist.", asset_model_id)
    else:
        logger.error(
            "Error creating asset %s. Here's why %s",
            asset_name,
            err.response["Error"]["Message"],
        )
    raise


def list_asset_models(self) -> List[Dict[str, Any]]:
    """
    Lists all AWS IoT SiteWise Asset Models.

    :return: A list of dictionaries containing information about each asset
    model.

    """
    try:
        asset_models = []
        paginator =
self.iotsitewise_client.get_paginator("list_asset_models")
        pages = paginator.paginate()
        for page in pages:
            asset_models.extend(page["assetModelSummaries"])
        return asset_models

```

```

    except ClientError as err:
        logger.error(
            "Error listing asset models. Here's why %s",
            err.response["Error"]["Message"],
        )
        raise

    def list_asset_model_properties(self, asset_model_id: str) -> List[Dict[str,
Any]]:
        """
        Lists all AWS IoT SiteWise Asset Model Properties.

        :param asset_model_id: The ID of the asset model to list values for.
        :return: A list of dictionaries containing information about each asset
model property.
        """
        try:
            asset_model_properties = []
            paginator = self.iotsitewise_client.get_paginator(
                "list_asset_model_properties"
            )
            pages = paginator.paginate(assetModelId=asset_model_id)
            for page in pages:

asset_model_properties.extend(page["assetModelPropertySummaries"])
            return asset_model_properties
        except ClientError as err:
            logger.error(
                "Error listing asset model values. Here's why %s",
                err.response["Error"]["Message"],
            )
            raise

    def batch_put_asset_property_value(
        self, asset_id: str, values: List[Dict[str, str]]
    ) -> None:
        """
        Sends data to an AWS IoT SiteWise Asset.

        :param asset_id: The asset ID.
        :param values: A list of dictionaries containing the values in the form
{propertyId : property_id,

```

```

        valueType : [stringValue|integerValue|doubleValue|
booleanValue],
        value : the_value}.

"""
try:
    entries = self.properties_to_values(asset_id, values)

self.iotsitewise_client.batch_put_asset_property_value(entries=entries)
except ClientError as err:
    if err.response["Error"]["Code"] == "ResourceNotFoundException":
        logger.error("Asset %s does not exist.", asset_id)
    else:
        logger.error(
            "Error sending data to asset. Here's why %s",
            err.response["Error"]["Message"],
        )
    raise

def properties_to_values(
    self, asset_id: str, values: list[dict[str, Any]]
) -> list[dict[str, Any]]:
    """
    Utility function to convert a values list to the entries parameter for
    batch_put_asset_property_value.
    :param asset_id : The asset ID.
    :param values : A list of dictionaries containing the values in the form
        {propertyId : property_id,
        valueType : [stringValue|integerValue|doubleValue|
booleanValue],
        value : the_value}.
    :return: An entries list to pass as the 'entries' parameter to
    batch_put_asset_property_value.
    """
    entries = []
    for value in values:
        epoch_ns = time.time_ns()
        self.entry_id += 1
        if value["valueType"] == "stringValue":
            property_value = {"stringValue": value["value"]}
        elif value["valueType"] == "integerValue":
            property_value = {"integerValue": value["value"]}
        elif value["valueType"] == "booleanValue":
            property_value = {"booleanValue": value["value"]}

```

```

        elif value["valueType"] == "doubleValue":
            property_value = {"doubleValue": value["value"]}
        else:
            raise ValueError("Invalid valueType: %s", value["valueType"])
    entry = {
        "entryId": f"{self.entry_id}",
        "assetId": asset_id,
        "propertyId": value["propertyId"],
        "propertyValues": [
            {
                "value": property_value,
                "timestamp": {
                    "timeInSeconds": int(epoch_ns / 1000000000),
                    "offsetInNanos": epoch_ns % 1000000000,
                },
            }
        ],
    }
    entries.append(entry)
return entries

def get_asset_property_value(
    self, asset_id: str, property_id: str
) -> Dict[str, Any]:
    """
    Gets the value of an AWS IoT SiteWise Asset Property.

    :param asset_id: The ID of the asset.
    :param property_id: The ID of the property.
    :return: A dictionary containing the value of the property.
    """
    try:
        response = self.iotsitewise_client.get_asset_property_value(
            assetId=asset_id, propertyId=property_id
        )
        return response["propertyValue"]
    except ClientError as err:
        if err.response["Error"]["Code"] == "ResourceNotFoundException":
            logger.error(
                "Asset %s or property %s does not exist.", asset_id,
property_id
            )
        else:

```

```

        logger.error(
            "Error getting asset property value. Here's why %s",
            err.response["Error"]["Message"],
        )
        raise

def create_portal(
    self, portal_name: str, iam_role_arn: str, portal_contact_email: str
) -> str:
    """
    Creates an AWS IoT SiteWise Portal.

    :param portal_name: The name of the portal to create.
    :param iam_role_arn: The ARN of an IAM role.
    :param portal_contact_email: The contact email of the portal.
    :return: The ID of the created portal.
    """
    try:
        response = self.iotsitewise_client.create_portal(
            portalName=portal_name,
            roleArn=iam_role_arn,
            portalContactEmail=portal_contact_email,
        )
        portal_id = response["portalId"]
        waiter = self.iotsitewise_client.get_waiter("portal_active")
        waiter.wait(portalId=portal_id, WaiterConfig={"MaxAttempts": 40})
        return portal_id
    except ClientError as err:
        if err.response["Error"]["Code"] == "ResourceAlreadyExistsException":
            logger.error("Portal %s already exists.", portal_name)
        else:
            logger.error(
                "Error creating portal %s. Here's why %s",
                portal_name,
                err.response["Error"]["Message"],
            )
            raise

def describe_portal(self, portal_id: str) -> Dict[str, Any]:
    """
    Describes an AWS IoT SiteWise Portal.

```

```

        :param portal_id: The ID of the portal to describe.
        :return: A dictionary containing information about the portal.
        """
        try:
            response =
self.iotsitewise_client.describe_portal(portalId=portal_id)
            return response
        except ClientError as err:
            logger.error(
                "Error describing portal %s. Here's why %s",
                portal_id,
                err.response["Error"]["Message"],
            )
            raise

def create_gateway(self, gateway_name: str, my_thing: str) -> str:
    """
    Creates an AWS IoT SiteWise Gateway.

    :param gateway_name: The name of the gateway to create.
    :param my_thing: The core device thing name.
    :return: The ID of the created gateway.
    """
    try:
        response = self.iotsitewise_client.create_gateway(
            gatewayName=gateway_name,
            gatewayPlatform={
                "greengrassV2": {"coreDeviceThingName": my_thing},
            },
            tags={"Environment": "Production"},
        )
        gateway_id = response["gatewayId"]
        return gateway_id
    except ClientError as err:
        if err.response["Error"]["Code"] == "ResourceAlreadyExistsException":
            logger.error("Gateway %s already exists.", gateway_name)
        else:
            logger.error(
                "Error creating gateway %s. Here's why %s",
                gateway_name,
                err.response["Error"]["Message"],
            )
            raise

```



```
def describe_gateway(self, gateway_id: str) -> Dict[str, Any]:
    """
    Describes an AWS IoT SiteWise Gateway.

    :param gateway_id: The ID of the gateway to describe.
    :return: A dictionary containing information about the gateway.
    """
    try:
        response =
self.iotsitewise_client.describe_gateway(gatewayId=gateway_id)
        return response
    except ClientError as err:
        if err.response["Error"]["Code"] == "ResourceNotFoundException":
            logger.error("Gateway %s does not exist.", gateway_id)
        else:
            logger.error(
                "Error describing gateway %s. Here's why %s",
                gateway_id,
                err.response["Error"]["Message"],
            )
        raise

def delete_gateway(self, gateway_id: str) -> None:
    """
    Deletes an AWS IoT SiteWise Gateway.

    :param gateway_id: The ID of the gateway to delete.
    """
    try:
        self.iotsitewise_client.delete_gateway(gatewayId=gateway_id)
    except ClientError as err:
        if err.response["Error"]["Code"] == "ResourceNotFoundException":
            logger.error("Gateway %s does not exist.", gateway_id)
        else:
            logger.error(
                "Error deleting gateway %s. Here's why %s",
                gateway_id,
                err.response["Error"]["Message"],
            )
        raise
```

```
def delete_portal(self, portal_id: str) -> None:
    """
    Deletes an AWS IoT SiteWise Portal.

    :param portal_id: The ID of the portal to delete.
    """
    try:
        self.iotsitewise_client.delete_portal(portalId=portal_id)
    except ClientError as err:
        if err.response["Error"]["Code"] == "ResourceNotFoundException":
            logger.error("Portal %s does not exist.", portal_id)
        else:
            logger.error(
                "Error deleting portal %s. Here's why %s",
                portal_id,
                err.response["Error"]["Message"],
            )
        raise

def delete_asset(self, asset_id: str) -> None:
    """
    Deletes an AWS IoT SiteWise Asset.

    :param asset_id: The ID of the asset to delete.
    """
    try:
        self.iotsitewise_client.delete_asset(assetId=asset_id)
    except ClientError as err:
        logger.error(
            "Error deleting asset %s. Here's why %s",
            asset_id,
            err.response["Error"]["Message"],
        )
        raise

def delete_asset_model(self, asset_model_id: str) -> None:
    """
    Deletes an AWS IoT SiteWise Asset Model.

    :param asset_model_id: The ID of the asset model to delete.
    """
```

```

try:

self.iotsitewise_client.delete_asset_model(assetModelId=asset_model_id)
except ClientError as err:
    logger.error(
        "Error deleting asset model %s. Here's why %s",
        asset_model_id,
        err.response["Error"]["Message"],
    )
    raise

def wait_asset_deleted(self, asset_id: str) -> None:
    """
    Waits for an AWS IoT SiteWise Asset to be deleted.

    :param asset_id: The ID of the asset to wait for.
    """
    try:
        waiter = self.iotsitewise_client.get_waiter("asset_not_exists")
        waiter.wait(assetId=asset_id)
    except ClientError as err:
        logger.error(
            "Error waiting for asset %s to be deleted. Here's why %s",
            asset_id,
            err.response["Error"]["Message"],
        )
        raise

```

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando esse serviço com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Ações para AWS IoT SiteWise usar AWS SDKs

Os exemplos de código a seguir demonstram como realizar AWS IoT SiteWise ações individuais com AWS SDKs. Cada exemplo inclui um link para GitHub, onde você pode encontrar instruções para configurar e executar o código.

Os exemplos a seguir incluem apenas as ações mais utilizadas. Para obter uma lista completa, consulte a [Referência de APIs do AWS IoT SiteWise](#).

Exemplos

- [Use BatchPutAssetPropertyValue com um AWS SDK ou CLI](#)
- [Use CreateAsset com um AWS SDK ou CLI](#)
- [Use CreateAssetModel com um AWS SDK ou CLI](#)
- [Use CreateGateway com um AWS SDK ou CLI](#)
- [Use CreatePortal com um AWS SDK ou CLI](#)
- [Use DeleteAsset com um AWS SDK ou CLI](#)
- [Use DeleteAssetModel com um AWS SDK ou CLI](#)
- [Use DeleteGateway com um AWS SDK ou CLI](#)
- [Use DeletePortal com um AWS SDK ou CLI](#)
- [Use DescribeAssetModel com um AWS SDK ou CLI](#)
- [Use DescribeGateway com um AWS SDK ou CLI](#)
- [Use DescribePortal com um AWS SDK ou CLI](#)
- [Use GetAssetPropertyValue com um AWS SDK ou CLI](#)
- [Use ListAssetModels com um AWS SDK ou CLI](#)

Use **BatchPutAssetPropertyValue** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o BatchPutAssetPropertyValue.

CLI

AWS CLI

Para enviar dados às propriedades do ativo

O exemplo batch-put-asset-property-value a seguir envia dados de potência e temperatura para as propriedades do ativo identificadas pelos aliases da propriedade.

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

Conteúdo de batch-put-asset-property-value.json:

```
{
  "entries": [
    {
      "entryId": "1575691200-company-windfarm-3-turbine-7-power",
      "propertyAlias": "company-windfarm-3-turbine-7-power",
      "propertyValues": [
        {
          "value": {
            "doubleValue": 4.92
          },
          "timestamp": {
            "timeInSeconds": 1575691200
          },
          "quality": "GOOD"
        }
      ]
    },
    {
      "entryId": "1575691200-company-windfarm-3-turbine-7-temperature",
      "propertyAlias": "company-windfarm-3-turbine-7-temperature",
      "propertyValues": [
        {
          "value": {
            "integerValue": 38
          },
          "timestamp": {
            "timeInSeconds": 1575691200
          }
        }
      ]
    }
  ]
}
```

Saída:

```
{
  "errorEntries": []
}
```

Para obter mais informações, consulte Como [ingerir dados usando a API de AWS SiteWise IoT no](#) Guia do usuário de AWS IoT SiteWise .

- Para obter detalhes da API, consulte [BatchPutAssetPropertyValue](#) em Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
/**
 * Sends data to the SiteWise service.
 *
 * @param assetId      the ID of the asset to which the data will be sent.
 * @param tempPropertyId the ID of the temperature property.
 * @param humidityPropId the ID of the humidity property.
 * @return a {@link CompletableFuture} that represents a {@link
BatchPutAssetPropertyValueResponse} result. The
 *      calling code can attach callbacks, then handle the result or
exception by calling
 *      {@link CompletableFuture#join()} or {@link
CompletableFuture#get()}.
 *      <p>
 *      If any completion stage in this method throws an exception, the
method logs the exception cause and keeps it
 *      available to the calling code as a {@link CompletionException}. By
calling
 *      {@link CompletionException#getCause()}, the calling code can
access the original exception.
 */
public CompletableFuture<BatchPutAssetPropertyValueResponse>
sendDataToSiteWiseAsync(String assetId, String tempPropertyId, String
humidityPropId) {
    Map<String, Double> sampleData = generateSampleData();
    long timestamp = Instant.now().toEpochMilli();

    TimeInNanos time = TimeInNanos.builder()
        .timeInSeconds(timestamp / 1000)
```

```

        .offsetInNanos((int) ((timestamp % 1000) * 1000000))
        .build();

    BatchPutAssetPropertyValueRequest request =
    BatchPutAssetPropertyValueRequest.builder()
        .entries(Arrays.asList(
            PutAssetPropertyValueEntry.builder()
                .entryId("entry-3")
                .assetId(assetId)
                .propertyId(tempPropertyId)
                .propertyValues(Arrays.asList(
                    AssetPropertyValue.builder()
                        .value(Variant.builder()
                            .doubleValue(sampleData.get("Temperature"))
                            .build())
                        .timestamp(time)
                        .build()
                ))
                .build(),
            PutAssetPropertyValueEntry.builder()
                .entryId("entry-4")
                .assetId(assetId)
                .propertyId(humidityPropId)
                .propertyValues(Arrays.asList(
                    AssetPropertyValue.builder()
                        .value(Variant.builder()
                            .doubleValue(sampleData.get("Humidity"))
                            .build())
                        .timestamp(time)
                        .build()
                ))
                .build()
        ))
        .build();

    return getAsyncClient().batchPutAssetPropertyValue(request)
        .whenComplete((response, exception) -> {
            if (exception != null) {
                logger.error("An exception occurred: {}",
exception.getCause().getMessage());
            }
        });
}

```

- Para obter detalhes da API, consulte [BatchPutAssetPropertyValue](#) a Referência AWS SDK for Java 2.x da API.

JavaScript

SDK para JavaScript (v3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
import {
  BatchPutAssetPropertyValueCommand,
  IoTSiteWiseClient,
} from "@aws-sdk/client-iotsitewise";
import { parseArgs } from "node:util";

/**
 * Batch put asset property values.
 * @param {{ entries : array }}
 */
export const main = async ({ entries }) => {
  const client = new IoTSiteWiseClient({});
  try {
    const result = await client.send(
      new BatchPutAssetPropertyValueCommand({
        entries: entries,
      }),
    );
    console.log("Asset properties batch put successfully.");
    return result;
  } catch (caught) {
    if (caught instanceof Error && caught.name === "ResourceNotFound") {
      console.warn(`${caught.message}. A resource could not be found.`);
    } else {
      throw caught;
    }
  }
}
```



```
}
};
```

- Para obter detalhes da API, consulte [BatchPutAssetPropertyValue](#) a Referência AWS SDK para JavaScript da API.

Python

SDK para Python (Boto3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
class IoTSiteWiseWrapper:
    """Encapsulates AWS IoT SiteWise actions using the client interface."""

    def __init__(self, iotsitewise_client: client) -> None:
        """
        Initializes the IoTSiteWiseWrapper with an AWS IoT SiteWise client.

        :param iotsitewise_client: A Boto3 AWS IoT SiteWise client. This client
        provides low-level
            access to AWS IoT SiteWise services.
        """
        self.iotsitewise_client = iotsitewise_client
        self.entry_id = 0 # Incremented to generate unique entry IDs for
        batch_put_asset_property_value.

    @classmethod
    def from_client(cls) -> "IoTSiteWiseWrapper":
        """
        Creates an IoTSiteWiseWrapper instance with a default AWS IoT SiteWise
        client.

        :return: An instance of IoTSiteWiseWrapper initialized with the default
        AWS IoT SiteWise client.
        """
```

```

    iotsitewise_client = boto3.client("iotsitewise")
    return cls(iotsitewise_client)

def batch_put_asset_property_value(
    self, asset_id: str, values: List[Dict[str, str]]
) -> None:
    """
    Sends data to an AWS IoT SiteWise Asset.

    :param asset_id: The asset ID.
    :param values: A list of dictionaries containing the values in the form
        {propertyId : property_id,
         valueType : [stringValue|integerValue|doubleValue|
booleanValue],
         value : the_value}.
    """
    try:
        entries = self.properties_to_values(asset_id, values)

self.iotsitewise_client.batch_put_asset_property_value(entries=entries)
    except ClientError as err:
        if err.response["Error"]["Code"] == "ResourceNotFoundException":
            logger.error("Asset %s does not exist.", asset_id)
        else:
            logger.error(
                "Error sending data to asset. Here's why %s",
                err.response["Error"]["Message"],
            )
        raise

```

Uma função auxiliar para gerar o parâmetro de entradas a partir de uma lista de valores.

```

def properties_to_values(
    self, asset_id: str, values: list[dict[str, Any]]
) -> list[dict[str, Any]]:
    """
    Utility function to convert a values list to the entries parameter for
    batch_put_asset_property_value.
    :param asset_id : The asset ID.
    :param values : A list of dictionaries containing the values in the form

```

```

        {propertyId : property_id,
         valueType : [stringValue|integerValue|doubleValue|
booleanValue],
         value : the_value}.
    :return: An entries list to pass as the 'entries' parameter to
batch_put_asset_property_value.
"""
entries = []
for value in values:
    epoch_ns = time.time_ns()
    self.entry_id += 1
    if value["valueType"] == "stringValue":
        property_value = {"stringValue": value["value"]}
    elif value["valueType"] == "integerValue":
        property_value = {"integerValue": value["value"]}
    elif value["valueType"] == "booleanValue":
        property_value = {"booleanValue": value["value"]}
    elif value["valueType"] == "doubleValue":
        property_value = {"doubleValue": value["value"]}
    else:
        raise ValueError("Invalid valueType: %s", value["valueType"])
    entry = {
        "entryId": f"{self.entry_id}",
        "assetId": asset_id,
        "propertyId": value["propertyId"],
        "propertyValues": [
            {
                "value": property_value,
                "timestamp": {
                    "timeInSeconds": int(epoch_ns / 1000000000),
                    "offsetInNanos": epoch_ns % 1000000000,
                },
            },
        ],
    }
    entries.append(entry)
return entries

```

Aqui está um exemplo de uma lista de valores para passar para a função auxiliar.

```
values = [
```

```
{
  "propertyId": humidity_property_id,
  "valueType": "doubleValue",
  "value": 65.0,
},
{
  "propertyId": temperature_property_id,
  "valueType": "doubleValue",
  "value": 23.5,
},
]
```

- Para obter detalhes da API, consulte a [BatchPutAssetPropertyValue](#) Referência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando esse serviço com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **CreateAsset** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o CreateAsset.

CLI

AWS CLI

Para criar um ativo

O exemplo create-asset a seguir cria um ativo de turbina eólica a partir de um modelo de ativo de turbina eólica.

```
aws iotsitewise create-asset \
  --asset-model-id a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
  --asset-name "Wind Turbine 1"
```

Saída:

```
{
```

```

    "assetId": "a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
    "assetArn": "arn:aws:iotsitewise:us-west-2:123456789012:asset/
a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
    "assetStatus": {
        "state": "CREATING"
    }
}

```

Para obter mais informações, consulte [Criação de ativos](#) no Guia do SiteWise Usuário de AWS IoT.

- Para obter detalhes da API, consulte [CreateAsset](#) em Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```

/**
 * Creates an asset with the specified name and asset model Id.
 *
 * @param assetName    the name of the asset to create.
 * @param assetModelId the Id of the asset model to associate with the asset.
 * @return a {@link CompletableFuture} that represents a {@link
CreateAssetResponse} result. The calling code can
 *         attach callbacks, then handle the result or exception by calling
{@link CompletableFuture#join()} or
 *         {@link CompletableFuture#get()}.
 *         <p>
 *         If any completion stage in this method throws an exception, the
method logs the exception cause and keeps it
 *         available to the calling code as a {@link CompletionException}. By
calling
 *         {@link CompletionException#getCause()}, the calling code can
access the original exception.
 */

```

```
public CompletableFuture<CreateAssetResponse> createAssetAsync(String
assetName, String assetModelId) {
    CreateAssetRequest createAssetRequest = CreateAssetRequest.builder()
        .assetModelId(assetModelId)
        .assetDescription("Created using the AWS SDK for Java")
        .assetName(assetName)
        .build();

    return getAsyncClient().createAsset(createAssetRequest)
        .whenComplete((response, exception) -> {
            if (exception != null) {
                logger.error("Failed to create asset: {}",
exception.getCause().getMessage());
            }
        });
}
```

- Para obter detalhes da API, consulte [CreateAsset](#) Referência AWS SDK for Java 2.x da API.

JavaScript

SDK para JavaScript (v3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
import {
    CreateAssetCommand,
    IoTSiteWiseClient,
} from "@aws-sdk/client-iotsitewise";
import { parseArgs } from "node:util";

/**
 * Create an Asset.
 * @param {{ assetName : string, assetModelId: string }}
 */
```

```
export const main = async ({ assetName, assetModelId }) => {
  const client = new IoTSiteWiseClient({});
  try {
    const result = await client.send(
      new CreateAssetCommand({
        assetName: assetName, // The name to give the Asset.
        assetModelId: assetModelId, // The ID of the asset model from which to
        // create the asset.
      })),
    );
    console.log("Asset created successfully.");
    return result;
  } catch (caught) {
    if (caught instanceof Error && caught.name === "ResourceNotFound") {
      console.warn(
        `${caught.message}. The asset model could not be found. Please check the
        asset model id.`);
    } else {
      throw caught;
    }
  }
};
```

- Para obter detalhes da API, consulte [CreateAsset](#) a Referência AWS SDK para JavaScript da API.

Python

SDK para Python (Boto3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
class IoTSiteWiseWrapper:
    """Encapsulates AWS IoT SiteWise actions using the client interface."""
```

```

def __init__(self, iotsitewise_client: client) -> None:
    """
    Initializes the IoTSiteWiseWrapper with an AWS IoT SiteWise client.

    :param iotsitewise_client: A Boto3 AWS IoT SiteWise client. This client
    provides low-level
                                access to AWS IoT SiteWise services.
    """
    self.iotsitewise_client = iotsitewise_client
    self.entry_id = 0 # Incremented to generate unique entry IDs for
    batch_put_asset_property_value.

    @classmethod
    def from_client(cls) -> "IoTSiteWiseWrapper":
        """
        Creates an IoTSiteWiseWrapper instance with a default AWS IoT SiteWise
        client.

        :return: An instance of IoTSiteWiseWrapper initialized with the default
        AWS IoT SiteWise client.
        """
        iotsitewise_client = boto3.client("iotsitewise")
        return cls(iotsitewise_client)

    def create_asset(self, asset_name: str, asset_model_id: str) -> str:
        """
        Creates an AWS IoT SiteWise Asset.

        :param asset_name: The name of the asset to create.
        :param asset_model_id: The ID of the asset model to associate with the
        asset.
        :return: The ID of the created asset.
        """
        try:
            response = self.iotsitewise_client.create_asset(
                assetName=asset_name, assetModelId=asset_model_id
            )
            asset_id = response["assetId"]
            waiter = self.iotsitewise_client.get_waiter("asset_active")
            waiter.wait(assetId=asset_id)
            return asset_id
        except ClientError as err:
            if err.response["Error"] == "ResourceNotFoundException":

```



```
        logger.error("Asset model %s does not exist.", asset_model_id)
    else:
        logger.error(
            "Error creating asset %s. Here's why %s",
            asset_name,
            err.response["Error"]["Message"],
        )
    raise
```

- Para obter detalhes da API, consulte a [CreateAsset](#)Referência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando esse serviço com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **CreateAssetModel** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o `CreateAssetModel`.

CLI

AWS CLI

Para criar um modelo de ativo

O exemplo `create-asset-model` a seguir cria um modelo de ativo que define uma turbina eólica com as seguintes propriedades:

Número de série - O número de série de uma turbina eólica
Energia gerada - O fluxo de dados de energia gerada de uma turbina eólica
Temperatura C - O fluxo de dados de temperatura de uma turbina eólica em Celsius
Temperatura F - Os pontos de dados de temperatura mapeados de Celsius a Fahrenheit

```
aws iotsitewise create-asset-model \
  --cli-input-json file://create-wind-turbine-model.json
```

Conteúdo de `create-wind-turbine-model.json`:

```
{
  "assetModelName": "Wind Turbine Model",
  "assetModelDescription": "Represents a wind turbine",
  "assetModelProperties": [
    {
      "name": "Serial Number",
      "dataType": "STRING",
      "type": {
        "attribute": {}
      }
    },
    {
      "name": "Generated Power",
      "dataType": "DOUBLE",
      "unit": "kW",
      "type": {
        "measurement": {}
      }
    },
    {
      "name": "Temperature C",
      "dataType": "DOUBLE",
      "unit": "Celsius",
      "type": {
        "measurement": {}
      }
    },
    {
      "name": "Temperature F",
      "dataType": "DOUBLE",
      "unit": "Fahrenheit",
      "type": {
        "transform": {
          "expression": "temp_c * 9 / 5 + 32",
          "variables": [
            {
              "name": "temp_c",
              "value": {
                "propertyId": "Temperature C"
              }
            }
          ]
        }
      }
    }
  ]
}
```

```

    }
  },
  {
    "name": "Total Generated Power",
    "dataType": "DOUBLE",
    "unit": "kW",
    "type": {
      "metric": {
        "expression": "sum(power)",
        "variables": [
          {
            "name": "power",
            "value": {
              "propertyId": "Generated Power"
            }
          }
        ],
        "window": {
          "tumbling": {
            "interval": "1h"
          }
        }
      }
    }
  }
]
}

```

Saída:

```

{
  "assetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
  "assetModelArn": "arn:aws:iotsitewise:us-west-2:123456789012:asset-model/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
  "assetModelStatus": {
    "state": "CREATING"
  }
}

```

Para obter mais informações, consulte [Definição de modelos de ativos](#) no Guia do SiteWise usuário de AWS IoT.

- Para obter detalhes da API, consulte [CreateAssetModel](#) em Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
/**
 * Creates an asset model.
 *
 * @param name the name of the asset model to create.
 * @return a {@link CompletableFuture} that represents a {@link
CreateAssetModelResponse} result. The calling code
 *       can attach callbacks, then handle the result or exception by
calling {@link CompletableFuture#join()} or
 *       {@link CompletableFuture#get()}.
 *       <p>
 *       If any completion stage in this method throws an exception, the
method logs the exception cause and keeps it
 *       available to the calling code as a {@link CompletionException}. By
calling
 *       {@link CompletionException#getCause()}, the calling code can
access the original exception.
 */
public CompletableFuture<CreateAssetModelResponse>
createAssetModelAsync(String name) {
    PropertyType humidity = PropertyType.builder()
        .measurement(Measurement.builder().build())
        .build();

    PropertyType temperaturePropertyType = PropertyType.builder()
        .measurement(Measurement.builder().build())
        .build();
```

```
AssetModelPropertyDefinition temperatureProperty =
AssetModelPropertyDefinition.builder()
    .name("Temperature")
    .dataType(PropertyDataType.DOUBLE)
    .type(temperaturePropertyType)
    .build();

AssetModelPropertyDefinition humidityProperty =
AssetModelPropertyDefinition.builder()
    .name("Humidity")
    .dataType(PropertyDataType.DOUBLE)
    .type(humidity)
    .build();

CreateAssetModelRequest createAssetModelRequest =
CreateAssetModelRequest.builder()
    .assetModelName(name)
    .assetModelDescription("This is my asset model")
    .assetModelProperties(temperatureProperty, humidityProperty)
    .build();

return getAsyncClient().createAssetModel(createAssetModelRequest)
    .whenComplete((response, exception) -> {
        if (exception != null) {
            logger.error("Failed to create asset model: {} ",
exception.getCause().getMessage());
        }
    });
}
```

- Para obter detalhes da API, consulte [CreateAssetModel](#) a Referência AWS SDK for Java 2.x da API.

JavaScript

SDK para JavaScript (v3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
import {
  CreateAssetModelCommand,
  IoTSiteWiseClient,
} from "@aws-sdk/client-iotsitewise";
import { parseArgs } from "node:util";

/**
 * Create an Asset Model.
 * @param {{ assetName : string, assetModelId: string }}
 */
export const main = async ({ assetModelName, assetModelId }) => {
  const client = new IoTSiteWiseClient({});
  try {
    const result = await client.send(
      new CreateAssetModelCommand({
        assetModelName: assetModelName, // The name to give the Asset Model.
      }),
    );
    console.log("Asset model created successfully.");
    return result;
  } catch (caught) {
    if (caught instanceof Error && caught.name === "IoTSiteWiseError") {
      console.warn(
        `${caught.message}. There was a problem creating the asset model.`
      );
    } else {
      throw caught;
    }
  }
};
```

- Para obter detalhes da API, consulte [CreateAssetModel](#) a Referência AWS SDK para JavaScript da API.

Python

SDK para Python (Boto3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
class IoTSiteWiseWrapper:
    """Encapsulates AWS IoT SiteWise actions using the client interface."""

    def __init__(self, iotsitewise_client: client) -> None:
        """
        Initializes the IoTSiteWiseWrapper with an AWS IoT SiteWise client.

        :param iotsitewise_client: A Boto3 AWS IoT SiteWise client. This client
        provides low-level
                                access to AWS IoT SiteWise services.
        """
        self.iotsitewise_client = iotsitewise_client
        self.entry_id = 0 # Incremented to generate unique entry IDs for
        batch_put_asset_property_value.

    @classmethod
    def from_client(cls) -> "IoTSiteWiseWrapper":
        """
        Creates an IoTSiteWiseWrapper instance with a default AWS IoT SiteWise
        client.

        :return: An instance of IoTSiteWiseWrapper initialized with the default
        AWS IoT SiteWise client.
        """
        iotsitewise_client = boto3.client("iotsitewise")
        return cls(iotsitewise_client)
```

```

def create_asset_model(
    self, asset_model_name: str, properties: List[Dict[str, Any]]
) -> str:
    """
    Creates an AWS IoT SiteWise Asset Model.

    :param asset_model_name: The name of the asset model to create.
    :param properties: The property definitions of the asset model.
    :return: The ID of the created asset model.
    """
    try:
        response = self.iotsitewise_client.create_asset_model(
            assetModelName=asset_model_name,
            assetModelDescription="This is a sample asset model
description.",
            assetModelProperties=properties,
        )
        asset_model_id = response["assetModelId"]
        waiter = self.iotsitewise_client.get_waiter("asset_model_active")
        waiter.wait(assetModelId=asset_model_id)
        return asset_model_id
    except ClientError as err:
        if err.response["Error"]["Code"] == "ResourceAlreadyExistsException":
            logger.error("Asset model %s already exists.", asset_model_name)
        else:
            logger.error(
                "Error creating asset model %s. Here's why %s",
                asset_model_name,
                err.response["Error"]["Message"],
            )
        raise

```

Aqui está um exemplo de uma lista de propriedades para passar para a função.

```

properties = [
    {
        "name": temperature_property_name,
        "dataType": "DOUBLE",
        "type": {
            "measurement": {},
        },
    },

```



```

    },
    {
      "name": humidity_property_name,
      "dataType": "DOUBLE",
      "type": {
        "measurement": {},
      },
    },
  ],
]

```

- Para obter detalhes da API, consulte a [CreateAssetModel](#) Referência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando esse serviço com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **CreateGateway** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o CreateGateway.

CLI

AWS CLI

Para criar um gateway

O create-gateway exemplo a seguir cria um gateway que é executado no AWS IoT Greengrass.

```

aws iotsitewise create-gateway \
  --gateway-name ExampleCorpGateway \
  --gateway-platform greengrass={groupArn=arn:aws:greengrass:us-west-2:123456789012:/greengrass/groups/a1b2c3d4-5678-90ab-cdef-1b1b1EXAMPLE}

```

Saída:

```

{
  "gatewayId": "a1b2c3d4-5678-90ab-cdef-1a1a1EXAMPLE",
  "gatewayArn": "arn:aws:iotsitewise:us-west-2:123456789012:gateway/a1b2c3d4-5678-90ab-cdef-1a1a1EXAMPLE"
}

```

```
}
```

Para obter mais informações, consulte [Configurando um gateway no Guia](#) do usuário de AWS SiteWise IoT.

- Para obter detalhes da API, consulte [CreateGateway](#) em Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
/**
 * Creates a new IoT Sitewise gateway.
 *
 * @param gatewayName The name of the gateway to create.
 * @param myThing      The name of the core device thing to associate with the
gateway.
 * @return a {@link CompletableFuture} that represents a {@link String}
result of the gateways ID. The calling code
 *         can attach callbacks, then handle the result or exception by
calling {@link CompletableFuture#join()} or
 *         {@link CompletableFuture#get()}.
 *         <p>
 *         If any completion stage in this method throws an exception, the
method logs the exception cause and keeps
 *         it available to the calling code as a {@link CompletionException}.
By calling
 *         {@link CompletionException#getCause()}, the calling code can
access the original exception.
 */
public CompletableFuture<String> createGatewayAsync(String gatewayName,
String myThing) {
    GreengrassV2 gg = GreengrassV2.builder()
```

```
        .coreDeviceThingName(myThing)
        .build();

GatewayPlatform platform = GatewayPlatform.builder()
    .greengrassV2(gg)
    .build();

Map<String, String> tag = new HashMap<>();
tag.put("Environment", "Production");

CreateGatewayRequest createGatewayRequest =
CreateGatewayRequest.builder()
    .gatewayName(gatewayName)
    .gatewayPlatform(platform)
    .tags(tag)
    .build();

return getAsyncClient().createGateway(createGatewayRequest)
    .handle((response, exception) -> {
        if (exception != null) {
            logger.error("Error creating the gateway.");
            throw (CompletionException) exception;
        }
        logger.info("The ARN of the gateway is {}" ,
response.gatewayArn());
        return response.gatewayId();
    });
}
```

- Para obter detalhes da API, consulte [CreateGateway](#) Referência AWS SDK for Java 2.x da API.

JavaScript

SDK para JavaScript (v3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
import {
  CreateGatewayCommand,
  IoTSiteWiseClient,
} from "@aws-sdk/client-iotsitewise";
import { parseArgs } from "node:util";

/**
 * Create a Gateway.
 * @param {{ }}
 */
export const main = async ({ gatewayName }) => {
  const client = new IoTSiteWiseClient({});
  try {
    const result = await client.send(
      new CreateGatewayCommand({
        gatewayName: gatewayName, // The name to give the created Gateway.
      }),
    );
    console.log("Gateway created successfully.");
    return result;
  } catch (caught) {
    if (caught instanceof Error && caught.name === "IoTSiteWiseError") {
      console.warn(
        `${caught.message}. There was a problem creating the Gateway.`,
      );
    } else {
      throw caught;
    }
  }
};
```

- Para obter detalhes da API, consulte [CreateGateway](#) a Referência AWS SDK para JavaScript da API.

Python

SDK para Python (Boto3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
class IoTSiteWiseWrapper:
    """Encapsulates AWS IoT SiteWise actions using the client interface."""

    def __init__(self, iotsitewise_client: client) -> None:
        """
        Initializes the IoTSiteWiseWrapper with an AWS IoT SiteWise client.

        :param iotsitewise_client: A Boto3 AWS IoT SiteWise client. This client
        provides low-level
                                access to AWS IoT SiteWise services.
        """
        self.iotsitewise_client = iotsitewise_client
        self.entry_id = 0 # Incremented to generate unique entry IDs for
        batch_put_asset_property_value.

    @classmethod
    def from_client(cls) -> "IoTSiteWiseWrapper":
        """
        Creates an IoTSiteWiseWrapper instance with a default AWS IoT SiteWise
        client.

        :return: An instance of IoTSiteWiseWrapper initialized with the default
        AWS IoT SiteWise client.
        """
        iotsitewise_client = boto3.client("iotsitewise")
        return cls(iotsitewise_client)

    def create_gateway(self, gateway_name: str, my_thing: str) -> str:
        """
        Creates an AWS IoT SiteWise Gateway.
```

```

:param gateway_name: The name of the gateway to create.
:param my_thing: The core device thing name.
:return: The ID of the created gateway.
"""
try:
    response = self.iotsitewise_client.create_gateway(
        gatewayName=gateway_name,
        gatewayPlatform={
            "greengrassV2": {"coreDeviceThingName": my_thing},
        },
        tags={"Environment": "Production"},
    )
    gateway_id = response["gatewayId"]
    return gateway_id
except ClientError as err:
    if err.response["Error"]["Code"] == "ResourceAlreadyExistsException":
        logger.error("Gateway %s already exists.", gateway_name)
    else:
        logger.error(
            "Error creating gateway %s. Here's why %s",
            gateway_name,
            err.response["Error"]["Message"],
        )
    raise

```

- Para obter detalhes da API, consulte a [CreateGateway](#) Referência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando esse serviço com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **CreatePortal** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o `CreatePortal`.

CLI

AWS CLI

Para criar um portal

O exemplo `create-portal` a seguir cria um portal da web para uma empresa de parques eólicos. Você pode criar portais somente na mesma região em que habilitou o AWS Single Sign-On.

```
aws iotsitewise create-portal \
  --portal-name WindFarmPortal \
  --portal-description "A portal that contains wind farm projects for Example Corp." \
  --portal-contact-email support@example.com \
  --role-arn arn:aws:iam::123456789012:role/service-role/MySiteWiseMonitorServiceRole
```

Saída:

```
{
  "portalId": "a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE",
  "portalArn": "arn:aws:iotsitewise:us-west-2:123456789012:portal/a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE",
  "portalStartUrl": "https://a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE.app.iotsitewise.aws",
  "portalStatus": {
    "state": "CREATING"
  },
  "ssoApplicationId": "ins-a1b2c3d4-EXAMPLE"
}
```

Para obter mais informações, consulte [Introdução ao AWS IoT SiteWise Monitor no Guia do Usuário de IoT](#) e [Habilitando o AWS SSO](#) no Guia SiteWise do Usuário de IoT.AWS SiteWise

- Para obter detalhes da API, consulte [CreatePortal](#) em Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

 Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
/**
 * Creates a new IoT SiteWise portal.
 *
 * @param portalName the name of the portal to create.
 * @param iamRole the IAM role ARN to use for the portal.
 * @param contactEmail the email address of the portal contact.
 * @return a {@link CompletableFuture} that represents a {@link String}
result of the portal ID. The calling code
 * can attach callbacks, then handle the result or exception by
calling {@link CompletableFuture#join()} or
 * {@link CompletableFuture#get()}.
 *
 * <p>
 * If any completion stage in this method throws an exception, the
method logs the exception cause and keeps
 * it available to the calling code as a {@link CompletionException}.
By calling
 * {@link CompletionException#getCause()}, the calling code can
access the original exception.
 */
public CompletableFuture<String> createPortalAsync(String portalName, String
iamRole, String contactEmail) {
    CreatePortalRequest createPortalRequest = CreatePortalRequest.builder()
        .portalName(portalName)
        .portalDescription("This is my custom IoT SiteWise portal.")
        .portalContactEmail(contactEmail)
        .roleArn(iamRole)
        .build();

    return getAsyncClient().createPortal(createPortalRequest)
        .handle((response, exception) -> {
            if (exception != null) {
```



```

        logger.error("Failed to create portal: {} ",
exception.getCause().getMessage());
        throw (CompletionException) exception;
    }
    return response.portalId();
});
}

```

- Para obter detalhes da API, consulte [CreatePortal](#) na Referência AWS SDK for Java 2.x da API.

JavaScript

SDK para JavaScript (v3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```

import {
    CreatePortalCommand,
    IoTSiteWiseClient,
} from "@aws-sdk/client-iotsitewise";
import { parseArgs } from "node:util";

/**
 * Create a Portal.
 * @param {{ portalName: string, portalContactEmail: string, roleArn: string }}
 */
export const main = async ({ portalName, portalContactEmail, roleArn }) => {
    const client = new IoTSiteWiseClient({});
    try {
        const result = await client.send(
            new CreatePortalCommand({
                portalName: portalName, // The name to give the created Portal.
                portalContactEmail: portalContactEmail, // A valid contact email.
                roleArn: roleArn, // The ARN of a service role that allows the portal's
                users to access the portal's resources.
            })
        );
    } catch (error) {
        console.error(error);
    }
};

```

```

    }},
    );
    console.log("Portal created successfully.");
    return result;
} catch (caught) {
    if (caught instanceof Error && caught.name === "IoTSiteWiseError") {
        console.warn(
            `${caught.message}. There was a problem creating the Portal.`
        );
    } else {
        throw caught;
    }
}
};

```

- Para obter detalhes da API, consulte [CreatePortal](#) na Referência AWS SDK para JavaScript da API.

Python

SDK para Python (Boto3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```

class IoTSiteWiseWrapper:
    """Encapsulates AWS IoT SiteWise actions using the client interface."""

    def __init__(self, iotsitewise_client: client) -> None:
        """
        Initializes the IoTSiteWiseWrapper with an AWS IoT SiteWise client.

        :param iotsitewise_client: A Boto3 AWS IoT SiteWise client. This client
        provides low-level
                                access to AWS IoT SiteWise services.
        """
        self.iotsitewise_client = iotsitewise_client

```

```

        self.entry_id = 0 # Incremented to generate unique entry IDs for
batch_put_asset_property_value.

    @classmethod
    def from_client(cls) -> "IoTSitewiseWrapper":
        """
        Creates an IoTSitewiseWrapper instance with a default AWS IoT SiteWise
client.

        :return: An instance of IoTSitewiseWrapper initialized with the default
AWS IoT SiteWise client.
        """
        iotsitewise_client = boto3.client("iotsitewise")
        return cls(iotsitewise_client)

    def create_portal(
        self, portal_name: str, iam_role_arn: str, portal_contact_email: str
    ) -> str:
        """
        Creates an AWS IoT SiteWise Portal.

        :param portal_name: The name of the portal to create.
        :param iam_role_arn: The ARN of an IAM role.
        :param portal_contact_email: The contact email of the portal.
        :return: The ID of the created portal.
        """
        try:
            response = self.iotsitewise_client.create_portal(
                portalName=portal_name,
                roleArn=iam_role_arn,
                portalContactEmail=portal_contact_email,
            )
            portal_id = response["portalId"]
            waiter = self.iotsitewise_client.get_waiter("portal_active")
            waiter.wait(portalId=portal_id, WaiterConfig={"MaxAttempts": 40})
            return portal_id
        except ClientError as err:
            if err.response["Error"]["Code"] == "ResourceAlreadyExistsException":
                logger.error("Portal %s already exists.", portal_name)
            else:
                logger.error(
                    "Error creating portal %s. Here's why %s",
                    portal_name,

```

```
err.response["Error"]["Message"],
    )
    raise
```

- Para obter detalhes da API, consulte a [CreatePortal](#) Referência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando esse serviço com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **DeleteAsset** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o DeleteAsset.

CLI

AWS CLI

Para excluir um ativo

O exemplo delete-asset a seguir exclui um modelo de ativo de turbina eólica.

```
aws iotsitewise delete-asset \
  --asset-id a1b2c3d4-5678-90ab-cdef-3333EXAMPLE
```

Saída:

```
{
  "assetStatus": {
    "state": "DELETING"
  }
}
```

Para obter mais informações, consulte [Excluindo ativos no Guia](#) do Usuário de AWS SiteWise IoT.

- Para obter detalhes da API, consulte [DeleteAsset](#) em Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

 Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
/**
 * Deletes an asset.
 *
 * @param assetId the ID of the asset to be deleted.
 * @return a {@link CompletableFuture} that represents a {@link
DeleteAssetResponse} result. The calling code can
 *         attach callbacks, then handle the result or exception by calling
{@link CompletableFuture#join()} or
 *         {@link CompletableFuture#get()}.
 *         <p>
 *         If any completion stage in this method throws an exception, the
method logs the exception cause and keeps
 *         it available to the calling code as a {@link CompletionException}.
By calling
 *         {@link CompletionException#getCause()}, the calling code can
access the original exception.
 */
public CompletableFuture<DeleteAssetResponse> deleteAssetAsync(String
assetId) {
    DeleteAssetRequest deleteAssetRequest = DeleteAssetRequest.builder()
        .assetId(assetId)
        .build();

    return getAsyncClient().deleteAsset(deleteAssetRequest)
        .whenComplete((response, exception) -> {
            if (exception != null) {
                logger.error("An error occurred deleting asset with id: {}",
assetId);
            }
        });
}
```

- Para obter detalhes da API, consulte [DeleteAsseta](#) Referência AWS SDK for Java 2.x da API.

JavaScript

SDK para JavaScript (v3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
import {
  DeleteAssetCommand,
  IoTSiteWiseClient,
} from "@aws-sdk/client-iotsitewise";
import { parseArgs } from "node:util";

/**
 * Delete an asset.
 * @param {{ assetId : string }}
 */
export const main = async ({ assetId }) => {
  const client = new IoTSiteWiseClient({});
  try {
    await client.send(
      new DeleteAssetCommand({
        assetId: assetId, // The model id to delete.
      }),
    );
    console.log("Asset deleted successfully.");
    return { assetDeleted: true };
  } catch (caught) {
    if (caught instanceof Error && caught.name === "ResourceNotFound") {
      console.warn(
        `${caught.message}. There was a problem deleting the asset.`,
      );
    } else {
      throw caught;
    }
  }
}
```

```
}
};
```

- Para obter detalhes da API, consulte [DeleteAsseta](#) Referência AWS SDK para JavaScript da API.

Python

SDK para Python (Boto3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
class IoTSitewiseWrapper:
    """Encapsulates AWS IoT SiteWise actions using the client interface."""

    def __init__(self, iotsitewise_client: client) -> None:
        """
        Initializes the IoTSitewiseWrapper with an AWS IoT SiteWise client.

        :param iotsitewise_client: A Boto3 AWS IoT SiteWise client. This client
        provides low-level
            access to AWS IoT SiteWise services.
        """
        self.iotsitewise_client = iotsitewise_client
        self.entry_id = 0 # Incremented to generate unique entry IDs for
        batch_put_asset_property_value.

    @classmethod
    def from_client(cls) -> "IoTSitewiseWrapper":
        """
        Creates an IoTSitewiseWrapper instance with a default AWS IoT SiteWise
        client.

        :return: An instance of IoTSitewiseWrapper initialized with the default
        AWS IoT SiteWise client.
        """
```

```

iotsitewise_client = boto3.client("iotsitewise")
return cls(iotsitewise_client)

def delete_asset(self, asset_id: str) -> None:
    """
    Deletes an AWS IoT SiteWise Asset.

    :param asset_id: The ID of the asset to delete.
    """
    try:
        self.iotsitewise_client.delete_asset(assetId=asset_id)
    except ClientError as err:
        logger.error(
            "Error deleting asset %s. Here's why %s",
            asset_id,
            err.response["Error"]["Message"],
        )
        raise

```

- Para obter detalhes da API, consulte a [DeleteAsset](#) Referência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando esse serviço com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **DeleteAssetModel** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o `DeleteAssetModel`.

CLI

AWS CLI

Para excluir um modelo de ativo

O exemplo `delete-asset-model` a seguir exclui um modelo de ativo de turbina eólica.

```
aws iotsitewise delete-asset-model \
```



```
--asset-model-id a1b2c3d4-5678-90ab-cdef-11111EXAMPLE
```

Saída:

```
{
  "assetModelStatus": {
    "state": "DELETING"
  }
}
```

Para obter mais informações, consulte [Excluindo modelos de ativos](#) no Guia do usuário de AWS SiteWise IoT.

- Para obter detalhes da API, consulte [DeleteAssetModel](#) em Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
/**
 * Deletes an Asset Model with the specified ID.
 *
 * @param assetModelId the ID of the Asset Model to delete.
 * @return a {@link CompletableFuture} that represents a {@link
DeleteAssetModelResponse} result. The calling code
 *       can attach callbacks, then handle the result or exception by
calling {@link CompletableFuture#join()} or
 *       {@link CompletableFuture#get()}.
 *       <p>
 *       If any completion stage in this method throws an exception, the
method logs the exception cause and keeps
 *       it available to the calling code as a {@link CompletionException}.
By calling
```

```

    *      {@link CompletionException#getCause()}, the calling code can
    access the original exception.
    */
    public CompletableFuture<DeleteAssetModelResponse>
deleteAssetModelAsync(String assetModelId) {
        DeleteAssetModelRequest deleteAssetModelRequest =
DeleteAssetModelRequest.builder()
            .assetModelId(assetModelId)
            .build();

        return getAsyncClient().deleteAssetModel(deleteAssetModelRequest)
            .whenComplete((response, exception) -> {
                if (exception != null) {
                    logger.error("Failed to delete asset model with ID:{}.\"",
exception.getMessage());
                }
            });
    }
}

```

- Para obter detalhes da API, consulte [DeleteAssetModel](#) na Referência AWS SDK for Java 2.x da API.

JavaScript

SDK para JavaScript (v3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```

import {
    DeleteAssetModelCommand,
    IoTSiteWiseClient,
} from "@aws-sdk/client-iotsitewise";
import { parseArgs } from "node:util";

/**
 * Delete an asset model.

```

```

* @param {{ assetModelId : string }}
*/
export const main = async ({ assetModelId }) => {
  const client = new IoTSiteWiseClient({});
  try {
    await client.send(
      new DeleteAssetModelCommand({
        assetModelId: assetModelId, // The model id to delete.
      }),
    );
    console.log("Asset model deleted successfully.");
    return { assetModelDeleted: true };
  } catch (caught) {
    if (caught instanceof Error && caught.name === "ResourceNotFound") {
      console.warn(
        `${caught.message}. There was a problem deleting the asset model.`
      );
    } else {
      throw caught;
    }
  }
};

```

- Para obter detalhes da API, consulte [DeleteAssetModel](#) na Referência AWS SDK para JavaScript da API.

Python

SDK para Python (Boto3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```

class IoTSiteWiseWrapper:
    """Encapsulates AWS IoT SiteWise actions using the client interface."""

    def __init__(self, iotsitewise_client: client) -> None:

```

```

    """
    Initializes the IoTSiteWiseWrapper with an AWS IoT SiteWise client.

    :param iotsitewise_client: A Boto3 AWS IoT SiteWise client. This client
    provides low-level
                                access to AWS IoT SiteWise services.
    """
    self.iotsitewise_client = iotsitewise_client
    self.entry_id = 0 # Incremented to generate unique entry IDs for
    batch_put_asset_property_value.

    @classmethod
    def from_client(cls) -> "IoTSiteWiseWrapper":
        """
        Creates an IoTSiteWiseWrapper instance with a default AWS IoT SiteWise
        client.

        :return: An instance of IoTSiteWiseWrapper initialized with the default
        AWS IoT SiteWise client.
        """
        iotsitewise_client = boto3.client("iotsitewise")
        return cls(iotsitewise_client)

    def delete_asset_model(self, asset_model_id: str) -> None:
        """
        Deletes an AWS IoT SiteWise Asset Model.

        :param asset_model_id: The ID of the asset model to delete.
        """
        try:
            self.iotsitewise_client.delete_asset_model(assetModelId=asset_model_id)
        except ClientError as err:
            logger.error(
                "Error deleting asset model %s. Here's why %s",
                asset_model_id,
                err.response["Error"]["Message"],
            )
            raise

```

- Para obter detalhes da API, consulte a [DeleteAssetModel](#) Referência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando esse serviço com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **DeleteGateway** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o DeleteGateway.

CLI

AWS CLI

Para excluir um gateway

O exemplo delete-gateway a seguir exclui um gateway.

```
aws iotsitewise delete-gateway \  
  --gateway-id a1b2c3d4-5678-90ab-cdef-1a1a1EXAMPLE
```

Este comando não produz saída.

Para obter mais informações, consulte Como [ingerir dados usando um gateway no Guia](#) do usuário de AWS SiteWise IoT.

- Para obter detalhes da API, consulte [DeleteGateway](#) em Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```

/**
 * Deletes the specified gateway.
 *
 * @param gatewayId the ID of the gateway to delete.
 * @return a {@link CompletableFuture} that represents a {@link
DeleteGatewayResponse} result.. The calling code
 *         can attach callbacks, then handle the result or exception by
calling {@link CompletableFuture#join()} or
 *         {@link CompletableFuture#get()}.
 *         <p>
 *         If any completion stage in this method throws an exception, the
method logs the exception cause and keeps
 *         it available to the calling code as a {@link CompletionException}.
By calling
 *         {@link CompletionException#getCause()}, the calling code can
access the original exception.
 */
public CompletableFuture<DeleteGatewayResponse> deleteGatewayAsync(String
gatewayId) {
    DeleteGatewayRequest deleteGatewayRequest =
DeleteGatewayRequest.builder()
        .gatewayId(gatewayId)
        .build();

    return getAsyncClient().deleteGateway(deleteGatewayRequest)
        .whenComplete((response, exception) -> {
            if (exception != null) {
                logger.error("Failed to delete gateway: {}",
exception.getCause().getMessage());
            }
        });
}

```

- Para obter detalhes da API, consulte [DeleteGateway](#) a Referência AWS SDK for Java 2.x da API.

JavaScript

SDK para JavaScript (v3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
import {
  DeleteGatewayCommand,
  IoTSiteWiseClient,
} from "@aws-sdk/client-iotsitewise";
import { parseArgs } from "node:util";

/**
 * Create an SSM document.
 * @param {{ content: string, name: string, documentType?: DocumentType }}
 */
export const main = async ({ gatewayId }) => {
  const client = new IoTSiteWiseClient({});
  try {
    await client.send(
      new DeleteGatewayCommand({
        gatewayId: gatewayId, // The ID of the Gateway to describe.
      }),
    );
    console.log("Gateway deleted successfully.");
    return { gatewayDeleted: true };
  } catch (caught) {
    if (caught instanceof Error && caught.name === "ResourceNotFound") {
      console.warn(
        `${caught.message}. The Gateway could not be found. Please check the Gateway Id.`,
      );
    } else {
      throw caught;
    }
  }
};
```

- Para obter detalhes da API, consulte [DeleteGateway](#) a Referência AWS SDK para JavaScript da API.

Python

SDK para Python (Boto3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
class IoTSiteWiseWrapper:
    """Encapsulates AWS IoT SiteWise actions using the client interface."""

    def __init__(self, iotsitewise_client: client) -> None:
        """
        Initializes the IoTSiteWiseWrapper with an AWS IoT SiteWise client.

        :param iotsitewise_client: A Boto3 AWS IoT SiteWise client. This client
        provides low-level
            access to AWS IoT SiteWise services.
        """
        self.iotsitewise_client = iotsitewise_client
        self.entry_id = 0 # Incremented to generate unique entry IDs for
        batch_put_asset_property_value.

    @classmethod
    def from_client(cls) -> "IoTSiteWiseWrapper":
        """
        Creates an IoTSiteWiseWrapper instance with a default AWS IoT SiteWise
        client.

        :return: An instance of IoTSiteWiseWrapper initialized with the default
        AWS IoT SiteWise client.
        """
        iotsitewise_client = boto3.client("iotsitewise")
        return cls(iotsitewise_client)
```



```
def delete_gateway(self, gateway_id: str) -> None:
    """
    Deletes an AWS IoT SiteWise Gateway.

    :param gateway_id: The ID of the gateway to delete.
    """
    try:
        self.iotsitewise_client.delete_gateway(gatewayId=gateway_id)
    except ClientError as err:
        if err.response["Error"]["Code"] == "ResourceNotFoundException":
            logger.error("Gateway %s does not exist.", gateway_id)
        else:
            logger.error(
                "Error deleting gateway %s. Here's why %s",
                gateway_id,
                err.response["Error"]["Message"],
            )
        raise
```

- Para obter detalhes da API, consulte a [DeleteGateway](#) Referência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando esse serviço com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **DeletePortal** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o DeletePortal.

CLI

AWS CLI

Para excluir um portal

O exemplo delete-portal a seguir exclui um portal da web para uma empresa de parques eólicos.

```
aws iotsitewise delete-portal \
```

```
--portal-id a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE
```

Saída:

```
{
  "portalStatus": {
    "state": "DELETING"
  }
}
```

Para obter mais informações, consulte [Excluindo um portal no Guia](#) do Usuário de AWS SiteWise IoT.

- Para obter detalhes da API, consulte [DeletePortal](#) em Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
/**
 * Deletes a portal.
 *
 * @param portalId the ID of the portal to be deleted.
 * @return a {@link CompletableFuture} that represents a {@link
DeletePortalResponse}. The calling code can attach
 *         callbacks, then handle the result or exception by calling {@link
CompletableFuture#join()} or
 *         {@link CompletableFuture#get()}.
 *         <p>
 *         If any completion stage in this method throws an exception, the
method logs the exception cause and keeps
 *         it available to the calling code as a {@link CompletionException}.
By calling
 *         {@link CompletionException#getCause()}, the calling code can
access the original exception.
```

```

    */
    public CompletableFuture<DeletePortalResponse> deletePortalAsync(String
portalId) {
        DeletePortalRequest deletePortalRequest = DeletePortalRequest.builder()
            .portalId(portalId)
            .build();

        return getAsyncClient().deletePortal(deletePortalRequest)
            .whenComplete((response, exception) -> {
                if (exception != null) {
                    logger.error("Failed to delete portal with ID: {}. Error:
{}", portalId, exception.getCause().getMessage());
                }
            });
    }
}

```

- Para obter detalhes da API, consulte [DeletePortal](#) a Referência AWS SDK for Java 2.x da API.

JavaScript

SDK para JavaScript (v3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```

import {
    DeletePortalCommand,
    IoTSiteWiseClient,
} from "@aws-sdk/client-iotsitewise";
import { parseArgs } from "node:util";

/**
 * List asset models.
 * @param {{ portalId : string }}
 */
export const main = async ({ portalId }) => {

```

```
const client = new IoTSiteWiseClient({});
try {
  await client.send(
    new DeletePortalCommand({
      portalId: portalId, // The id of the portal.
    }),
  );
  console.log("Portal deleted successfully.");
  return { portalDeleted: true };
} catch (caught) {
  if (caught instanceof Error && caught.name === "ResourceNotFound") {
    console.warn(
      `${caught.message}. There was a problem deleting the portal. Please check the portal id.`,
    );
  } else {
    throw caught;
  }
}
};
```

- Para obter detalhes da API, consulte [DeletePortal](#) a Referência AWS SDK para JavaScript da API.

Python

SDK para Python (Boto3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
class IoTSiteWiseWrapper:
    """Encapsulates AWS IoT SiteWise actions using the client interface."""

    def __init__(self, iotsitewise_client: client) -> None:
        """
        Initializes the IoTSiteWiseWrapper with an AWS IoT SiteWise client.
```

```

        :param iotsitewise_client: A Boto3 AWS IoT SiteWise client. This client
        provides low-level
            access to AWS IoT SiteWise services.
        """
        self.iotsitewise_client = iotsitewise_client
        self.entry_id = 0 # Incremented to generate unique entry IDs for
        batch_put_asset_property_value.

    @classmethod
    def from_client(cls) -> "IoTSitewiseWrapper":
        """
        Creates an IoTSitewiseWrapper instance with a default AWS IoT SiteWise
        client.

        :return: An instance of IoTSitewiseWrapper initialized with the default
        AWS IoT SiteWise client.
        """
        iotsitewise_client = boto3.client("iotsitewise")
        return cls(iotsitewise_client)

    def delete_portal(self, portal_id: str) -> None:
        """
        Deletes an AWS IoT SiteWise Portal.

        :param portal_id: The ID of the portal to delete.
        """
        try:
            self.iotsitewise_client.delete_portal(portalId=portal_id)
        except ClientError as err:
            if err.response["Error"]["Code"] == "ResourceNotFoundException":
                logger.error("Portal %s does not exist.", portal_id)
            else:
                logger.error(
                    "Error deleting portal %s. Here's why %s",
                    portal_id,
                    err.response["Error"]["Message"],
                )
            raise

```

- Para obter detalhes da API, consulte a [DeletePortal](#)Referência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando esse serviço com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **DescribeAssetModel** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o `DescribeAssetModel`.

CLI

AWS CLI

Para descrever um modelo de ativo

O exemplo `describe-asset-model` a seguir descreve um modelo de ativo de parque eólico.

```
aws iotsitewise describe-asset-model \  
  --asset-model-id a1b2c3d4-5678-90ab-cdef-2222EXAMPLE
```

Saída:

```
{  
  "assetModelId": "a1b2c3d4-5678-90ab-cdef-2222EXAMPLE",  
  "assetModelArn": "arn:aws:iotsitewise:us-west-2:123456789012:asset-model/  
a1b2c3d4-5678-90ab-cdef-2222EXAMPLE",  
  "assetModelName": "Wind Farm Model",  
  "assetModelDescription": "Represents a wind farm that comprises many wind  
turbines",  
  "assetModelProperties": [  
    {  
      "id": "a1b2c3d4-5678-90ab-cdef-99999EXAMPLE",  
      "name": "Total Generated Power",  
      "dataType": "DOUBLE",  
      "unit": "kW",  
      "type": {  
        "metric": {  
          "expression": "sum(power)",  
          "variables": [  

```

```

        {
            "name": "power",
            "value": {
                "propertyId": "a1b2c3d4-5678-90ab-
cdef-66666EXAMPLE",
                "hierarchyId": "a1b2c3d4-5678-90ab-
cdef-77777EXAMPLE"
            }
        }
    ],
    "window": {
        "tumbling": {
            "interval": "1h"
        }
    }
}
},
{
    "id": "a1b2c3d4-5678-90ab-cdef-88888EXAMPLE",
    "name": "Region",
    "dataType": "STRING",
    "type": {
        "attribute": {
            "defaultValue": " "
        }
    }
}
],
"assetModelHierarchies": [
    {
        "id": "a1b2c3d4-5678-90ab-cdef-77777EXAMPLE",
        "name": "Wind Turbines",
        "childAssetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE"
    }
],
"assetModelCreationDate": 1575671284.0,
"assetModelLastUpdateDate": 1575671988.0,
"assetModelStatus": {
    "state": "ACTIVE"
}
}

```

Para obter mais informações, consulte [Descrição de um modelo de ativo específico](#) no Guia do SiteWise usuário de AWS IoT.

- Para obter detalhes da API, consulte [DescribeAssetModel](#) em Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
/**
 * Retrieves the property IDs associated with a specific asset model.
 *
 * @param assetModelId the ID of the asset model that defines the properties.
 * @return a {@link CompletableFuture} that represents a {@link Map} result
 * that associates the property name to the
 *         property ID. The calling code can attach callbacks, then handle the
 * result or exception by calling
 *         {@link CompletableFuture#join()} or {@link
 * CompletableFuture#get()}.
 *
 * <p>
 *         If any completion stage in this method throws an exception, the
 * method logs the exception cause and keeps
 *         it available to the calling code as a {@link CompletionException}.
 * By calling
 *         {@link CompletionException#getCause()}, the calling code can
 * access the original exception.
 */
public CompletableFuture<Map<String, String>> getPropertyIds(String
assetModelId) {
    ListAssetModelPropertiesRequest modelPropertiesRequest =
ListAssetModelPropertiesRequest.builder().assetModelId(assetModelId).build();
    return getAsyncClient().listAssetModelProperties(modelPropertiesRequest)
        .handle((response, throwable) -> {
            if (response != null) {
                return response.assetModelPropertySummaries().stream()
```



```

        .collect(Collectors
            .toMap(AssetModelPropertySummary::name,
                AssetModelPropertySummary::id));
    } else {
        logger.error("Error occurred while fetching property IDs:
        {}. ", throwable.getCause().getMessage());
        throw (CompletionException) throwable;
    }
    });
}

```

- Para obter detalhes da API, consulte [DescribeAssetModel](#) na Referência AWS SDK for Java 2.x da API.

JavaScript

SDK para JavaScript (v3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```

import {
    DescribeAssetModelCommand,
    IoTSiteWiseClient,
} from "@aws-sdk/client-iotsitewise";
import { parseArgs } from "node:util";

/**
 * Describe an asset model.
 * @param {{ assetModelId : string }}
 */
export const main = async ({ assetModelId }) => {
    const client = new IoTSiteWiseClient({});
    try {
        const { assetModelDescription } = await client.send(
            new DescribeAssetModelCommand({
                assetModelId: assetModelId, // The ID of the Gateway to describe.
            })
        );
    } catch (error) {
        console.error(error);
    }
};

```

```

    }},
  );
  console.log("Asset model information retrieved successfully.");
  return { assetModelDescription: assetModelDescription };
} catch (caught) {
  if (caught instanceof Error && caught.name === "ResourceNotFound") {
    console.warn(
      `${caught.message}. The asset model could not be found. Please check the
asset model id.`
    );
  } else {
    throw caught;
  }
}
};

```

- Para obter detalhes da API, consulte [DescribeAssetModel](#) na Referência AWS SDK para JavaScript da API.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando esse serviço com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **DescribeGateway** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o `DescribeGateway`.

CLI

AWS CLI

Para descrever um gateway

O exemplo `describe-gateway` a seguir descreve um gateway.

```

aws iotsitewise describe-gateway \
  --gateway-id a1b2c3d4-5678-90ab-cdef-1a1a1EXAMPLE

```

Saída:

```
{
```

```

    "gatewayId": "a1b2c3d4-5678-90ab-cdef-1a1a1EXAMPLE",
    "gatewayName": "ExampleCorpGateway",
    "gatewayArn": "arn:aws:iotsitewise:us-west-2:123456789012:gateway/a1b2c3d4-5678-90ab-cdef-1a1a1EXAMPLE",
    "gatewayPlatform": {
      "greengrass": {
        "groupArn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/groups/a1b2c3d4-5678-90ab-cdef-1b1b1EXAMPLE"
      }
    },
    "gatewayCapabilitySummaries": [
      {
        "capabilityNamespace": "iotsitewise:opcuacollector:1",
        "capabilitySyncStatus": "IN_SYNC"
      }
    ],
    "creationDate": 1588369971.457,
    "lastUpdateDate": 1588369971.457
  }

```

Para obter mais informações, consulte Como [ingerir dados usando um gateway no Guia](#) do usuário de AWS SiteWise IoT.

- Para obter detalhes da API, consulte [DescribeGateway](#) em Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```

/**
 * Describes the specified gateway.
 *
 * @param gatewayId the ID of the gateway to describe.
 * @return a {@link CompletableFuture} that represents a {@link
 * DescribeGatewayResponse} result. The calling code

```

```

    *      can attach callbacks, then handle the result or exception by
    calling {@link CompletableFuture#join()} or
    *      {@link CompletableFuture#get()}.
    *      <p>
    *      If any completion stage in this method throws an exception, the
    method logs the exception cause and keeps
    *      it available to the calling code as a {@link CompletionException}.
    By calling
    *      {@link CompletionException#getCause()}, the calling code can
    access the original exception.
    */
    public CompletableFuture<DescribeGatewayResponse> describeGatewayAsync(String
gatewayId) {
        DescribeGatewayRequest request = DescribeGatewayRequest.builder()
            .gatewayId(gatewayId)
            .build();

        return getAsyncClient().describeGateway(request)
            .whenComplete((response, exception) -> {
                if (exception != null) {
                    logger.error("An error occurred during the describeGateway
method: {}", exception.getCause().getMessage());
                }
            });
    }
}

```

- Para obter detalhes da API, consulte [DescribeGateway](#) a Referência AWS SDK for Java 2.x da API.

JavaScript

SDK para JavaScript (v3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
import {
```

```
DescribeGatewayCommand,  
IoTSiteWiseClient,  
} from "@aws-sdk/client-iotsitewise";  
import { parseArgs } from "node:util";  
  
/**  
 * Create an SSM document.  
 * @param {{ content: string, name: string, documentType?: DocumentType }}  
 */  
export const main = async ({ gatewayId }) => {  
  const client = new IoTSiteWiseClient({});  
  try {  
    const { gatewayDescription } = await client.send(  
      new DescribeGatewayCommand({  
        gatewayId: gatewayId, // The ID of the Gateway to describe.  
      })),  
    );  
    console.log("Gateway information retrieved successfully.");  
    return { gatewayDescription: gatewayDescription };  
  } catch (caught) {  
    if (caught instanceof Error && caught.name === "ResourceNotFound") {  
      console.warn(  
        `${caught.message}. The Gateway could not be found. Please check the  
Gateway Id.`,  
      );  
    } else {  
      throw caught;  
    }  
  }  
};
```

- Para obter detalhes da API, consulte [DescribeGateway](#) a Referência AWS SDK para JavaScript da API.

Python

SDK para Python (Boto3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
class IoTSitewiseWrapper:
    """Encapsulates AWS IoT SiteWise actions using the client interface."""

    def __init__(self, iotsitewise_client: client) -> None:
        """
        Initializes the IoTSitewiseWrapper with an AWS IoT SiteWise client.

        :param iotsitewise_client: A Boto3 AWS IoT SiteWise client. This client
        provides low-level
                                access to AWS IoT SiteWise services.
        """
        self.iotsitewise_client = iotsitewise_client
        self.entry_id = 0 # Incremented to generate unique entry IDs for
        batch_put_asset_property_value.

    @classmethod
    def from_client(cls) -> "IoTSitewiseWrapper":
        """
        Creates an IoTSitewiseWrapper instance with a default AWS IoT SiteWise
        client.

        :return: An instance of IoTSitewiseWrapper initialized with the default
        AWS IoT SiteWise client.
        """
        iotsitewise_client = boto3.client("iotsitewise")
        return cls(iotsitewise_client)

    def describe_gateway(self, gateway_id: str) -> Dict[str, Any]:
        """
        Describes an AWS IoT SiteWise Gateway.
```

```

:param gateway_id: The ID of the gateway to describe.
:return: A dictionary containing information about the gateway.
"""
try:
    response =
self.iotsitewise_client.describe_gateway(gatewayId=gateway_id)
    return response
except ClientError as err:
    if err.response["Error"]["Code"] == "ResourceNotFoundException":
        logger.error("Gateway %s does not exist.", gateway_id)
    else:
        logger.error(
            "Error describing gateway %s. Here's why %s",
            gateway_id,
            err.response["Error"]["Message"],
        )
    raise

```

- Para obter detalhes da API, consulte a [DescribeGateway](#) Referência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando esse serviço com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **DescribePortal** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o `DescribePortal`.

CLI

AWS CLI

Para descrever um portal

O exemplo `describe-portal` a seguir descreve um portal da web para uma empresa de parques eólicos.

```

aws iotsitewise describe-portal \
  --portal-id a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE

```

Saída:

```
{
  "portalId": "a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE",
  "portalArn": "arn:aws:iotsitewise:us-west-2:123456789012:portal/a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE",
  "portalName": "WindFarmPortal",
  "portalDescription": "A portal that contains wind farm projects for Example Corp.",
  "portalClientId": "E-a1b2c3d4e5f6_a1b2c3d4e5f6EXAMPLE",
  "portalStartUrl": "https://a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE.app.iotsitewise.aws",
  "portalContactEmail": "support@example.com",
  "portalStatus": {
    "state": "ACTIVE"
  },
  "portalCreationDate": "2020-02-04T23:01:52.90248068Z",
  "portalLastUpdateDate": "2020-02-04T23:01:52.90248078Z",
  "roleArn": "arn:aws:iam::123456789012:role/MySiteWiseMonitorServiceRole"
}
```

Para obter mais informações, consulte [Administrando seus portais no Guia](#) do Usuário de AWS SiteWise IoT.

- Para obter detalhes da API, consulte [DescribePortal](#) em Referência de AWS CLI Comandos.

Java**SDK para Java 2.x**** Note**

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
/**
 * Retrieves a portal's description.
 *
 * @param portalId the ID of the portal to describe.
 * @return a {@link CompletableFuture} that represents a {@link String}
 * result of the portal's start URL
```



```

    *      (see: {@link DescribePortalResponse#portalStartUrl()}). The
    calling code can attach callbacks, then handle the
    *      result or exception by calling {@link CompletableFuture#join()} or
    {@link CompletableFuture#get()}.
    *      <p>
    *      If any completion stage in this method throws an exception, the
    method logs the exception cause and keeps
    *      it available to the calling code as a {@link CompletionException}.
    By calling
    *      {@link CompletionException#getCause()}, the calling code can
    access the original exception.
    */
    public CompletableFuture<String> describePortalAsync(String portalId) {
        DescribePortalRequest request = DescribePortalRequest.builder()
            .portalId(portalId)
            .build();

        return getAsyncClient().describePortal(request)
            .handle((response, exception) -> {
                if (exception != null) {
                    logger.error("An exception occurred retrieving the portal
description: {}", exception.getCause().getMessage());
                    throw (CompletionException) exception;
                }
                return response.portalStartUrl();
            });
    }

```

- Para obter detalhes da API, consulte [DescribePortal](#) a Referência AWS SDK for Java 2.x da API.

JavaScript

SDK para JavaScript (v3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
import {
  DescribePortalCommand,
  IoTSiteWiseClient,
} from "@aws-sdk/client-iotsitewise";
import { parseArgs } from "node:util";

/**
 * Describe a portal.
 * @param {{ portalId: string }}
 */
export const main = async ({ portalId }) => {
  const client = new IoTSiteWiseClient({});
  try {
    const result = await client.send(
      new DescribePortalCommand({
        portalId: portalId, // The ID of the Gateway to describe.
      }),
    );
    console.log("Portal information retrieved successfully.");
    return result;
  } catch (caught) {
    if (caught instanceof Error && caught.name === "ResourceNotFound") {
      console.warn(
        `${caught.message}. The Portal could not be found. Please check the Portal Id.`
      );
    } else {
      throw caught;
    }
  }
};
```

- Para obter detalhes da API, consulte [DescribePortal](#) a Referência AWS SDK para JavaScript da API.

Python

SDK para Python (Boto3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
class IoTSiteWiseWrapper:
    """Encapsulates AWS IoT SiteWise actions using the client interface."""

    def __init__(self, iotsitewise_client: client) -> None:
        """
        Initializes the IoTSiteWiseWrapper with an AWS IoT SiteWise client.

        :param iotsitewise_client: A Boto3 AWS IoT SiteWise client. This client
        provides low-level
                                access to AWS IoT SiteWise services.
        """
        self.iotsitewise_client = iotsitewise_client
        self.entry_id = 0 # Incremented to generate unique entry IDs for
        batch_put_asset_property_value.

    @classmethod
    def from_client(cls) -> "IoTSiteWiseWrapper":
        """
        Creates an IoTSiteWiseWrapper instance with a default AWS IoT SiteWise
        client.

        :return: An instance of IoTSiteWiseWrapper initialized with the default
        AWS IoT SiteWise client.
        """
        iotsitewise_client = boto3.client("iotsitewise")
        return cls(iotsitewise_client)

    def create_gateway(self, gateway_name: str, my_thing: str) -> str:
        """
        Creates an AWS IoT SiteWise Gateway.
```

```
:param gateway_name: The name of the gateway to create.
:param my_thing: The core device thing name.
:return: The ID of the created gateway.
"""
try:
    response = self.iotsitewise_client.create_gateway(
        gatewayName=gateway_name,
        gatewayPlatform={
            "greengrassV2": {"coreDeviceThingName": my_thing},
        },
        tags={"Environment": "Production"},
    )
    gateway_id = response["gatewayId"]
    return gateway_id
except ClientError as err:
    if err.response["Error"]["Code"] == "ResourceAlreadyExistsException":
        logger.error("Gateway %s already exists.", gateway_name)
    else:
        logger.error(
            "Error creating gateway %s. Here's why %s",
            gateway_name,
            err.response["Error"]["Message"],
        )
    raise
```

- Para obter detalhes da API, consulte a [DescribePortal](#) Referência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando esse serviço com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **GetAssetPropertyValue** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o `GetAssetPropertyValue`.

CLI

AWS CLI

Para recuperar o valor atual de uma propriedade do ativo

O exemplo `get-asset-property-value` a seguir recupera a potência total atual de um ativo de turbina eólica.

```
aws iotsitewise get-asset-property-value \  
  --asset-id a1b2c3d4-5678-90ab-cdef-33333EXAMPLE \  
  --property-id a1b2c3d4-5678-90ab-cdef-66666EXAMPLE
```

Saída:

```
{  
  "propertyValue": {  
    "value": {  
      "doubleValue": 6890.8677520453875  
    },  
    "timestamp": {  
      "timeInSeconds": 1580853000,  
      "offsetInNanos": 0  
    },  
    "quality": "GOOD"  
  }  
}
```

Para obter mais informações, consulte [Consultar os valores atuais das propriedades do ativo](#) no Guia do Usuário de AWS SiteWise IoT.

- Para obter detalhes da API, consulte [GetAssetPropertyValue](#) em Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
/**
 * Fetches the value of an asset property.
 *
 * @param propId the ID of the asset property to fetch.
 * @param assetId the ID of the asset to fetch the property value for.
 * @return a {@link CompletableFuture} that represents a {@link Double}
 * result. The calling code can attach
 *     callbacks, then handle the result or exception by calling {@link
 * CompletableFuture#join()} or
 *     {@link CompletableFuture#get()}.
 *     <p>
 *     If any completion stage in this method throws an exception, the
 * method logs the exception cause and keeps
 *     it available to the calling code as a {@link CompletionException}.
 * By calling
 *     {@link CompletionException#getCause()}, the calling code can
 * access the original exception.
 */
public CompletableFuture<Double> getAssetPropValueAsync(String propId, String
assetId) {
    GetAssetPropertyValueRequest assetPropertyValueRequest =
    GetAssetPropertyValueRequest.builder()
        .propertyId(propId)
        .assetId(assetId)
        .build();

    return getAsyncClient().getAssetPropertyValue(assetPropertyValueRequest)
        .handle((response, exception) -> {
            if (exception != null) {
                logger.error("Error occurred while fetching property
value: {}.", exception.getCause().getMessage());
                throw (CompletionException) exception;
            }
        });
}
```

```

        }
        return response.propertyValue().value().doubleValue();
    });
}

```

- Para obter detalhes da API, consulte [GetAssetPropertyValue](#) a Referência AWS SDK for Java 2.x da API.

JavaScript

SDK para JavaScript (v3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```

import {
    GetAssetPropertyValueCommand,
    IoTSiteWiseClient,
} from "@aws-sdk/client-iotsitewise";
import { parseArgs } from "node:util";

/**
 * Describe an asset property value.
 * @param {{ entryId : string }}
 */
export const main = async ({ entryId }) => {
    const client = new IoTSiteWiseClient({});
    try {
        const result = await client.send(
            new GetAssetPropertyValueCommand({
                entryId: entryId, // The ID of the Gateway to describe.
            }),
        );
        console.log("Asset property information retrieved successfully.");
        return result;
    } catch (caught) {
        if (caught instanceof Error && caught.name === "ResourceNotFound") {

```

```

        console.warn(
            `${caught.message}. The asset property entry could not be found. Please
            check the entry id.` ,
        );
    } else {
        throw caught;
    }
}
};

```

- Para obter detalhes da API, consulte [GetAssetPropertyValue](#) a Referência AWS SDK para JavaScript da API.

Python

SDK para Python (Boto3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```

class IoTSiteWiseWrapper:
    """Encapsulates AWS IoT SiteWise actions using the client interface."""

    def __init__(self, iotsitewise_client: client) -> None:
        """
        Initializes the IoTSiteWiseWrapper with an AWS IoT SiteWise client.

        :param iotsitewise_client: A Boto3 AWS IoT SiteWise client. This client
        provides low-level
                                access to AWS IoT SiteWise services.
        """
        self.iotsitewise_client = iotsitewise_client
        self.entry_id = 0 # Incremented to generate unique entry IDs for
        batch_put_asset_property_value.

    @classmethod
    def from_client(cls) -> "IoTSiteWiseWrapper":

```



```

        """
        Creates an IoTSiteWiseWrapper instance with a default AWS IoT SiteWise
        client.

        :return: An instance of IoTSiteWiseWrapper initialized with the default
        AWS IoT SiteWise client.
        """
        iotsitewise_client = boto3.client("iotsitewise")
        return cls(iotsitewise_client)

def get_asset_property_value(
    self, asset_id: str, property_id: str
) -> Dict[str, Any]:
    """
    Gets the value of an AWS IoT SiteWise Asset Property.

    :param asset_id: The ID of the asset.
    :param property_id: The ID of the property.
    :return: A dictionary containing the value of the property.
    """
    try:
        response = self.iotsitewise_client.get_asset_property_value(
            assetId=asset_id, propertyId=property_id
        )
        return response["propertyValue"]
    except ClientError as err:
        if err.response["Error"]["Code"] == "ResourceNotFoundException":
            logger.error(
                "Asset %s or property %s does not exist.", asset_id,
property_id
            )
        else:
            logger.error(
                "Error getting asset property value. Here's why %s",
                err.response["Error"]["Message"],
            )
        raise

```

- Para obter detalhes da API, consulte a [GetAssetPropertyValue](#) Referência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando esse serviço com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **ListAssetModels** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o `ListAssetModels`.

CLI

AWS CLI

Para listar todos os modelos de ativos

O `list-asset-models` exemplo a seguir lista todos os modelos de ativos definidos em sua AWS conta na região atual.

```
aws iotsitewise list-asset-models
```

Saída:

```
{
  "assetModelSummaries": [
    {
      "id": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
      "arn": "arn:aws:iotsitewise:us-west-2:123456789012:asset-model/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
      "name": "Wind Farm Model",
      "description": "Represents a wind farm that comprises many wind turbines",
      "creationDate": 1575671284.0,
      "lastUpdateDate": 1575671988.0,
      "status": {
        "state": "ACTIVE"
      }
    },
    {
      "id": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
      "arn": "arn:aws:iotsitewise:us-west-2:123456789012:asset-model/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
      "name": "Wind Turbine Model",
      "description": "Represents a wind turbine manufactured by Example Corp",

```

```

        "creationDate": 1575671207.0,
        "lastUpdateDate": 1575686273.0,
        "status": {
            "state": "ACTIVE"
        }
    }
]
}

```

Para obter mais informações, consulte [Listar todos os modelos de ativos](#) no Guia do SiteWise usuário de AWS IoT.

- Para obter detalhes da API, consulte [ListAssetModels](#) em Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```

/**
 * Retrieves the asset model ID for the given asset model name.
 *
 * @param assetModelName the name of the asset model for the ID.
 * @return a {@link CompletableFuture} that represents a {@link String}
 * result of the asset model ID or null if the
 *         asset model cannot be found. The calling code can attach
 * callbacks, then handle the result or exception
 *         by calling {@link CompletableFuture#join()} or {@link
 * CompletableFuture#get()}.
 *
 * <p>
 *         If any completion stage in this method throws an exception, the
 * method logs the exception cause and keeps
 *         it available to the calling code as a {@link CompletionException}.
 * By calling
 *         {@link CompletionException#getCause()}, the calling code can
 * access the original exception.

```

```

    */
    public CompletableFuture<String> getAssetModelIdAsync(String assetModelName)
    {
        ListAssetModelsRequest listAssetModelsRequest =
        ListAssetModelsRequest.builder().build();
        return getAsyncClient().listAssetModels(listAssetModelsRequest)
            .handle((listAssetModelsResponse, exception) -> {
                if (exception != null) {
                    logger.error("Failed to retrieve Asset Model ID: {}",
                    exception.getCause().getMessage());
                    throw (CompletionException) exception;
                }
                for (AssetModelSummary assetModelSummary :
                listAssetModelsResponse.assetModelSummaries()) {
                    if (assetModelSummary.name().equals(assetModelName)) {
                        return assetModelSummary.id();
                    }
                }
                return null;
            });
    }
}

```

- Para obter detalhes da API, consulte [ListAssetModels](#) na Referência AWS SDK for Java 2.x da API.

JavaScript

SDK para JavaScript (v3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```

import {
    ListAssetModelsCommand,
    IoTSiteWiseClient,
} from "@aws-sdk/client-iotsitewise";
import { parseArgs } from "node:util";

```

```
/**
 * List asset models.
 * @param {{ assetModelTypes : array }}
 */
export const main = async ({ assetModelTypes = [] }) => {
  const client = new IoTSiteWiseClient({});
  try {
    const result = await client.send(
      new ListAssetModelsCommand({
        assetModelTypes: assetModelTypes, // The model types to list
      }),
    );
    console.log("Asset model types retrieved successfully.");
    return result;
  } catch (caught) {
    if (caught instanceof Error && caught.name === "IoTSiteWiseError") {
      console.warn(
        `${caught.message}. There was a problem listing the asset model types.`
      );
    } else {
      throw caught;
    }
  }
};
```

- Para obter detalhes da API, consulte [ListAssetModels](#) a Referência AWS SDK para JavaScript da API.

Python

SDK para Python (Boto3)

Note

Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no [AWS Code Examples Repository](#).

```
class IoTSitewiseWrapper:
```

```

"""Encapsulates AWS IoT SiteWise actions using the client interface."""

def __init__(self, iotsitewise_client: client) -> None:
    """
    Initializes the IoTSitewiseWrapper with an AWS IoT SiteWise client.

    :param iotsitewise_client: A Boto3 AWS IoT SiteWise client. This client
    provides low-level
                                access to AWS IoT SiteWise services.
    """
    self.iotsitewise_client = iotsitewise_client
    self.entry_id = 0 # Incremented to generate unique entry IDs for
    batch_put_asset_property_value.

    @classmethod
    def from_client(cls) -> "IoTSitewiseWrapper":
        """
        Creates an IoTSitewiseWrapper instance with a default AWS IoT SiteWise
        client.

        :return: An instance of IoTSitewiseWrapper initialized with the default
        AWS IoT SiteWise client.
        """
        iotsitewise_client = boto3.client("iotsitewise")
        return cls(iotsitewise_client)

    def list_asset_models(self) -> List[Dict[str, Any]]:
        """
        Lists all AWS IoT SiteWise Asset Models.

        :return: A list of dictionaries containing information about each asset
        model.

        """
        try:
            asset_models = []
            paginator =
self.iotsitewise_client.get_paginator("list_asset_models")
            pages = paginator.paginate()
            for page in pages:
                asset_models.extend(page["assetModelSummaries"])
            return asset_models
        except ClientError as err:

```

```
logger.error(  
    "Error listing asset models. Here's why %s",  
    err.response["Error"]["Message"],  
)  
raise
```

- Para obter detalhes da API, consulte a [ListAssetModels](#) Referência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando esse serviço com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

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 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](#)
- [Criptografia de dados em AWS IoT SiteWise](#)
- [Gerenciamento de identidade e acesso para AWS IoT SiteWise](#)
- [Validação de conformidade para AWS IoT SiteWise](#)
- [Resiliência em AWS IoT SiteWise](#)
- [Segurança da infraestrutura em AWS IoT SiteWise](#)
- [Análise de configuração e vulnerabilidade em AWS IoT SiteWise](#)
- [VPC endpoints para AWS IoT SiteWise](#)
- [Melhores práticas de segurança para AWS IoT SiteWise](#)

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 o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as [Data Privacy FAQ](#). Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog [AWS Shared Responsibility Model and RGPD](#) no Blog de segurança da AWS .

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 AWS os recursos. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como [trabalhar com CloudTrail trilhas](#) no Guia AWS CloudTrail do usuário.
- 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 140-3 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para obter mais informações sobre os endpoints FIPS disponíveis, consulte [Federal Information Processing Standard \(FIPS\) 140-3](#).

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sigilosas, como endereços de e-mail de clientes, em tags ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com AWS IoT SiteWise ou Serviços da AWS usa o console, a API ou AWS SDKs. AWS CLI Quaisquer dados inseridos em tags ou em 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, é fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse servidor.

Tópicos

- [Privacidade de tráfego entre redes para AWS IoT SiteWise](#)
- [AWS IoT SiteWise Melhoria do serviço comercial assistente](#)

Privacidade de tráfego entre redes para AWS IoT SiteWise

As conexões entre aplicativos locais AWS IoT SiteWise e aplicativos, como gateways SiteWise Edge, são protegidas por conexões TLS (Transport Layer Security). Para obter mais informações, consulte [Criptografia de dados em trânsito para AWS IoT SiteWise](#).

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.

AWS IoT SiteWise Melhoria do serviço comercial assistente

AWS IoT SiteWise O Assistant não usa dados do cliente para melhorar o serviço ou melhorar o subjacente LLMs.

Criptografia de dados em AWS IoT SiteWise

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 as APIs que estão hospedadas nos gateways do SiteWise Edge e acessíveis pela rede local. Eles APIs são expostos por meio

de uma conexão TLS apoiada por um certificado de servidor de propriedade do conector Edge. AWS IoT SiteWise Para autenticação do cliente, eles APIs usam 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 em repouso em AWS IoT SiteWise](#)
- [Criptografia de dados em trânsito para AWS IoT SiteWise](#)
- [Gerenciamento de chaves em AWS IoT SiteWise](#)

Criptografia em repouso em AWS IoT SiteWise

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 fontes OPC UA
- O conjunto de caminhos de fluxo de dados OPC UA das fontes 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 seu 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 de dados em trânsito para AWS IoT SiteWise

AWS IoT SiteWise usa criptografia em trânsito para proteger os dados transmitidos entre seus dispositivos, gateways e a AWS nuvem. A comunicação com AWS IoT SiteWise é criptografada usando HTTPS e TLS 1.2, garantindo que seus dados permaneçam confidenciais e protegidos contra acesso ou interceptação não autorizados.

Existem três modos de comunicação nos quais 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](#)
- [Dados em trânsito por meio da rede local](#)
- [Dados em trânsito entre componentes locais no SiteWise Edge](#)

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 [Adicione fontes de dados ao seu gateway AWS IoT SiteWise Edge](#).

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 “Gerenciar gateways”](#)

Dados em trânsito entre componentes locais no 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 em AWS IoT SiteWise

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 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. AWS IoT Greengrass 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 para AWS IoT SiteWise segurança](#)
- [Autenticar com identidades em AWS IoT SiteWise](#)

- [Como AWS IoT SiteWise funciona com o IAM](#)
- [AWS políticas gerenciadas para AWS IoT SiteWise](#)
- [Use funções vinculadas ao serviço para AWS IoT SiteWise](#)
- [Configure permissões para alarmes de eventos em AWS IoT SiteWise](#)
- [Prevenção confusa de delegados entre serviços em AWS IoT SiteWise](#)
- [Solucionar problemas de AWS IoT SiteWise identidade e acesso](#)

Público para AWS IoT SiteWise segurança

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 [Solucionar problemas de AWS IoT SiteWise 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. Envie as solicitações ao administrador do IAM para alterar as permissões dos usuários de serviço. Revise as informações nesta página para compreender os conceitos básicos do IAM. Para saber mais sobre como sua empresa pode usar o IAM com AWS IoT SiteWise, consulte [Como 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 o 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](#)

Autenticar com identidades em AWS IoT SiteWise

A autenticação é a forma 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 designar solicitações por conta própria, consulte [Versão 4 do AWS Signature para solicitações de API](#) no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser necessário fornecer 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 Guia do usuário do AWS IAM Identity Center e [Usar a autenticação multifator da AWS no IAM](#) 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 puder 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, é recomendável contar com 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, é recomendável alternar as chaves de acesso. Para obter mais informações, consulte [Alternar as 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 grupo chamado IAMAdminse conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte [Casos de uso para usuários do IAM](#) 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. Para assumir temporariamente uma função do IAM no AWS Management Console, você pode [alternar de um usuário para uma função do IAM \(console\)](#). 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 [Métodos para assumir um perfil](#) no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- **Acesso de usuário federado:** para atribuir permissões a identidades federadas, é possível 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 por ele. Para ter mais informações sobre perfis para federação, consulte [Criar um perfil para um provedor de identidade de terceiros \(federação\)](#) no Guia do usuário do IAM. Se usar o Centro de Identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de Identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte [Conjuntos de Permissões](#) no Guia do Usuário do AWS IAM Identity Center .
- **Permissões temporárias para usuários do IAM:** um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.

- **Acesso entre contas:** é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma 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 conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte [Acesso a recursos entre contas no IAM](#) 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 na Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões da entidade principal da chamada, usando um perfil de serviço ou um perfil vinculado 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 [Sessões de acesso direto](#).
- **Perfil de serviço:** um perfil de serviço é um [perfil 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 [Criar 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 presumir o perfil para 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 editar as permissões para perfis vinculados a serviço.
- **Aplicativos em execução na Amazon EC2** — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo solicitações AWS CLI de AWS API. Isso é preferível a armazenar chaves de acesso na EC2 instância. Para atribuir uma AWS função a uma EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que os programas em execução na EC2 instância recebam credenciais

temporárias. Para obter mais informações, consulte [Usar uma função do IAM para conceder permissões a aplicativos executados em EC2 instâncias da Amazon](#) 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 SiteWise
Políticas baseadas em identidade com permissões em nível de recurso	Sim
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de políticas	Sim
Políticas baseadas em recurso	Não
Listas de controle de acesso (ACLs)	Não
Autorização baseada em etiquetas (ABAC)	Sim
Credenciais temporárias	Sim
Sessões de acesso direto (FAS)	Sim
Perfis vinculados 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](#)
 - [Use credenciais temporárias com AWS IoT SiteWise](#)
 - [Sessões de acesso direto \(FAS\) para AWS IoT SiteWise](#)
 - [Perfis vinculados a serviço](#)
 - [Perfis de serviço](#)
 - [Escolher um perfil do IAM no AWS IoT SiteWise](#)
- [Autorização baseada em tags do AWS IoT SiteWise](#)
- [AWS IoT SiteWise políticas baseadas em identidade](#)
 - [Ações de políticas](#)
 - [BatchPutAssetPropertyValue autorização](#)
 - [Recursos de políticas](#)
 - [Chaves de condição de políticas](#)
 - [Exemplos](#)
- [AWS IoT SiteWise exemplos de políticas baseadas em identidade](#)
 - [Práticas recomendadas de política](#)
 - [Usar o console do AWS IoT SiteWise](#)
 - [Permitir que os usuários visualizem suas próprias permissões](#)
 - [Permitir que os usuários façam a ingestão de dados para ativos em uma hierarquia](#)
 - [Visualize AWS IoT SiteWise ativos com base em tags](#)
- [Gerencie o acesso usando políticas em AWS IoT SiteWise](#)
 - [Políticas baseadas em identidade](#)
 - [Políticas baseadas em recursos](#)
 - [Listas de controle de acesso \(ACLs\)](#)
 - [Outros tipos de política](#)
 - [Vários tipos de política](#)

AWS IoT SiteWise Funções do IAM

[Perfil do IAM](#) é uma entidade dentro da sua conta da AWS que tem permissões específicas.

Como AWS IoT SiteWise funciona com o IAM

Use 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. Obtenha credenciais de segurança temporárias chamando operações de API AWS STS tais como [AssumeRole](#) ou [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 [Use funções de serviço para AWS IoT SiteWise Monitor](#).

Sessões de acesso direto (FAS) para AWS IoT SiteWise

Compatibilidade com o recurso de encaminhamento de sessões de acesso (FAS): sim

Quando você usa um usuário ou uma função do IAM para realizar ações em 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 [Sessões de acesso direto](#).

Perfis vinculados a serviço

[As funções vinculadas ao serviço](#) permitem que os AWS serviços acessem recursos em outros serviços para concluir uma ação em seu nome. As funções vinculadas ao serviço aparecem na sua AWS conta 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 [Use funções vinculadas ao serviço para 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. As funções de serviço aparecem na sua AWS conta e são de propriedade da conta. Isso significa que um administrador do IAM pode alterar as permissões para esse perfil. 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 obter mais informações, consulte [Use 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 obter mais informações, consulte [Configure permissões para alarmes de eventos em AWS IoT SiteWise](#).

Escolher 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 obter mais informações, consulte [Use 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 as tags no [elemento de condição](#) de uma política usando as `aws:ResourceTag/key-name`,

`aws:RequestTag/key-name` ou chaves de condição `aws:TagKeys`. Para obter mais informações sobre recursos de marcação do AWS IoT SiteWise, consulte [Marque seus AWS IoT SiteWise recursos](#).

Para visualizar um exemplo de política baseada em identidade para limitar o acesso a um recurso baseado em tags desse recurso, consulte [Visualize AWS IoT SiteWise ativos com base em tags](#).

AWS IoT SiteWise políticas baseadas em identidade

As políticas do IAM permitem que você controle quem pode fazer o quê no 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 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 `Action` de uma política JSON descreve as ações que podem ser usadas 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. Algumas operações também 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 AWS IoT SiteWise](#) no Guia do usuário do IAM.

BatchPutAssetPropertyValue autorização

AWS IoT SiteWise autoriza o acesso à [BatchPutAssetPropertyValue](#) ação de uma forma incomum. Para a maioria das ações, quando você permite ou nega acesso a uma ação, esta ação retornará um erro se as permissões não tiverem sido concedidas. Com `BatchPutAssetPropertyValue`, você pode enviar várias entradas de dados para diferentes ativos e propriedades de ativo em uma única solicitação de API. O AWS IoT SiteWise autoriza cada entrada de dados de maneira 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 fluxo de dados, faça o seguinte:

- Autorize o recurso `time-series` se você usar um alias de propriedade para identificar o fluxo de dados.
- Autorize o recurso `asset` se você usar um ID de ativo para identificar o ativo que contém a propriedade de ativo associada.

Recursos 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 de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática

recomendada, especifique um recurso usando seu [nome do recurso da Amazon \(ARN\)](#). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em 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 seus ARNs. Um ARN tem a seguinte sintaxe geral.

```
arn:${Partition}:${Service}:${Region}:${Account}:${ResourceType}/${ResourcePath}
```

Para obter mais informações sobre o formato de ARNs, consulte [Identificar AWS recursos com nomes de recursos da Amazon \(ARNs\)](#).

Por exemplo, para especificar ativo com o ID a1b2c3d4-5678-90ab-cdef-2222EXAMPLE em sua instrução, use o seguinte ARN.

```
"Resource": "arn:aws:iotsitewise:region:123456789012:asset/a1b2c3d4-5678-90ab-cdef-2222EXAMPLE"
```

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 [Tipos de recursos definidos AWS IoT SiteWise](#) no Guia do usuário do IAM. Para saber com quais ações é possível especificar o ARN de cada atributo, 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 entidade principal pode executar ações em quais recursos e em que condições.

O elemento Condition (ou bloco Condition) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento Condition é opcional. É possível criar expressões condicionais que usem [agentes de condição](#), como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos de Condition em uma declaração ou várias chaves em um único elemento de Condition, 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 recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte [Elementos da 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
<code>iotsitewise:isAssociatedWithAssetProperty</code>	Se os fluxos de dados estão associados a uma propriedade 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: <code>true</code>	String
<code>iotsitewise:assetHierarchyPath</code>	O caminho da hierarquia do ativo, que é uma sequência de ativos, IDs cada um separado 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: <code>/a1b2c3d4-5678-90ab-cdef-2222EXAMPLE/</code>	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
<code>iotsitewise:iam</code>	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: <code>arn:aws:iam::123456789012:user/JohnDoe</code>	Sequência, nula
<code>iotsitewise:propertyAlias</code>	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
<code>iotsitewise:user</code>	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: <code>a1b2c3d4e5-a1b2c3d4-5678-90ab-cdef-aaaaEXAMPLE</code>	Sequência, nula

Chave de condição	Descrição	Tipos
<code>iotsitewise:group</code>	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
<code>iotsitewise:portal</code>	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
<code>iotsitewise:project</code>	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, as entidades (usuários e perfis) não têm permissão para criar ou modificar recursos do AWS IoT SiteWise. 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. Criar políticas do IAM que concedam aos usuários e perfis permissão para realizar operações de API específicas nos recursos necessários.
2. Anexar 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

- [Práticas recomendadas de política](#)
- [Usar o console do AWS IoT SiteWise](#)
- [Permitir que os usuários visualizem suas próprias permissões](#)
- [Permitir que os usuários façam a ingestão de dados para ativos em uma hierarquia](#)
- [Visualize AWS IoT SiteWise ativos com base em tags](#)

Práticas recomendadas 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 sua 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 [Políticas gerenciadas pela AWS 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 recursos 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.
- Use 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 escrever 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 [Elementos da política JSON do IAM: condição](#) no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações práticas para ajudar a criar políticas seguras e funcionais. Para obter mais informações, consulte [Validação de políticas 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 [Configuração de 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 sua AWS conta.

Se você criar uma política muito restritiva, o console poderá não funcionar conforme o esperado para usuários ou perfis (entidades) com essa política. Para garantir que essas entidades ainda possam usar o AWS IoT SiteWise console, anexe a política [AWSIoTSiteWiseConsoleFullAccess](#) gerenciada a elas ou defina permissões equivalentes para essas entidades. Para obter informações, consulte [Adicionar 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 conceder a elas acesso às ações específicas de que precisam para as 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 façam a ingestão de dados para ativos em uma hierarquia

Neste exemplo, você deseja conceder a um usuário da sua AWS conta acesso para gravar dados em todas as propriedades do ativo em uma hierarquia específica de ativos, começando pelo ativo `a1b2c3d4-5678-90ab-cdef-2222EXAMPLE` 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-2222EXAMPLE",
            "/a1b2c3d4-5678-90ab-cdef-2222EXAMPLE/*"
          ]
        }
      }
    }
  ]
}

```

Visualize AWS IoT SiteWise ativos 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}"
        }
      }
    }
  ]
}
```

Você pode anexar essa política aos usuários na 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`. Do contrário, Richard terá o acesso negado. Os nomes de chave de etiqueta da condição não diferenciam maiúsculas de minúsculas. Assim, `Owner` corresponde a `Owner` e `owner`. Para obter mais informações, consulte [IAM JSON Policy Elements: Condition](#) (Elementos da política JSON do IAM: Condição) no Guia do usuário do IAM.

Gerencie o acesso usando políticas em AWS IoT SiteWise

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 perfis não têm permissões. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação independentemente 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, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte [Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente](#) no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. 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 escolher entre uma política gerenciada ou uma política em linha, consulte [Escolher 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 perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo 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 recursos são políticas em linha 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 diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o AWS WAF Amazon VPC são exemplos de serviços que oferecem suporte. ACLs Para saber mais ACLs, consulte a [visão geral 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 com seus limites de permissões. As políticas baseadas em recurso 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 identidades 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 recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas 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 Organizations e SCPs, consulte [Políticas de controle de serviços](#) no Guia AWS Organizations do Usuário.

- Políticas de controle de recursos (RCPs) — RCPs são políticas JSON que você pode usar para definir o máximo de permissões disponíveis para recursos em suas contas sem atualizar as políticas do IAM anexadas a cada recurso que você possui. O RCP limita as permissões para recursos nas contas dos membros e pode afetar as permissões efetivas para identidades, incluindo a Usuário raiz da conta da AWS, independentemente de pertencerem à sua organização. Para obter mais informações sobre Organizations e RCPs, incluindo uma lista Serviços da AWS desse suporte RCPs, consulte [Políticas de controle de recursos \(RCPs\)](#) no Guia AWS Organizations do usuário.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil 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 recursos. 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 necessário tempo e experiência para [criar políticas gerenciadas pelo cliente do IAM](#) que concedam permissões precisas à equipe. Para uma configuração mais rápida, considere usar nossas políticas AWS gerenciadas para casos de uso comuns. Encontre políticas AWS gerenciadas em sua AWS conta. Para obter mais informações

sobre as políticas gerenciadas da AWS , consulte [Políticas gerenciadas da AWS](#) no Guia do usuário do IAM.

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 jamais são removidas, garantindo que as configurações permaneçam intactas.

Além disso, AWS oferece suporte a políticas gerenciadas para funções de trabalho que abrangem vários serviços. Por exemplo, a política ReadOnlyAccess AWS gerenciada 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: AWSIoT Site WiseReadOnlyAccess

Use a política AWSIoT Site WiseReadOnlyAccess AWS gerenciada para permitir acesso somente para leitura a. AWS IoT SiteWise

É possível anexar a política AWSIoT Site WiseReadOnlyAccess às 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: AWSService RoleForIoT Site Wise

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 — Atualização de 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, <code>BatchGet*</code> , que permite realizar operações de leitura em lote.	16 de setembro de 2022
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

Use funções vinculadas ao serviço para 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. 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 AWS IoT SiteWise.

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 que oferecem suporte a funções vinculadas a serviços, consulte [AWS serviços que funcionam com IAM](#) e procure os serviços que têm 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 a serviço para o AWS IoT SiteWise](#)
- [Atualizar um perfil vinculado ao serviço para o AWS IoT SiteWise](#)
- [Excluir um perfil vinculado ao serviço para o AWS IoT SiteWise](#)
- [Regiões suportadas para funções vinculadas a AWS IoT SiteWise serviços](#)
- [Use 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.

O perfil vinculado ao serviço `AWSServiceRoleForIoTSiteWise` usa a política `AWSServiceRoleForIoTSiteWise` com as permissões a seguir. 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 ter mais informações sobre as ações permitidas em `AWSServiceRoleForIoTSiteWise`, consulte [AWS managed policies for 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": [

```

```
"IOTSITWISE"  
  ]  
}  
}  
}  
]  
}
```

Você pode usar os registros para monitorar e solucionar problemas em seus gateways do SiteWise Edge. Para obter mais informações, consulte [Monitore os registros do gateway SiteWise 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 obter mais informações, consulte [Service-linked role permissions](#) (Permissões de nível vinculado a serviços) no Guia do usuário do IAM.

Crie uma função vinculada a serviço para o AWS IoT SiteWise

AWS IoT SiteWise requer uma função vinculada ao serviço para realizar determinadas ações e acessar recursos em seu nome. Uma função vinculada ao serviço é um tipo exclusivo de função de AWS Identity and Access Management (IAM) vinculada diretamente a. AWS IoT SiteWise Ao criar essa função, você AWS IoT SiteWise concede as permissões necessárias para acessar outros AWS serviços e recursos necessários para sua operação, como o Amazon S3 para armazenamento de dados ou AWS IoT comunicação com dispositivos.

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você executa as seguintes operações no AWS IoT SiteWise console, AWS IoT SiteWise cria a função vinculada ao serviço para você.

- Criar um gateway do Greengrass V1.
- Configurar a opção de registro em log.
- Escolher o botão de aceitação no banner de execução da consulta.

Se excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, será possível 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 política da `AWSServiceRoleForIoTSiteWise` e uma relação de confiança `comiotsitewise.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 `comiotsitewise.amazonaws.com`.

Para ter mais informações, consulte [Criar um perfil vinculado ao 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.

Atualizar um perfil vinculado ao serviço para o AWS IoT SiteWise

AWS IoT SiteWise não permite que você edite a função vinculada ao serviço da `AWSServiceRoleForIoTSiteWise`. 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 poderá editar a descrição do perfil usando o IAM. Para ter mais informações, consulte [Atualizar um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

Excluir um perfil vinculado ao serviço para o AWS IoT SiteWise

Se um recurso ou um serviço que exige um perfil vinculado ao serviço não está mais em uso, é recomendável excluí-lo. Isso é para evitar a presença de uma entidade inativa que não esteja sendo monitorada nem mantida. No entanto, você deve limpar os recursos de seu perfil vinculado ao serviço antes de excluí-lo 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 AWSService RoleForlo TSite Wise

1. Desative o registro para AWS IoT SiteWise. Para obter mais informações, consulte [Alterar o nível de registro em log](#).
2. Exclua todos os gateways ativos SiteWise do Edge.

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função vinculada ao serviço da AWSService RoleForlo TSite Wise. Para ter mais informações, consulte [Delete roles or instance profiles](#) 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](#).

Use funções de serviço para AWS IoT SiteWise Monitor

O perfil de serviço é um [perfil 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 [Criar 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 SiteWise e 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 [AWSIoTSiteWiseMonitorPortalAccess](#) gerenciada 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 SiteWise e 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

- [Permissões de função de serviço para SiteWise Monitor \(Classic\)](#)
- [Permissões de função de serviço para SiteWise Monitor \(com reconhecimento de IA\)](#)
- [Gerenciar a função de serviço do SiteWise Monitor \(console\)](#)
 - [Encontrar um perfil de serviço do portal \(console\)](#)
 - [Criar uma função de serviço do SiteWise Monitor \(AWS IoT SiteWise console\)](#)
 - [Crie uma função de serviço do SiteWise Monitor \(console do IAM\)](#)
 - [Alterar um perfil de serviço do portal \(console\)](#)
- [Gerenciar a função de serviço do SiteWise Monitor \(CLI\)](#)
 - [Encontrar um perfil de serviço do portal \(CLI\)](#)
 - [Crie a função de serviço do SiteWise Monitor \(CLI\)](#)
- [SiteWise Monitore as atualizações do AWSIoTSiteWiseMonitorServiceRole](#)

Permissões de função de serviço para SiteWise Monitor (Classic)

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, que começa com `AWSIoTSiteWiseMonitorServicePortalPolicy`, para permitir que os usuários do SiteWise Monitor concluam ações nos recursos da sua conta. A política gerenciada [AWSIoTSiteWiseMonitorPortalAccess](#) 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 [Configure permissões para alarmes de eventos em AWS IoT SiteWise](#).

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 [Administre seus portais do SiteWise Monitor](#) [CreateAccessPolicy](#).

Permissões de função de serviço para SiteWise Monitor (com reconhecimento de IA)

Quando você cria um portal, AWS IoT SiteWise permite criar uma função cujo nome começa com `loTSite WisePortalRole`. 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.

Warning

As funções de proprietário do projeto e visualizador do projeto não são suportadas pelo SiteWise Monitor (compatível com IA).

A função confia que o seguinte serviço assuma a função:

- `monitor.iotsitewise.amazonaws.com`

A função usa a seguinte política de permissões, que começa com `IoT Site Wise API Portal AccessPolicy`, para permitir que os usuários do SiteWise Monitor concluam ações nos recursos da sua conta.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iotsitewise:CreateProject",
        "iotsitewise:DescribePortal",
        "iotsitewise:ListProjects",
        "iotsitewise:DescribeProject",
        "iotsitewise:UpdateProject",
        "iotsitewise>DeleteProject",
        "iotsitewise:CreateDashboard",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:UpdateDashboard",
        "iotsitewise>DeleteDashboard",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListAssets",
        "iotsitewise:DescribeAsset",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:ListAssetProperties",
        "iotsitewise:DescribeAssetProperty",
        "iotsitewise:GetAssetPropertyValue",
        "iotsitewise:GetAssetPropertyValueHistory",
        "iotsitewise:GetAssetPropertyAggregates",
        "iotsitewise:GetInterpolatedAssetPropertyValues",
        "iotsitewise:BatchGetAssetPropertyAggregates",
        "iotsitewise:BatchGetAssetPropertyValue",
        "iotsitewise:BatchGetAssetPropertyValueHistory",
        "iotsitewise:ListAssetRelationships",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:ListAssetModels",
        "iotsitewise:DescribeAssetCompositeModel",
        "iotsitewise:DescribeAssetModelCompositeModel",

```

```

        "iotsitewise:ListAssetModelProperties",
        "iotsitewise:ExecuteQuery",
        "iotsitewise:ListTimeSeries",
        "iotsitewise:DescribeTimeSeries",
        "iotsitewise:InvokeAssistant",
        "iotsitewise:DescribeDataset",
        "iotsitewise:ListDatasets",
        "iotevents:DescribeAlarmModel",
        "iotevents:ListTagsForResource",
        "iottwinmaker:ListWorkspaces",
        "iottwinmaker:ExecuteQuery",
        "iottwinmaker:GetWorkspace",
        "identitystore:DescribeUser"
    ],
    "Resource": "*"
}
]
}

```

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.

Gerenciar a função de serviço do 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 os perfis existentes adequados para anexação. Se nenhum estiver disponível, o console poderá criar e configurar um perfil de serviço para você. Para obter mais informações, consulte [Crie um portal no SiteWise Monitor](#).

Tópicos

- [Encontrar um perfil de serviço do portal \(console\)](#)
- [Criar uma função de serviço do SiteWise Monitor \(AWS IoT SiteWise console\)](#)
- [Crie uma função de serviço do SiteWise Monitor \(console do IAM\)](#)
- [Alterar um perfil de serviço do portal \(console\)](#)

Encontrar um perfil de serviço do 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).

Criar 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 obter mais informações, consulte [Crie um portal no SiteWise Monitor](#).

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. Escolha Salvar.

Crie 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 [AWSIoTSiteWiseMonitorPortalAccess](#) gerenciada 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, selecione Perfis.
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 Próximo: Permissões.
7. Escolha Next: Tags (Próximo: tags).
8. Selecione Próximo: revisar.
9. Insira um Nome do perfil para o novo perfil de serviço.
10. Selecione Criar perfil.

Alterar um perfil de serviço do 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. Escolha Salvar.

Gerenciar 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 um perfil de serviço do portal \(CLI\)](#)
- [Crie a função de serviço do SiteWise Monitor \(CLI\)](#)

Encontrar um perfil de serviço do 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 [DescribePortal](#) operação para localizar a função do seu portal se você souber a ID do seu portal.

Crie 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 [CreatePortal](#) na Referência AWS IoT SiteWise da API.
3. a. Para o SiteWise Monitor (Clássico) — anexe a `AWSIoTSiteWiseMonitorPortalAccess` política 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
```

- b. Para o SiteWise monitor (compatível com IA) — anexe a `IoTSiteWiseAIPortalAccessPolicy` política à função ou anexe uma política que defina permissões equivalentes. Por exemplo, crie uma política com permissões de acesso ao portal. O exemplo a seguir cria uma política chamada `MySiteWiseMonitorPortalAccess`.

```
aws iam create-policy \
  --policy-name MySiteWiseMonitorPortalAccess \
  --policy-document '{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
```

```

        "iotsitewise:CreateProject",
        "iotsitewise:DescribePortal",
        "iotsitewise:ListProjects",
        "iotsitewise:DescribeProject",
        "iotsitewise:UpdateProject",
        "iotsitewise>DeleteProject",
        "iotsitewise:CreateDashboard",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:UpdateDashboard",
        "iotsitewise>DeleteDashboard",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListAssets",
        "iotsitewise:DescribeAsset",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:ListAssetProperties",
        "iotsitewise:DescribeAssetProperty",
        "iotsitewise:GetAssetPropertyValue",
        "iotsitewise:GetAssetPropertyValueHistory",
        "iotsitewise:GetAssetPropertyAggregates",
        "iotsitewise:GetInterpolatedAssetPropertyValues",
        "iotsitewise:BatchGetAssetPropertyAggregates",
        "iotsitewise:BatchGetAssetPropertyValue",
        "iotsitewise:BatchGetAssetPropertyValueHistory",
        "iotsitewise:ListAssetRelationships",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:ListAssetModels",
        "iotsitewise:DescribeAssetCompositeModel",
        "iotsitewise:DescribeAssetModelCompositeModel",
        "iotsitewise:ListAssetModelProperties",
        "iotsitewise:ExecuteQuery",
        "iotsitewise:ListTimeSeries",
        "iotsitewise:DescribeTimeSeries",
        "iotsitewise:InvokeAssistant",
        "iotsitewise:DescribeDataset",
        "iotsitewise:ListDatasets",
        "iotevents:DescribeAlarmModel",
        "iotevents:ListTagsForResource",
        "iottwinmaker:ListWorkspaces",
        "iottwinmaker:ExecuteQuery",
        "iottwinmaker:GetWorkspace",
        "identitystore:DescribeUser"
    ],
    "Resource": "*"
}

```

```
]
}'
```

Como anexar uma função de serviço a um portal existente

1. Para recuperar os detalhes existentes do portal, execute o comando a seguir. *portal-id* Substitua pela 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. *role-arn* Substitua 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 AWS IoT SiteWise Monitor Service Role

Você pode ver detalhes sobre as atualizações do SiteWise Monitor, a AWS IoT SiteWise Monitor Service Role, 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
AWS IoT SiteWise Monitor Portal Access : política atualizada	AWS IoT SiteWise atualizou a política AWS IoT SiteWise Monitor Portal Access gerenciada 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

Configure permissões para alarmes de eventos em AWS IoT SiteWise

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 podem ser usadas 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`, `iotsitewise:ListAssetModels` — 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.

Exemplo 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:ListAssetModels",
        "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",
        "iotsitewise:ListAssetModels"
      ],
      "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 habilitar esse recurso AWS IoT SiteWise, você deve ter a `iotevents:ListInputRoutings` permissão. Essa permissão permite AWS IoT SiteWise fazer chamadas para a operação de [ListInputRoutings](#) API suportada pelo AWS IoT Events.

Note

É altamente recomendável adicionar a permissão `ListInputRoutings`.

Exemplo 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 confusa de delegados entre serviços em AWS IoT SiteWise

“Confused deputy” é um problema de segurança no qual uma entidade sem 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 personificação 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, a 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 [aws:SourceAccount](#) global [aws:SourceArn](#) as chaves de contexto nas políticas de recursos para limitar as permissões que AWS IoT SiteWise concede 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:service:*:123456789012:*`

Example – Prevenção contra representante confuso

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"
      }
    }
  }
}
```

```
}  
}  
}
```

Solucionar problemas de AWS IoT SiteWise 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 AWS conta 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 AWS conta acessem meus AWS IoT SiteWise recursos

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. É possível 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 essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se é AWS IoT SiteWise compatível com esses recursos, consulte [Como AWS IoT SiteWise funciona com o IAM](#).
- Para saber como fornecer acesso aos seus recursos em todas as Contas da AWS que você possui, consulte Como [fornecer acesso a um usuário do IAM em outra 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.
- Para saber como conceder acesso por meio da federação de identidades, consulte [Conceder acesso a usuários autenticados externamente \(federação de identidades\)](#) no Guia do usuário do IAM.
- Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte [Acesso a recursos entre contas no IAM](#) 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 (IIoT) industrial 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 altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center 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 [Interaja com outros AWS serviços](#) e [Exportar dados para o Amazon S3 com notificações de propriedades de ativo](#).
- Você pode usar o AWS IoT SiteWise Get * APIs para recuperar e fazer backup de dados históricos de propriedades do ativo. Para obter mais informações, consulte [Consulte valores históricos de propriedades de ativos em AWS IoT SiteWise](#).
- Você pode usar o 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 oferecer compatibilidade 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, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando 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. 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 em AWS IoT SiteWise

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 normalmente têm capacidade de processamento, memória e armazenamento limitados, os dispositivos 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 [O que é o AWS IoT Device Defender?](#) no Guia do desenvolvedor do AWS IoT Device Defender .

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 [Gerencie gateways SiteWise Edge](#) e.

VPC endpoints para AWS IoT SiteWise

Uma interface VPC endpoint estabelece uma conexão privada entre sua nuvem privada virtual (VPC) e. AWS IoT SiteWise [AWS PrivateLink](#) alimenta os endpoints da interface, permitindo acesso privado às operações AWS IoT SiteWise da API. Você pode ignorar a necessidade de um gateway da 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 um VPC endpoint AWS IoT SiteWise, consulte [Acesse um AWS serviço usando uma interface VPC](#) endpoint no Guia.AWS PrivateLink

Operações de API para endpoints VPC em AWS IoT SiteWise

AWS IoT SiteWise suporta fazer chamadas para as seguintes operações de AWS IoT SiteWise API da sua VPC:

- Para todas as operações de API do plano de dados, use o endpoint a seguir. Substitua *region* pela sua Região da AWS.

```
data.iotsitewise.region.amazonaws.com
```

As operações da API do plano de dados incluem o seguinte:

- [BatchGetAssetPropertyValue](#)

- [BatchGetAssetPropertyValueHistory](#)
 - [BatchPutAssetPropertyValue](#)
 - [GetAssetPropertyAggregates](#)
 - [GetAssetPropertyValue](#)
 - [GetAssetPropertyValueHistory](#)
 - [GetInterpolatedAssetPropertyValues](#)
- 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 sua Região da AWS.

```
api.iotsitewise.region.amazonaws.com
```

As operações de API do ambiente de gerenciamento suportadas incluem o seguinte:

- [AssociateAssets](#)
- [CreateAsset](#)
- [CreateAssetModel](#)
- [DeleteAsset](#)
- [DeleteAssetModel](#)
- [DeleteDashboard](#)
- [DescribeAsset](#)
- [DescribeAssetModel](#)
- [DescribeAssetProperty](#)
- [DescribeDashboard](#)
- [DescribeLoggingOptions](#)
- [DisassociateAssets](#)
- [ListAssetModels](#)
- [ListAssetRelationships](#)
- [ListAssets](#)
- [ListAssociatedAssets](#)
- [PutLoggingOptions](#)

- [UpdateAssetModel](#)
- [UpdateAssetProperty](#)
- [CreateGateway](#)
- [DeleteGateway](#)
- [DescribeDefaultEncryptionConfiguration](#)
- [DescribeGateway](#)
- [DescribeGatewayCapabilityConfiguration](#)
- [DescribeStorageConfiguration](#)
- [ListGateways](#)
- [ListTagsForResource](#)
- [UpdateGateway](#)
- [UpdateGatewayCapabilityConfiguration](#)
- [PutDefaultEncryptionConfiguration](#)
- [PutStorageConfiguration](#)
- [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](#)
- [CreateAccessPolicy](#)
- [CreateDashboard](#)
- [CreatePortal](#)
- [CreateProject](#)
- [DeleteAccessPolicy](#)
- [DeletePortal](#)
- [DeleteProject](#)
- [DescribeAccessPolicy](#)

- [DescribePortal](#)
- [DescribeProject](#)
- [ListAccessPolicies](#)
- [ListDashboards](#)
- [ListPortals](#)
- [ListProjects](#)
- [ListProjectAssets](#)
- [UpdateAccessPolicy](#)
- [UpdateDashboard](#)
- [UpdatePortal](#)
- [UpdateProject](#)

Criar um endpoint de VPC da interface para 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 CLIPara obter mais informações, consulte [Acessar um AWS serviço usando uma interface VPC endpoint no Guia](#).AWS PrivateLink

Crie um VPC endpoint para AWS IoT SiteWise usando um dos seguintes nomes de serviço:

- Para as operações de API do plano de dados, use o seguinte nome de serviço:

```
com.amazonaws.region.iotsitewise.data
```

- Para as operações de API do ambiente de gerenciamento, use o seguinte nome de serviço:

```
com.amazonaws.region.iotsitewise.api
```

Acesso 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: *region* Substitua por seu Região da AWS.

```
data.iotsitewise.region.amazonaws.com
```

- Para as operações da API do plano de controle, use o seguinte endpoint: *region* Substitua por seu 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 URL de endpoint a seguir. Substitua *vpc-endpoint-id* e *region* por seu ID de endpoint de VPC e sua região.

```
vpc-endpoint-id.data.iotsitewise.region.vpce.amazonaws.com
```

- Para as operações da API do ambiente de gerenciamento, use o URL de endpoint a seguir. Substitua *vpc-endpoint-id* e *region* por seu ID de endpoint de VPC e sua região.

```
vpc-endpoint-id.api.iotsitewise.region.vpce.amazonaws.com
```

2. Desative a injeção do prefixo do host. O AWS CLI e AWS SDKs precede o endpoint do serviço com vários prefixos de host quando você chama cada operação de API. Esse recurso faz com que o AWS CLI e AWS SDKs produza coisas URLs que não são válidas 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 Ferramentas da AWS para PowerShell. Isso significa que, se você desabilitar 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 Ferramentas da AWS para PowerShell para acessar AWS IoT SiteWise por meio do endpoint.

Para obter mais informações sobre como desabilitar a injeção de prefixo de host no AWS SDKs, consulte as seções de documentação a seguir para cada SDK:

- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java](#)
- [AWS SDK for Java 2.x](#)
- [AWS SDK para JavaScript](#)
- [AWS SDK para .NET](#)
- [AWS SDK para PHP](#)
- [AWS SDK para Python \(Boto3\)](#)
- [AWS SDK para Ruby](#)

Para obter mais informações, consulte [Acessar um AWS serviço usando uma interface VPC endpoint no Guia](#).AWS PrivateLink

Crie 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 obter mais informações, consulte [Controlar o acesso aos endpoints da VPC usando políticas de endpoint](#) 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 123456789012* na AWS conta do 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 nos servidores OPC UA

Exija credenciais de autenticação para conexão 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 obter mais informações, consulte [Configurar a autenticação da fonte de dados para o SiteWise Edge](#).

Usar modos de comunicação criptografados para os 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 uma fonte OPC UA no SiteWise Edge](#).

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.

Para obter informações sobre como atualizar componentes no AWS IoT SiteWise console, consulte [Alterar a versão dos pacotes de componentes do SiteWise Edge Gateway](#).

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.

Proteger dados no Siemens Industrial Edge Management

Os dados do dispositivo que você escolhe compartilhar com o AWS IoT SiteWise Edge são determinados nos tópicos Siemens IEM Databus de configuração. Ao escolher tópicos para compartilhar com o SiteWise Edge, você está compartilhando dados em nível de tópico. AWS IoT SiteWise Siemens Industrial Edge Marketplace É um mercado independente, separado do AWS. Para proteger seus dados compartilhados, o aplicativo SiteWise Edge não será executado a menos que você o utilize Siemens Secured Storage. Para ter mais informações, consulte [Secure Storage](#) na documentação da Siemens.

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 obter mais informações, consulte [Use 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 obter mais informações, consulte [Práticas recomendadas 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
- [Ten security golden rules for Industrial IoT solutions](#)

Faça login e monitore 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 rastreie métricas, crie painéis personalizados e defina alarmes que notificam você ou realizam ações quando uma métrica atinge determinado limite. Por exemplo, você pode CloudWatch rastrear o uso da CPU ou outras métricas de suas EC2 instâncias da Amazon 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 CloudTrail captura 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 do AWS CloudTrail](#).

Tópicos

- [Monitore com Amazon CloudWatch Logs](#)
- [Monitore os registros do gateway SiteWise Edge](#)
- [Monitore AWS IoT SiteWise com CloudWatch métricas da Amazon](#)
- [Registre chamadas de AWS IoT SiteWise API com AWS CloudTrail](#)

Monitore 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 obter mais informações, consulte [Crie uma função vinculada a 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.
- *source-ARN* Substitua 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.
- *account-ID* Substitua pelo ID da AWS conta associado ao AWS IoT SiteWise recurso especificado.

```
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 obter mais informações, consulte [Monitore os registros do gateway SiteWise 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 obter mais informações, consulte [Solucionar problemas de uma ação de AWS IoT SiteWise regra](#).

Sumário

- [Gerenciar o login AWS IoT SiteWise](#)
 - [Encontrar o nível de registro em log](#)
 - [Alterar o nível de registro em log](#)
- [Exemplo: entradas do arquivo de AWS IoT SiteWise log](#)

Gerenciar o login AWS IoT SiteWise

Use o AWS IoT SiteWise console ou AWS CLI para as seguintes tarefas de configuração de registro.

Encontrar o nível de registro em log

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"
  }
}
```

Alterar o nível de registro em log

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 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.
logging-level Substitua pelo nível de registro 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"
  }
}
```

Monitore os registros do gateway SiteWise Edge

Você pode configurar seu gateway AWS IoT SiteWise Edge para registrar informações no Amazon CloudWatch Logs ou no sistema de arquivos local.

Tópicos

- [Use Amazon CloudWatch Logs](#)
- [Use os registros de serviço AWS IoT SiteWise](#)

Use 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.

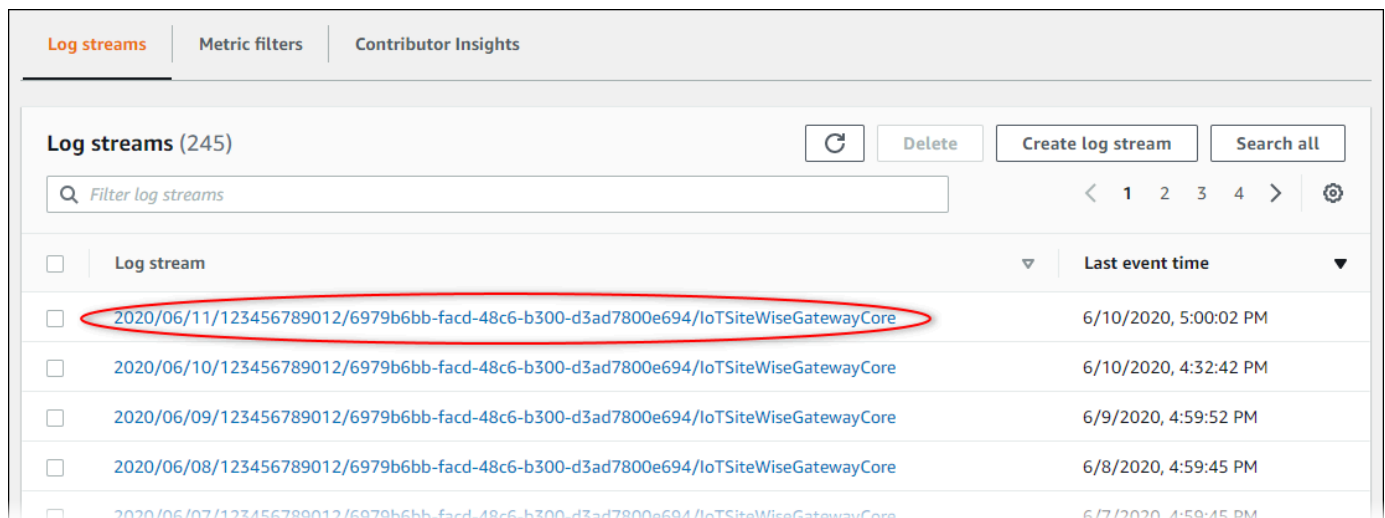
Para configurar e acessar CloudWatch os registros (console)

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 para o AWS IoT SiteWise

Escolha o grupo de logs para a função a ser depurada.

4. Escolha um stream 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.

The screenshot shows the 'Log events' interface in AWS IoT SiteWise. A modal window is open for selecting a time range. The 'Relative' tab is selected, and the 'Minutes' section has '5' selected. The 'custom (5m)' button is highlighted in the top right of the modal. The 'Apply' button is highlighted in the bottom right of the modal.

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.

Use os registros de serviço AWS IoT SiteWise

SiteWise Os dispositivos Edge Gateway incluem arquivos de registro de serviços 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 log 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 exibir os logs 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 exibir os logs 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
```

Monitore 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 2 métricas de gateway

AWS IoT SiteWise publica métricas de gateway para fluxos clássicos, gateways V2 e gateways V3 habilitados para MQTT. Salvo indicação em contrário, cada métrica é aplicável às duas versões de gateway auto-hospedado. Todas as métricas do SiteWise Edge Gateway são publicadas em um intervalo de um minuto.

SiteWise Métricas do gateway Edge

Métrica	Descrição
<code>Gateway.AvailableMemory</code>	A memória disponível de um gateway SiteWise Edge. Unidade: bytes Dimensões: nenhuma
<code>Gateway.AvailableDiskSpace</code>	O espaço em disco disponível de um gateway SiteWise Edge. Unidade: bytes Dimensões: nenhuma
<code>Gateway.CloudConnectivity</code>	O status da conectividade na nuvem de um gateway SiteWise Edge. Unidade: nenhuma Dimensão: GatewayId
<code>Gateway.CpuUsage</code>	O uso da CPU de um gateway SiteWise Edge. Unidade: porcentagem Dimensões: nenhuma
<code>Gateway.TotalDiskSpace</code>	O espaço total em disco de um gateway SiteWise Edge. Unidade: bytes Dimensões: nenhuma
<code>Gateway.TotalMemory</code>	A memória total de um gateway SiteWise Edge. Unidade: bytes

Métrica	Descrição
	Dimensões: nenhuma
<code>Gateway.UsedDiskSpace</code>	O espaço em disco usado de um gateway SiteWise Edge. Unidade: bytes Dimensões: nenhuma
<code>Gateway.UsedMemory</code>	A memória usada de um gateway SiteWise Edge. Unidade: bytes Dimensões: nenhuma
<code>Gateway.UsedPercentageDiskSpace</code>	A porcentagem usada do espaço em disco de um gateway SiteWise Edge. Unidade: bytes Dimensões: nenhuma
<code>Gateway.UsedPercentageMemory</code>	A porcentagem de memória usada de um gateway SiteWise Edge. Unidade: bytes Dimensões: nenhuma

AWS IoT SiteWise métricas do editor

Métrica	Descrição
<code>IoTSiteWisePublisher.ComponentBuildVersion</code>	Essa métrica indica a versão de compilação do componente SiteWise editor de IoT em execução no gateway. Um valor de 1 significa que o gateway está executando uma versão

Métrica	Descrição
	do editor correspondente à Component BuildVersion dimensão. Unidade: 1 Dimensões: GatewayId, ComponentBuildVersion
IoTSiteWisePublisher.DroppedCount	O número de pontos de dados que são descartados por um gateway SiteWise Edge (GatewayId) e não publicados na nuvem, gerados a cada minuto. Unidade: Contagem Dimensões: GatewayId
IoTSiteWisePublisher.Heartbeat	Gerado a cada minuto pelo editor no gateway SiteWise Edge. Unidade: 1 (1 indica que o publicador está em execução e sem o ponto de dados que indica que o publicador não está em execução) Dimensões: GatewayId
IoTSiteWisePublisher.IsConnectedToMqttBroker	Gerado a cada minuto pelo editor no gateway SiteWise Edge. Unidade: 1 (1 indica que o publicador está conectado a um agente MQTT) Dimensões: GatewayId

Métrica	Descrição
<code>IoTSiteWisePublisher.MessageCheckpointPersistenceErrorCount</code>	A métrica indica que o gateway detectou um problema no arquivo de ponto de verificação usado para rastrear os dados processados pelo publicador. Um valor de 1 indica que ocorreu uma falha. Unidade: nenhuma Dimensões: AccountId, GatewayId
<code>IoTSiteWisePublisher.MqttMessageReceivedSuccessCount</code>	O número de mensagens recebidas com êxito pelo publicador do agente MQTT. Métrica gerada a cada minuto. Unidade: Contagem Dimensões: GatewayId
<code>IoTSiteWisePublisher.MqttReceivedSuccessBytes</code>	O número de bytes de dados de mensagem recebidos com êxito pelo publicador do agente MQTT. Métrica gerada a cada minuto. Unidade: Contagem Dimensões: GatewayId
<code>IoTSiteWisePublisher.NumberOfSubscriptionsToMqttBroker</code>	O número de tópicos inscritos no agente MQTT pelo publicador. Métrica gerada a cada minuto. Um tópico curinga multinível é contado como 1. Unidade: Contagem Dimensões: GatewayId

Métrica	Descrição
<code>IoTSiteWisePublisher.NumberOfUniqueMqttTopicsReceived</code>	O número de tópicos exclusivos recebidos pelo publicador do agente MQTT. Métrica gerada a cada minuto. Unidade: Contagem Dimensões: GatewayId
<code>IoTSiteWisePublisher.PublisherFailureCount</code>	O número de pontos de dados que um gateway SiteWise Edge (GatewayId) falhou em publicar, gerados a cada minuto. Unidade: Contagem Dimensões: GatewayId
<code>IoTSiteWisePublisher.PublisherRejectedCount</code>	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
<code>IoTSiteWisePublisher.PublisherSuccessCount</code>	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
<code>IoTSiteWisePublisher.PublisherToS3FailureCount</code>	O número de pontos de dados que um gateway (GatewayId) não conseguiu publicar em um bucket do Amazon S3. Unidade: Contagem Dimensões: GatewayId

Métrica	Descrição
<code>IoTSiteWisePublisher.PublisherToS3SuccessCount</code>	O número de pontos de dados que um gateway (GatewayId) publicou com êxito em um bucket do Amazon S3. Unidade: Contagem Dimensões: GatewayId

Métricas de coletor OPC UA

Métrica	Descrição
<code>OpcUaCollector.ActiveDataStreamCount</code>	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
<code>OpcUaCollector.ComponentBuildVersion</code> (não disponível em streams clássicos, gateways V2)	Essa métrica indica a versão de compilação do componente coletor IoT SiteWise OPC UA em execução no gateway. Um valor de 1 significa que o gateway está executando uma versão do coletor correspondente à Component BuildVersion dimensão. Unidade: 1 Dimensões: GatewayId, ComponentBuildVersion
<code>OpcUaCollector.ConversionErrors</code>	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

Métrica	Descrição
	dados para AWS IoT SiteWise. Esses pontos de dados não serão ingeridos pelo coletor OPC UA. Unidade: Contagem Dimensões: GatewayId, SourceName
<code>OpcUaCollector.Heartbeat</code>	Gerado a cada minuto para cada fonte OPC UA (<code>sourceName</code>) conectada a um gateway SiteWise Edge (<code>gatewayId</code>). Unidade: contagem (1 indica que a fonte está conectada e 0 indica que a fonte está desconectada) Dimensões: GatewayId, SourceName
<code>OpcUaCollector.IncomingValuesCount</code>	O número de pontos de dados que um gateway SiteWise Edge (<code>gatewayId</code>) recebeu para uma fonte OPC UA (<code>sourceName</code>), gerados a cada minuto. Unidade: Contagem Dimensões: GatewayId, SourceName, PropertyGroup

Métrica	Descrição
<code>OpcUaCollector.IncomingValueErrors</code>	O número de pontos de dados que um gateway SiteWise Edge (<code>gatewayId</code>) recebe de uma fonte OPC UA (<code>sourceName</code>) que não são valores válidos. Esses pontos de dados não são ingeridos pelo coletor OPC UA. Métrica gerada a cada minuto. Unidade: Contagem Dimensões: <code>GatewayId</code>, <code>SourceName</code>, <code>PropertyGroup</code>
<code>OpcUaCollector.IsConnectedToMqttBroker</code> (não disponível em streams clássicos, gateways V2)	Gerado a cada minuto pelo componente coletor IoT SiteWise OPC UA no gateway Edge. SiteWise Unidade: 1 (1 representando o componente coletor IoT SiteWise OPC UA está conectado a um broker MQTT) Dimensões: <code>GatewayId</code>
<code>OpcUaCollector.MqttMessagesDroppedCount</code> (não disponível em streams clássicos, gateways V2)	O número de mensagens MQTT eliminadas pelo componente coletor SiteWise IOT OPC UA. Unidade: Contagem Dimensões: <code>GatewayId</code>, <code>SourceName</code>
<code>OpcUaCollector.MqttMessagesPublishedBytes</code> (não disponível em streams clássicos, gateways V2)	O número de bytes de dados de mensagens MQTT publicados com sucesso pelo componente coletor SiteWise IoT OPC UA para o agente MQTT. Unidade: Contagem Dimensões: <code>GatewayId</code>, <code>SourceName</code>

Métrica	Descrição
<code>OpcUaCollector.MqttMessagesPublishedCount</code> (não disponível em streams clássicos, gateways V2)	O número de mensagens MQTT publicadas com sucesso pelo componente coletor SiteWise IOT OPC UA para o agente MQTT. Unidade: Contagem Dimensões: GatewayId, SourceName
<code>OpcUaCollector.NullValueCount</code> (não disponível em streams clássicos, gateways V2)	O número de valores nulos recebidos pelo componente coletor SiteWise IOT OPC UA do servidor OPC UA. Unidade: Contagem Dimensões: GatewayId, SourceName, PropertyGroup
<code>OpcUaCollector.NumberOfUniqueMqttTopicsPublished</code> (não disponível em streams clássicos, gateways V2)	O número de tópicos exclusivos de MQTT publicados pelo coletor SiteWise IoT OPC UA para o corretor MQTT. Unidade: Contagem Dimensões: GatewayId, SourceName

AWS IoT SiteWise métricas do processador

Métrica	Descrição
<code>Gateway.DataProcessor.IngestionThrottled</code> (não disponível em gateways V3 habilitados para MQTT)	O número de pontos de dados que sofreram controle de utilização. Métrica gerada a cada minuto. Unidade: Contagem Dimensões: ThrottledAt

Métrica	Descrição
<code>Gateway.DataProcessor.MeasurementRejected</code> (não disponível em gateways V3 habilitados para MQTT)	O número de medições que foram rejeitadas. Métrica gerada a cada minuto. Unidade: Contagem Dimensões: Reason
<code>Gateway.DataProcessor.MessagesRemaining</code> (não disponível em gateways V3 habilitados para MQTT)	O número de mensagens restantes em um fluxo. Métrica gerada a cada minuto. Unidade: Contagem Dimensões: StreamName
<code>Gateway.DataProcessor.ProcessingError</code> (não disponível em gateways V3 habilitados para MQTT)	O número de erros de processamento. Métrica gerada a cada minuto. Unidade: Contagem Dimensões: Reason

Registre 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 uma trilha é criada no console, a mesma é aplicada a todas as regiões da AWS. 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 obter 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 o seguinte:

- 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 uma função 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). 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. Selecione Eventos de dados para registrar eventos de dados em log.
 2. Em Tipo de evento de dados, escolha o tipo de recurso para o qual você deseja registrar eventos de dados em log.
 3. Selecione o modelo de seletor de logs que deseja usar. Você pode registrar todos os eventos de dados para o tipo de recurso, registrar todos os eventos `readOnly`, registrar todos os eventos `writeOnly` ou criar um modelo de seletor de logs personalizado para filtrar os campos `readOnly`, `eventName` e `resources.ARN`.
- 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](#)). É possível adicionar condições para filtrar os valores dos campos `readOnly`, `eventName` e `resources.ARN`.
 - Para configurar uma trilha para registrar eventos de dados, execute o [AWS CloudTrail put-event-selectors](#) comando. Para ter mais informações, consulte [Logging data events for trails with the AWS CLI](#).
 - Para configurar um armazenamento de dados de eventos para registrar eventos de dados, execute o [AWS CloudTrail create-event-data-store](#) comando para criar um novo armazenamento de dados de eventos para registrar eventos de dados ou execute o [AWS CloudTrail update-event-data-store](#) comando para atualizar um armazenamento de dados de eventos existente. Para ter mais informações, consulte [Registrar em log eventos de dados para armazenamentos de dados de eventos com a AWS CLI](#).

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 o `awscli` ou `awscli` CloudTrail APIs. A CloudTrail coluna Dados APIs registrados em mostra as chamadas de API registradas CloudTrail para o tipo de recurso.

Tipo de evento de dados (console)	valor <code>resources.type</code>	Dados APIs registrados em * CloudTrail
AWS IoT SiteWise asset	<code>AWS::IoTSiteWise::Asset</code>	• BatchPutAssetPropertyValues • GetAssetPropertyValue • GetAssetPropertyValueHistory • GetAssetPropertyAggregates • GetInterpolatedAssetPropertyValues • BatchGetAssetPropertyValues • BatchGetAssetPropertyValueHistory • BatchGetAssetPropertyAggregates
AWS IoT SiteWise séries temporais	<code>AWS::IoTSiteWise::TimeSeries</code>	• BatchPutAssetPropertyValues • GetAssetPropertyValue • GetAssetPropertyValueHistory • GetAssetPropertyAggregates • GetInterpolatedAssetPropertyValues

Tipo de evento de dados (console)	valor resources.type	Dados APIs registrados em * CloudTrail
		• BatchGetAssetProperty • BatchGetAssetPropertyHistory • BatchGetAssetPropertyAggregates
AWS IoT SiteWise Assistente	AWS::SitewiseAssistant::Conversation	• InvokeAssistant

Note

O resources.type registrado em log no evento do CloudTrail depende do identificador usado na solicitação de API. Se um ID de ativo for especificado na solicitação, o Asset resources.type será registrado, caso contrário, o TimeSeries resources.type será registrado.

*É possível configurar seletores de eventos avançados para filtrar os campos eventName, readOnly e resources.ARN e registrar em log somente os eventos que são importantes para você. Para obter mais informações sobre esses campos, consulte [AdvancedFieldSelector](#).

AWS IoT SiteWise eventos de gerenciamento em CloudTrail

O [registro de eventos de](#) gerenciamento fornece informações sobre as operações de gerenciamento que são realizadas nos recursos AWS da sua conta. Também são conhecidas como operações de ambiente de gerenciamento. 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-bbbbbbEXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
```

Marque seus AWS IoT SiteWise recursos

Marcar seus AWS IoT SiteWise recursos fornece uma maneira poderosa de categorizar, gerenciar e recuperar ativos organizacionais com eficiência. Ao atribuir etiquetas, que consistem em pares de chave/valor, você pode anexar metadados descritivos aos recursos. Os metadados das etiquetas podem ser usados para simplificar as operações. Por exemplo, em um cenário de parque eólico, as etiquetas permitem identificar turbinas com atributos específicos, como localização, capacidade e status operacional, permitindo rápida identificação e gerenciamento dentro do 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 somente usuários com determinadas etiquetas. Por exemplo, somente aqueles que estiverem marcados com determinado perfil ou departamento poderão acessar ou modificar recursos específicos.

Use 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 etiqueta consiste em uma chave e um valor opcional definidos por você. Por exemplo, você pode estabelecer uma série de etiquetas para os modelos de ativo a fim de rastreá-los de acordo com os processos industriais aos quais oferecem suporte. É recomendável desenvolver um conjunto personalizado de chaves de etiqueta para cada tipo de recurso que você gerencia. Usar um conjunto consistente de chaves de etiqueta facilita o gerenciamento dos recursos.

Marque 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 [Introdução ao Editor de tags](#) no Guia do usuário dos AWS Recursos de marcação e do editor de tags.

Marque com a AWS IoT SiteWise API

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 [TagResource](#) operação.
- Para remover tags de um recurso, use a [UntagResource](#) operação.
- Para recuperar as tags associadas a um recurso, use a [ListTagsForResource](#) operação 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 operações correspondentes.

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 etiquetas de um recurso a qualquer momento. Para atualizar o valor de uma chave de etiqueta existente, adicione uma nova etiqueta com a mesma chave e o novo valor desejado ao recurso. Essa ação substitui o valor anterior pelo novo. Embora seja possível atribuir uma string vazia como valor de etiqueta, você não pode atribuir um valor nulo.

A exclusão de um recurso também remove todas as etiquetas vinculadas a ele.

Usar etiquetas com políticas do IAM

Use etiquetas de recurso nas políticas do IAM para controlar o acesso e as permissões dos usuários. Por exemplo, as políticas podem permitir que os usuários criem somente os recursos que tenham uma etiqueta específica. 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 poderá ignorar as restrições e obter acesso a um recurso ao modificar as etiquetas.

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 [PutLoggingOptions](#) porque 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

- [Visualize AWS IoT SiteWise ativos com base em tags](#)

Solução de problemas AWS IoT SiteWise

Use as informações a seguir para solucionar problemas com AWS IoT SiteWise.

Tópicos

- [Solução de problemas de um gateway SiteWise Edge](#)
- [Solucionar problemas em um portal AWS IoT SiteWise](#)
- [Solucionar problemas de uma ação de AWS IoT SiteWise regra](#)
- [Solucionar problemas em operações de importação e exportação em massa](#)

Solução de problemas de um gateway SiteWise Edge

Solucione problemas comuns do AWS IoT SiteWise Edge Gateway explorando tópicos relevantes.

Você também pode visualizar CloudWatch as métricas relatadas pelos seus gateways do SiteWise Edge para solucionar problemas de conectividade ou fluxos de dados. Para obter mais informações, consulte [Monitore AWS IoT SiteWise com CloudWatch métricas da Amazon](#).

Tópicos

- [Configurar e acessar os registros SiteWise do gateway Edge](#)
- [Solução de problemas SiteWise do Edge Gateway](#)
- [Solução de problemas do aplicativo AWS IoT SiteWise Edge em Siemens Industrial Edge](#)
- [Solução de problemas de integrações de código aberto no Edge](#)
- [Solução de AWS IoT Greengrass problemas](#)

Configurar e acessar os registros SiteWise do gateway Edge

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 obter mais informações, consulte [Use 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 obter mais informações, consulte [Use os registros de serviço AWS IoT SiteWise](#).

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](#)
- [AWS IoT SiteWise não recebe dados dos servidores OPC UA](#)
- [Nenhum dado é mostrado no painel](#)
- [“Não foi possível encontrar ou carregar a classe principal” que aparece no aws.iot.SiteWiseEdgePublisher registra em//greengrass/v2/logerror](#)
- [Eu vejo 'SESSION_TAKEN_OVER' ou 'com.aws.greengrass.mqttclient. MqttClient: Falha ao publicar a mensagem via Spooler e tentarei novamente. ' nos logs](#)
- [Eu vejo 'com.aws.greengrass.deployment. lotJobsHelper: Nenhum trabalho de implantação encontrado. ' ou “Resultado da implantação já relatado.” nos logs](#)
- [Eu vejo um status 'SYNC_FAILED' ao tentar definir a configuração de timestamp em um grupo de propriedades em uma fonte de dados OPC UA](#)
- [Os tipos de dados convertidos não estão incluídos](#)
- [Problemas com a Trust Store](#)
- [Problemas de instalação habilitada para proxy](#)

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.

Para atualizar 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 a um 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 ativo. Para obter mais informações, consulte [Gerencie fluxos de dados para AWS IoT SiteWise](#).

Se você já mapeou todas as variáveis OPC UA que deseja inserir AWS IoT SiteWise, você pode filtrar quais variáveis OPC UA o gateway SiteWise Edge envia. Para obter mais informações, consulte [Use filtros de nó OPC UA no SiteWise Edge](#).

- **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 OPC UA tiver um tipo de

dados inteiro, a propriedade de ativo correspondente deverá ser do tipo de dados inteiro. Uma propriedade de ativo do 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.
- **ThrottlingException** ou **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 é 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 dessincronizadas, a atualização do nome da fonte de dados pode acelerar a sincronização da nuvem com a borda, corrigindo o erro de assincronia.

Como atualizar o nome de uma fonte de dados

1. Navegue até o [console do AWS IoT SiteWise](#).
2. No painel de navegação, escolha Gateways de borda.
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/logerror`

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 mode)
```

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 [Alterar a versão dos pacotes de componentes do SiteWise Edge Gateway](#).

Eu vejo 'SESSION_TAKEN_OVER' ou 'com.aws.greengrass.mqttclient. MqttClient: Falha ao publicar a mensagem via Spooler e tentarei novamente. ' nos logs

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 à sua AWS conta.

Eu vejo 'com.aws.greengrass.deployment. IotJobsHelper: Nenhum trabalho de implantação encontrado. ' ou "Resultado da implantação já relatado." nos logs

Se vir com.aws.greengrass.deployment.IotJobsHelper: No deployment job found. ou Deployment result already reported. nos logs em /greengrass/v2/logs/greengrass.log, talvez você esteja tentando reutilizar o mesmo arquivo de configuração.

Existem 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, escolha Gateways de borda.
3. Escolha o gateway SiteWise Edge que você deseja reutilizar.
4. Escolha a guia Atualizações.
5. Selecione uma versão diferente do publicador e escolha Implantar.

Siga as etapas em [Criar um gateway para o Siemens Industrial Edge](#) para criar outro arquivo de configuração.

Eu vejo um status 'SYNC_FAILED' ao tentar definir a configuração de timestamp em um grupo de propriedades em uma fonte de dados OPC UA

Quando AWS IoT SiteWise atualizamos o componente coletor OPC UA para AWS IoT Greengrass a versão 2.5.0, introduzimos uma nova opção de configuração de timestamp. Você pode usar o timestamp do seu dispositivo ou o timestamp do servidor. Versões mais antigas do componente coletor OPC UA não suportam essa opção e falham na sincronização.

Há duas maneiras de resolver uma falha no status de sincronização da fonte de dados. A forma recomendada é atualizar o componente coletor IoT SiteWise OPC UA para a versão 2.5.0 ou superior. Como alternativa, você pode continuar usando a versão mais antiga do componente coletor OPC UA, se você definir o timestamp como. Source Para saber como atualizar o componente coletor do IoT SiteWise OPC UA, consulte. [Atualizar a versão de um AWS IoT SiteWise componente](#) Recomendamos usar as versões mais recentes de todos os componentes.

Note

Não há interrupção de dados quando o status de sincronização da fonte de dados falha. Os dados de origem continuam fluindo para dentro AWS IoT SiteWise. A configuração simplesmente não está sincronizando com o componente coletor SiteWise IoT OPC UA em sua implantação. AWS IoT Greengrass V2

Para alterar a configuração do timestamp de um grupo de propriedades

1. Navegue até o [console do AWS IoT SiteWise](#).
2. No painel de navegação, escolha Gateways de borda.
3. Selecione o gateway a ser editado.

4. Na seção Fontes de dados, selecione a fonte de dados com o status de falha na sincronização e escolha Editar.
5. Expanda Configuração avançada e, em seguida, expanda Configurações de grupo.
6. Em Timestamp, selecione Origem. Selecionar Fonte remove a `timestampToReturn` propriedade da configuração. Essa configuração permite a coleta do timestamp da fonte de dados do seu dispositivo por padrão, permitindo que a fonte de dados seja sincronizada com o componente coletor IoT SiteWise OPC UA.
7. Escolha Salvar.

Os tipos de dados convertidos não estão incluídos

Se você ver um erro ao converter tipos de dados OPC UA não suportados em cadeias de caracteres AWS IoT SiteWise, há alguns motivos possíveis:

- O tipo de dados que você está tentando converter é um tipo de dados complexo. Os tipos de dados complexos não são compatíveis.
- Ao usar Destinos como AWS IoT SiteWise armazenado em buffer usando o Amazon S3, o valor completo da string é preservado nos arquivos enviados a um bucket do Amazon S3. Quando você ingere dados posteriormente AWS IoT SiteWise, valores completos de cadeia de caracteres maiores que 1024 bytes são rejeitados.

Problemas com a Trust Store

Se você encontrar problemas relacionados a lojas confiáveis no SiteWise Edge, considere as seguintes etapas de solução de problemas:

- Verifique se o certificado CA AWS IoT Greengrass raiz está presente e formatado corretamente nos repositórios confiáveis apropriados
- Certifique-se de que a KeyStore senha Java esteja corretamente definida e acessível aos componentes do SiteWise Edge
- Verifique se todos os certificados personalizados (como para proxies HTTPS) estão no formato correto (normalmente PEM) e foram importados corretamente para os repositórios confiáveis
- Confirme se os repositórios confiáveis têm as permissões de arquivo corretas e estão acessíveis aos processos do SiteWise Edge

- Revise os registros do SiteWise Edge em busca de erros SSL/TLS relacionados, o que pode indicar problemas no armazenamento confiável
- Teste SSL/TLS as conexões de forma independente usando ferramentas como `openssl` verificar a funcionalidade do armazenamento confiável

Problemas de instalação habilitada para proxy

Se você encontrar problemas durante o processo de configuração do proxy, considere as seguintes etapas de solução de problemas:

- Verifique se o URL do proxy está formatado corretamente e inclui o esquema adequado (`http://` ou `https://`)
- Certifique-se de que todas as credenciais de proxy sejam codificadas em URL se contiverem caracteres especiais
- Confirme se a lista sem proxy inclui todos os endereços locais e endpoints de AWS serviço necessários
- Para proxies HTTPS, verifique se o certificado CA fornecido está no formato PEM
- Verifique os registros de instalação em busca de mensagens de erro específicas que possam indicar a origem do problema
- Teste a conexão proxy de forma independente para garantir que ela esteja funcionando corretamente

Solução de problemas do aplicativo AWS IoT SiteWise Edge em Siemens Industrial Edge

Para solucionar problemas do aplicativo AWS IoT SiteWise Edge em seu Siemens Industrial Edge dispositivo, você pode acessar os registros do aplicativo por meio dos portais Siemens Industrial Edge Management ou do Siemens Industrial Edge dispositivo (IED). Para ter mais informações, consulte [Downloading Logs](#) na documentação da Siemens.

Meus dados não são exibidos em AWS IoT SiteWise

- Garanta que não haja problemas com os usuários do Databus e que o ícone de marca de seleção de `Databus_Configuration` está verde em vez de cinza.

- Talvez você não esteja executando o Siemens Industrial Edge Management em uma versão que contém Secure Storage. Atualize a versão do sistema operacional da Siemens. Para obter mais informações, consulte [Siemens Secure Storage e o aplicativo AWS IoT SiteWise Edge](#).

Vejo “Arquivo de configuração ausente AWS_REGION” nos registros

Se você vir `Config file missing AWS_REGION` nos logs da Siemens, o JSON do arquivo de configuração terá sido corrompido. Você precisará criar outro arquivo de configuração. Siga as etapas em [Criar um gateway para o Siemens Industrial Edge](#) para criar outro arquivo de configuração.

Eu vejo uma mensagem de erro “Fora de sincronização” na configuração do gateway Edge

Se você ver uma mensagem de `Out of sync` erro em seu Siemens Industrial Edge gateway após a conclusão da implantação, isso significa que o componente do SiteWise editor de IoT está fora de sincronia com seu gateway. O componente do SiteWise editor de IoT funciona em segundo plano nos Siemens Industrial Edge gateways para fornecer a funcionalidade de tópicos do MQTT. Atualizamos os Siemens Industrial Edge gateways para usar o namespace `iotsitewise:publisher:3` de recursos em vez de `iotsitewise:publisher:2`. Você pode atualizar para a versão mais recente do editor para resolver esse problema.

Para atualizar para a versão mais recente do editor de IoT SiteWise

1. Navegue até o [console do AWS IoT SiteWise](#).
2. No painel de navegação, escolha Gateways de borda.
3. Selecione o Siemens Industrial Edge gateway a ser editado.
4. Na seção Capacidades do Edge, selecione Exibir versões do software.
5. Selecione a versão mais recente do SiteWise editor de IoT no menu suspenso Editor.
6. Selecione Concluído.

Solução de problemas de integrações de código aberto no Edge

Esta seção fornece soluções para problemas comuns que você pode encontrar ao integrar ferramentas de código aberto com SiteWise o Edge.

 Note

Node-RED®, InfluxDB® e Grafana® não são fornecedores ou fornecedores do Edge SiteWise

Problemas de conexão

O Node-RED não consegue se conectar ao corretor MQTT

Verifique se o agente MQTT está em execução e acessível na porta especificada. Verifique sua configuração de rede e certifique-se de que o endereço do agente esteja correto.

Para verificar o status do agente MQTT, execute:

```
docker ps | grep emqx
```

Erros de conexão do InfluxDB

Verifique se o token de autenticação é válido e se você especificou os nomes corretos da organização e do bucket. Verifique se o InfluxDB está em execução e acessível.

Para verificar o status do InfluxDB, execute:

```
curl -I http://localhost:8086
```

Grafana não consegue se conectar ao InfluxDB

Verifique se a configuração da fonte de dados do InfluxDB no Grafana está correta, incluindo o URL, o token de autenticação, a organização e o bucket.

Problemas de fluxo de dados

Nenhum dado aparece em AWS IoT SiteWise

Verifique se o alias de sua propriedade no fluxo do Node-RED corresponde ao formato esperado. Verifique se a estrutura de tópicos do MQTT está correta e se o gateway SiteWise Edge está configurado corretamente para receber dados do agente do MQTT.

Nenhum dado SiteWise do Edge armazenado no InfluxDB

Verifique se o fluxo de retenção do Node-RED está configurado corretamente e se o nó gravador do InfluxDB tem as configurações adequadas de bucket e medição. Verifique se há erros na saída de depuração do Node-RED.

Erros de formato de dados

Certifique-se de que suas funções de transformação de dados convertam corretamente os dados entre formatos. Use os nós de depuração Node-RED para inspecionar os dados em cada estágio do fluxo.

Problemas de desempenho

Alto uso de CPU ou memória

Monitore o uso de recursos e ajuste a configuração de seus componentes conforme necessário. Considere reduzir a frequência de coleta de dados ou implementar a filtragem de dados para reduzir a carga de processamento.

Para monitorar o uso de recursos, execute:

```
docker stats
```

Carregamento lento do painel do Grafana

Otimize suas consultas do InfluxDB e considere adicionar limitações de intervalo de tempo aos painéis do painel. Reduza o número de pontos de dados exibidos usando as funções de agregação apropriadas.

Registro e diagnóstico

Para solucionar problemas, verifique os registros de cada componente:

Registros do Node-RED

Visualize os registros no console do Node-RED ou execute:

```
docker logs node-red
```

Registros do InfluxDB

Acesse os registros executando:

```
docker logs influxdb
```

Registros da Grafana

Visualize os registros executando:

```
docker logs grafana
```

SiteWise Troncos Edge

Verifique os registros do gateway SiteWise Edge quanto a problemas de conexão e processamento de dados com o MQTT. Para obter mais informações, consulte [Solução de problemas de um gateway SiteWise Edge](#).

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.

Solucionar problemas em um portal AWS IoT SiteWise

Solucione problemas comuns com seus AWS IoT SiteWise portais.

Usuários e administradores não podem acessar o portal do 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.

Solucionar 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

- [Configurar AWS IoT Core registros](#)
- [Configurar uma ação de erro na republicação](#)
- [Solucionar problemas em regras](#)
- [Solucionar problemas em uma regra \(AWS IoT SiteWise\)](#)
- [Solucionar problemas em uma regra \(DynamoDB\)](#)

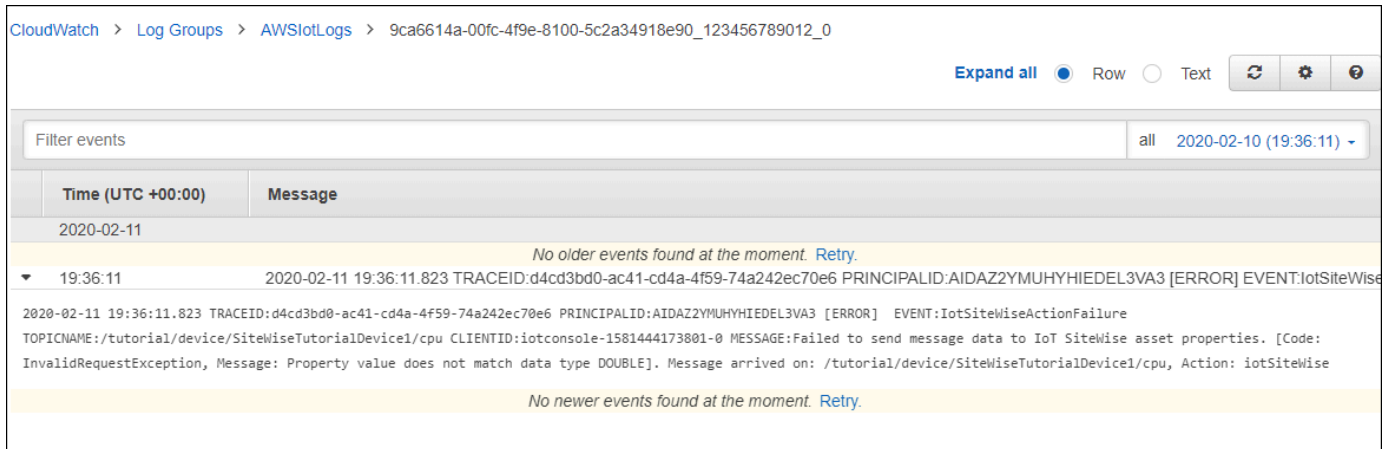
Configurar AWS IoT Core registros

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 grupo AWSIoTRegistros.
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 na 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.

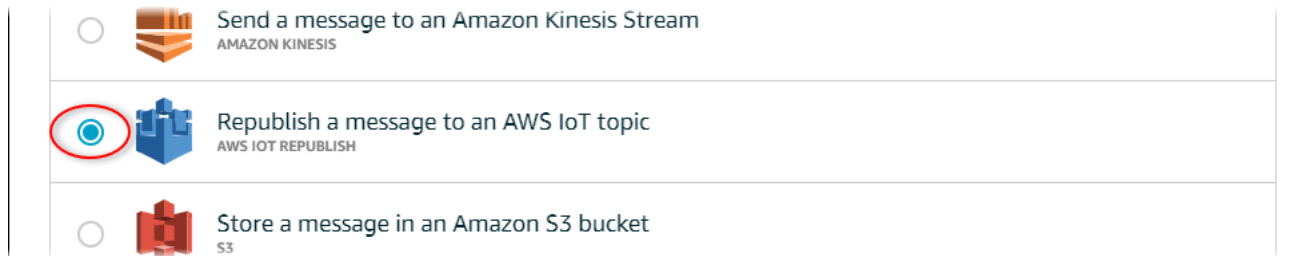
Note

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

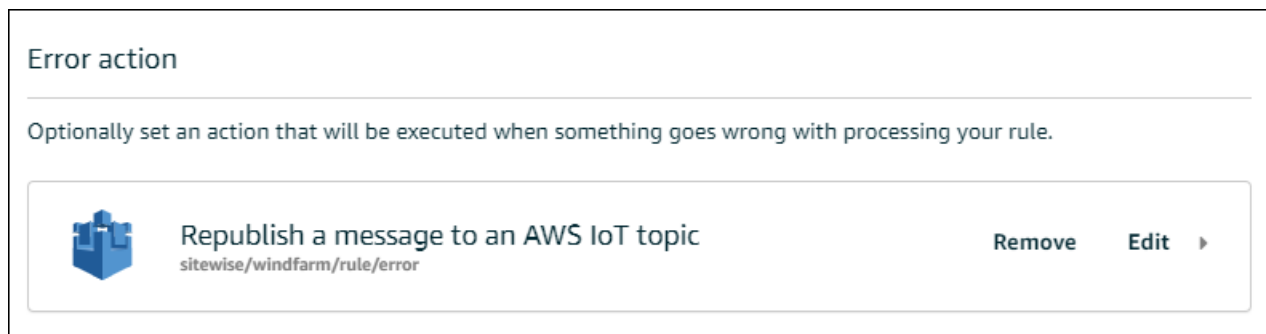
1. Navegue até o [console do AWS IoT](#).
2. No painel de navegação esquerdo, escolha Agir e Regras.
3. Selecione a regra.
4. Em Error action (Ação de erro), escolha Add action (Adicionar ação).

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.

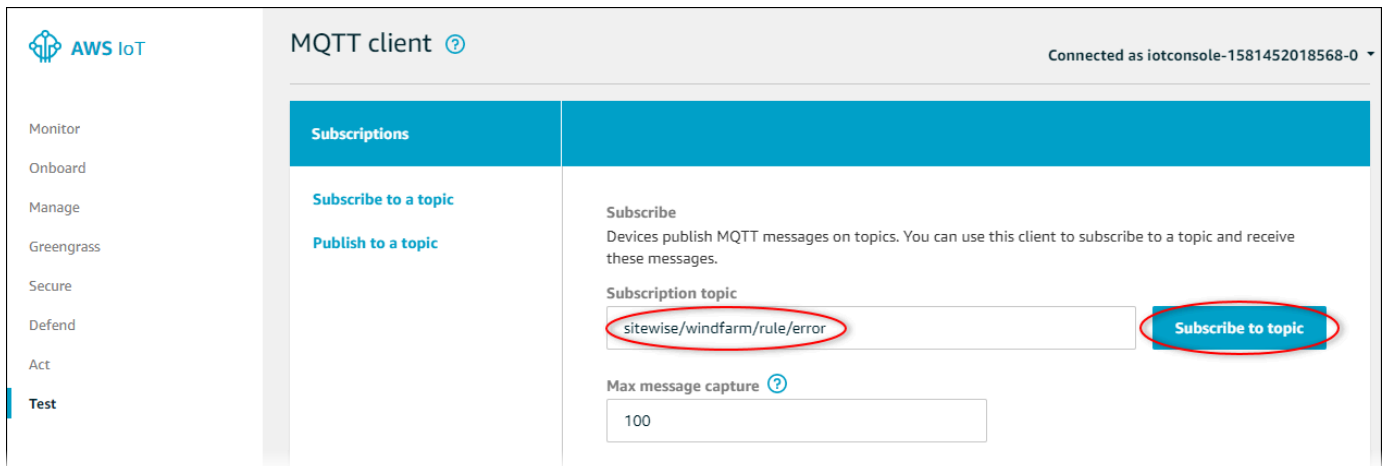
Depois de configurar a ação de erro de republicação, você pode visualizar as mensagens de erro no cliente de teste MQTT no AWS IoT Core.

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).



The screenshot shows the AWS IoT MQTT client interface. On the left is a navigation menu with options: Monitor, Onboard, Manage, Greengrass, Secure, Defend, Act, and Test. The main area is titled 'MQTT client' and shows a 'Subscriptions' section. Under 'Subscriptions', there are links for 'Subscribe to a topic' and 'Publish to a topic'. The 'Subscribe' section contains a text input field for 'Subscription topic' with the value 'sitewise/windfarm/rule/error' and a blue 'Subscribe to topic' button. Below this is a 'Max message capture' field with the value '100'. The interface is connected as 'iotconsole-1581452018568-0'.

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.

Solucionar problemas em regras

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 se 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 obter mais informações, consulte [Gerencie fluxos de dados para AWS IoT SiteWise](#).
- 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 obter mais informações, consulte [AWS IoT Conceda 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 em uma regra (AWS IoT SiteWise)

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 obter mais informações, consulte [Solucionar 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. Selecione 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 [Solucionar 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.

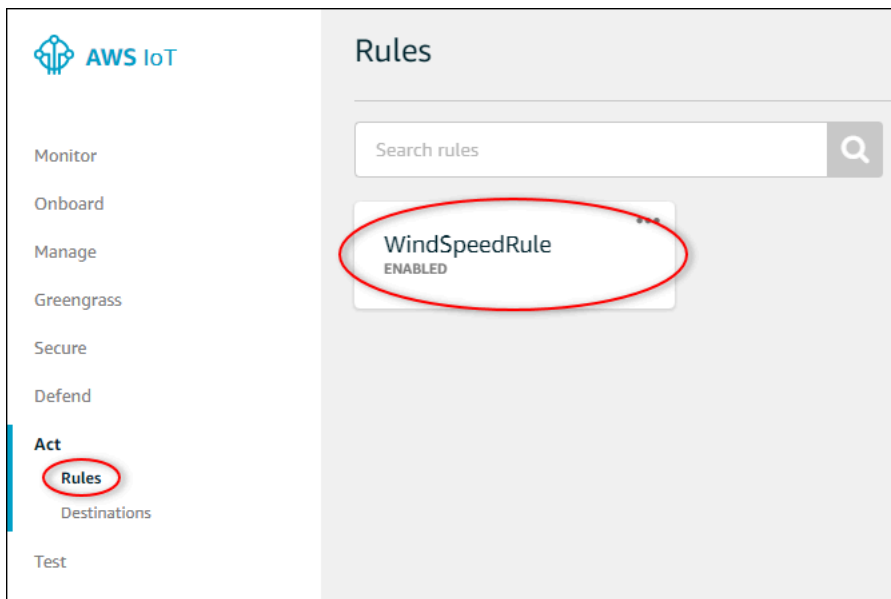
```
$aws/things/+/shadow/update/accepted
```

Solucionar problemas em uma regra (DynamoDB)

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.

☐		Send a message to an Amazon Kinesis Stream AMAZON KINESIS
☒		Republish a message to an AWS IoT topic AWS IOT REPUBLISH
☐		Store a message in an Amazon S3 bucket S3

- Escolha Configurar ação na parte inferior da página.
- Em Tópico, insira **windspeed/error**. AWS IoT O Core republicará as mensagens de erro neste tópico.

Configure action

 Republish a message to an AWS IoT topic
AWS IOT REPUBLISH

This action will republish the message to another AWS IoT topic.

*Topic 

windspeed/error

Quality of Service 

☒ 0 - The message is delivered zero or more times.

☐ 1 - The message is delivered one or more times.

Choose or create a role to grant AWS IoT access to perform this action.

No role selected

Create Role

Select

Cancel

Add action

- Escolha Selecionar para conceder acesso ao AWS IoT Core para executar a ação de erro usando a função que você criou anteriormente.
- Escolha Select (Selecionar) ao lado da função.

Choose or create a role to grant AWS IoT access to perform this action.

No role selected	Refresh	Create Role	Close
Search for IAM roles			
WindSpeedDataRole			Select

10. Escolha Update Role (Atualizar função) para adicionar outras permissões à função.

1 - The message is delivered one or more times.

Choose or create a role to grant AWS IoT access to perform this action.

WindSpeedDataRole	Update Role	Create Role	Select

Cancel

Add action

11. Escolha Add action (Adicionar ação) para concluir a adição da ação de erro.

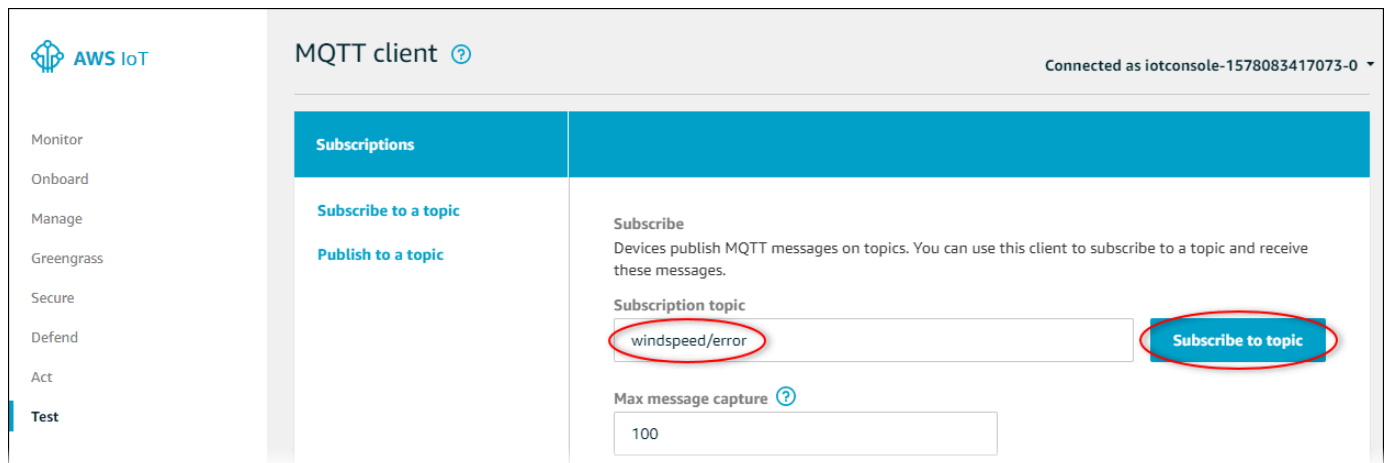
12. Escolha a seta para trás no canto superior esquerdo do console para retornar à página inicial do console AWS IoT Core.

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 e a propriedade IDs atualizados do ativo.

Solucionar problemas em 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 [MetadataTransferJobProgress](#) objeto.
4. 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 transferidos com êxito no 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 de API, que contém um URL pré-assinado. Se o trabalho de transferência tiver erros que precisem ser investigados, você poderá fazer download de um relatório de erros completo neste URL.

AWS IoT SiteWise endpoints e cotas

As seções a seguir descrevem os endpoints e as cotas para AWS IoT SiteWise

Tópicos

- [AWS IoT SiteWise endpoints](#)
- [AWS IoT SiteWise cotas](#)

AWS IoT SiteWise endpoints

O Referência geral da AWS Guia lista os AWS IoT SiteWise endpoints de um Conta da AWS. Para ter mais informações, consulte [AWS IoT SiteWise endpoints and quotas](#) no Guia de Referência geral 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 AWS IoT SiteWise ativos e modelos de ativos

Recurso	Descrição	Quota	Ajustável
Número de modelos de ativos em cada um Região da AWS para cada Conta da AWS	O número máximo de modelos de ativos que você pode criar em um Região da AWS para um Conta da AWS.	1000	Sim
Número de ativos em cada modelo de ativo	O número máximo de ativos que você pode criar para cada modelo de ativo.	10.000	Sim

Recurso	Descrição	Quota	Ajustável
Número de ativos infantis em cada ativo dos pais	O número máximo de ativos secundários que você pode associar a um ativo principal.	2000	Sim
Profundidade da árvore hierárquica de ativos	A profundidade máxima da árvore da hierarquia de ativos para um modelo de ativo.	30	Sim
Número de definições de hierarquia em cada modelo de ativo	O número máximo de definições de hierarquia que você pode ter em um modelo de ativo.	30	Yes
Número de propriedades no nível raiz em cada modelo de ativo	O número máximo de <code>assetModelProperties</code> para cada modelo de ativo. Essa contagem não inclui <code>compositeModelProperties</code> . Essa cota também se aplica a qualquer ativo exclusivo criado com base nesse modelo de ativo.	500	Sim

Recurso	Descrição	Quota	Ajustável
Número de propriedades em um modelo de ativo	O número máximo de propriedades de um modelo de ativo do tipo <code>ASSET_MODEL</code> ou <code>COMPONENT_MODEL</code> . 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 com base nesse modelo de ativo.	5000	Sim
Número de propriedades em cada modelo composto	O número máximo de propriedades permitido para modelos compostos. Além disso, o número máximo de propriedades permitido para um modelo de ativo do tipo <code>COMPONENT_MODEL</code> .	100	Sim

Recurso	Descrição	Quota	Ajustável
Profundidade da árvore de propriedades em um modelo de ativo	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.	10	Não
Número de modelos de ativos em cada árvore hierárquica	O número máximo de modelos de ativos que você pode incluir em uma única árvore hierárquica.	100	Sim

Recurso	Descrição	Quota	Ajustável
Número de propriedades diretamente dependentes de um modelo de ativo	Essa cota limita quantas propriedades podem depender diretamente de uma única propriedade, conforme definido nas expressões de fórmula de propriedade. O número de propriedades diretamente dependentes deve ser maior que o número de propriedades diretamente dependentes de um modelo de ativo. Solicite um aumento para ambas as cotas se houver mais propriedades diretamente dependentes do que propriedades dependentes para um modelo de ativo.	20	Sim

Recurso	Descrição	Quota	Ajustável
Número de propriedades dependentes em um modelo de ativo	Essa cota limita quantas propriedades podem depender direta ou indiretamente de uma única propriedade, conforme definido nas expressões de fórmula de propriedade.	30	Não
Número de modelos compostos em um modelo de ativo	O número máximo de modelos compostos que você pode ter em um único modelo de ativo.	50	Sim
Profundidade de modelos compostos	A profundidade máxima da árvore do modelo composto em cada modelo de ativo, incluindo modelos em linha e component-model-based compostos.	2	Sim

Recurso	Descrição	Quota	Ajustável
Número de modelos de ativo exclusivos que usam o mesmo modelo de componente	O número máximo de modelos de ativos exclusivos que têm pelo menos um modelo component-model-based composto que faz referência direta a um modelo de ativo específico do tipo COMPONENT_MODEL.	20	Sim
Número de variáveis de propriedade em uma expressão de fórmula de propriedade	Por exemplo, há duas variáveis de propriedade power e temp, na expressão <code>avg(power) + max(temp)</code> . Isso também se aplica aos resultados da computação de transformação.	10	Não
Número de funções em uma expressão de fórmula de propriedade	Por exemplo, há duas funções, avg e max, na expressão <code>avg(power) + max(temp)</code> .	10	Não

Cotas para dados de propriedades AWS IoT SiteWise de ativos

Recurso	Descrição	Quota	Ajustável
Taxa de solicitação para operações de API de dados de propriedade de ativos	O número máximo de solicitações da API de dados de propriedades de ativos a cada segundo que você pode realizar Região da AWS em cada uma delas Conta da AWS. Essa cota se aplica a operações de API, como GetAssetProperty e BatchPutAssetProperty.	1000	Sim
Número de pontos de dados por segundo para cada qualidade de dados para cada propriedade do ativo	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 para cada qualidade de dados de cada propriedade do ativo. Você pode armazenar até esse número de pontos de dados de boa qualidade, de qualidade incerta, e	10	Não

Recurso	Descrição	Quota	Ajustável
	de baixa qualidade a qualquer segundo para cada propriedade do ativo.		
Número de BatchPutAssetPropertyValues entradas ingeridas a cada segundo em cada propriedade do ativo para cada uma Região da AWS para um Conta da AWS.	O número máximo de entradas em cada propriedade do ativo BatchPutAssetPropertyValues de todas as fontes, incluindo gateways, AWS IoT Core regras e chamadas de API do SiteWise Edge.	10	Não
Taxa de pontos de dados ingeridos	O número máximo de pontos de dados timestamp-quality-value (TQV) ingeridos por segundo em cada um Região da AWS para um. Conta da AWS	5000	Sim

Recurso	Descrição	Quota	Ajustável
Taxa de solicitações para BatchGetAssessmentPropertyAggregates	O número máximo de BatchGetAssessmentPropertyAggregates solicitações por segundo que você pode realizar Região da AWS em cada uma delas Conta da AWS.	200	Sim
Taxa de solicitações para BatchGetAssessmentPropertyValue	O número máximo de BatchGetAssessmentPropertyValue solicitações por segundo que você pode realizar Região da AWS em cada uma delas Conta da AWS.	500	Sim
Taxa de solicitações para BatchGetAssessmentPropertyValueHistory	O número máximo de BatchGetAssessmentPropertyValueHistory solicitações a cada segundo que você pode realizar.	200	Sim

Recurso	Descrição	Quota	Ajustável
Número de BatchPutAssetPropertyValues entradas ingeridas a cada segundo para cada propriedade do ativo Região da AWS em um Conta da AWS.	Essa cota se aplica às entradas em cada propriedade do ativo BatchPutAssetPropertyValues de todas as fontes, incluindo gateways, AWS IoT Core regras e chamadas de API do SiteWise Edge.	10	Não
Taxa de GetAssetPropertyAggregates solicitações e consultas BatchGetAssetPropertyAggregates de entrada para cada propriedade do ativo	O número máximo de GetAssetPropertyAggregates solicitações e BatchGetAssetPropertyAggregates entradas totais para cada propriedade do ativo por segundo Região da AWS em cada uma Conta da AWS.	50	Não

Recurso	Descrição	Quota	Ajustável
Taxa de GetAssetPropertyValue solicitações e consultas BatchGetAssetPropertyValue de entrada para cada propriedade do ativo	O número máximo de GetAssetPropertyValue solicitações e BatchGetAssetPropertyValue entradas totais para cada propriedade do ativo a cada segundo Região da AWS em cada uma Conta da AWS.	500	Não
Taxa de GetAssetPropertyValueHistory solicitações e consultas BatchGetAssetPropertyValueHistory de entrada para cada propriedade do ativo	O número máximo de GetAssetPropertyValueHistory solicitações e BatchGetAssetPropertyValueHistory entradas totais para cada propriedade do ativo a cada segundo Região da AWS em cada uma Conta da AWS.	30	Não

Recurso	Descrição	Quota	Ajustável
Taxa de solicitações GetInterpolatedAssetPropertyValues	O número máximo de GetInterpolatedAssetPropertyValues solicitações por segundo que você pode realizar Região da AWS em cada uma delas Conta da AWS.	500	Sim
Número de resultados em cada GetInterpolatedAssetPropertyValues solicitação	O número máximo de resultados a serem retornados para uma solicitação paginada. GetInterpolatedAssetPropertyValues	10	Sim

Recurso	Descrição	Quota	Ajustável
Taxa de pontos de dados recuperados de e GetAssetPropertyValueHistory e BatchGetAssetPropertyHistory	A taxa máxima de bytes (MB/segundo) dos pontos de dados recuperados a cada segundo para cada um em um ponto e. Região da AWS Conta da AWS GetAssetPropertyValueHistory e BatchGetAssetPropertyHistory A carga de resposta avaliada para essa cota usa campos Timestamp-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. Timestamp-quality-value Os pontos de dados (TQV) recuperados a cada segundo variam para cada tipo de dados:	100	Sim

Recurso	Descrição	Quota	Ajustável
	- Número inteiro — até 5 milhões de TQV por segundo - Duplo — até 4 milhões de TQV por segundo - Booleano — 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	Descrição	Quota	Ajustável
Número de gateways SiteWise Edge em cada um Região da AWS para um Conta da AWS	O número máximo de gateways do SiteWise Edge que você pode criar em um Região da AWS para um Conta da AWS.	100	Sim
Número de fontes OPC UA em um gateway SiteWise Edge	O número máximo de fontes OPC UA que você pode configurar em um gateway SiteWise Edge.	100	Não
Número total de destinos em um	O número máximo de destinos que você pode configurar em	100	Não

Recurso	Descrição	Quota	Ajustável
gateway SiteWise Edge	um gateway SiteWise Edge.		

Cotas para AWS IoT SiteWise Monitor

Recurso	Descrição	Quota	Ajustável
Número de portais em cada um Região da AWS para um Conta da AWS	O número máximo de portais de SiteWise monitoramento que você pode criar em um Região da AWS para um Conta da AWS.	100	Sim
Número de projetos em um portal	O número máximo de projetos que você pode criar em um portal do SiteWise Monitor.	100	Sim
Número de painéis em um projeto	O número máximo de painéis que você pode criar em um projeto no SiteWise Monitor.	100	Sim
Número de ativos raiz em um projeto	O número máximo de ativos de nível superior que você pode adicionar a um projeto no SiteWise Monitor.	1	Não
Número de visualizações em um painel	O número máximo de elementos visuais	10	Sim

Recurso	Descrição	Quota	Ajustável
	(como tabelas, gráficos ou tabelas) que você pode adicionar a um painel no SiteWise Monitor.		
Número de métricas em cada visualização do painel	O número máximo de métricas ou pontos de dados que você pode exibir em uma única visualização em um painel no SiteWise Monitor.	5	Sim
Número de limites para cada visualização do painel	O número máximo de níveis de limite que você pode definir para cada visualização em um painel no SiteWise Monitor.	12	Não

Cotas para importação e exportação AWS IoT SiteWise em massa de metadados

Recurso	Descrição	Quota	Ajustável
Número de trabalhos de transferência de metadados na fila	O número máximo de trabalhos de transferência de metadados no estado PENDING na fila.	10	Sim
Tamanho do arquivo de importação do trabalho de transferência de metadados	O tamanho máximo do arquivo importado (em MB).	100	Sim

Recurso	Descrição	Quota	Ajustável
Número de recursos de AWS IoT SiteWise importação em uma tarefa	O número máximo de recursos de AWS IoT SiteWise importação em um único trabalho. Um recurso inclui ativos e modelos de ativo.	5000	Sim
Número de recursos de AWS IoT SiteWise exportação em um trabalho	O número máximo de recursos de AWS IoT SiteWise exportação em um único trabalho. Um recurso inclui ativos e modelos de ativo.	5000	Sim

Cotas para importação AWS IoT SiteWise em massa de dados

Recurso	Descrição	Quota	Ajustável
Número de trabalhos de importação em massa em execução	O número máximo de trabalhos de importação em massa que podem ser executados simultaneamente.	100	Não
Tamanho do arquivo CSV	O tamanho máximo do arquivo CSV (em GB) em uma tarefa de importação em massa.	10	Não

Recurso	Descrição	Quota	Ajustável
Tamanho do arquivo parquet não compactado	O tamanho máximo do arquivo (em MB) para um arquivo de parquet não compactado em um trabalho de importação em massa.	256 MB	Não
Tamanho do arquivo CSV para ingestão em buffer	O tamanho máximo do arquivo CSV (em MB) ao usar a ingestão em buffer em um trabalho de importação em massa.	256 MB	Não
Tamanho do grupo de linhas do parquet não compactado	O tamanho máximo de um grupo de linhas de parquet não compactado.	64 MB	Não
Número de medidas exclusivas em uma lima de parquet	O número máximo de medidas exclusivas em um arquivo de parquet.	10000	Não
Número de dias entre o carimbo de data/hora passado e hoje para ingestão armazenada em buffer	O número máximo de dias entre um carimbo de data/hora no passado e a data atual ao usar a ingestão em buffer.	30	Sim

Recurso	Descrição	Quota	Ajustável
Taxa de solicitação para cada um CreateBulkImportJobs Região da AWS em cada Conta da AWS		10	Sim
Taxa de solicitação ListBulkImportJobs para cada um Região da AWS em cada Conta da AWS		50	Sim
Taxa de solicitação DescribeBulkImportJobs para cada um Região da AWS em cada Conta da AWS		50	Sim

Cotas para limitação da API AWS IoT SiteWise Assistant

Cotas para limites de limitação da API AWS IoT SiteWise Assistant

Recurso	Descrição	Quota	Ajustável
Taxa de solicitação para InvokeAssistant operação	O número máximo de transações por minuto (TPM) que podem ser feitas na AWS IoT SiteWise InvokeAssistant API em um Conta da AWS. Os limites do TPM se	10	Não

Recurso	Descrição	Quota	Ajustável
	aplicam a todas as regiões suportadas e são ajustáveis em algumas regiões.		

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 ter mais informações, consulte [Quotas for using 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
Conecte aplicativos externos ao corretor EMQX com nomes de usuário e senhas	Foi adicionado suporte para conectar aplicativos externos usando nomes de usuário e senhas ao agente AWS IoT Greengrass EMQX, que é implantado por padrão ao criar um novo gateway V3 habilitado para MQTT.	1.º de maio de 2025
Support para gateways V3 habilitados para MQTT no Edge SiteWise	Novos recursos adicionados e conteúdo obsoleto removido • Foi adicionado suporte para gateways V3 habilitados para MQTT. Configuração de destino aprimorada usando filtros de caminho para assinar tópicos do MQTT, incluindo ingestão de dados em tempo real diretamente AWS IoT SiteWise ou ingestão de dados em buffer usando o Amazon S3. • Lançou a versão 3.0.0 do coletor SiteWise IoT OPC	26 de fevereiro de 2025

UA e a versão 4.0.0 do componente Editor de IoT para. SiteWise AWS IoT Greengrass V2

- A versão anterior dos gateways SiteWise Edge auto-hospedados foi renomeada para fluxos clássicos, gateways V2.
- As referências à AWS IoT Greengrass V1 documentação do SiteWise Edge foram removidas porque não há mais suporte para uso com AWS IoT SiteWise o.

[Suporte para AWS IoT SiteWise Assistant](#)

Foi adicionado suporte para o AWS IoT SiteWise Assistant - um assistente generativo alimentado por IA.

18 de novembro de 2024

[Foram adicionados tempos limite de sessão configuráveis para o Edge SiteWise APIs](#)

Foram adicionadas configurações de tempo limite de sessão configuráveis para gerenciar os períodos de inatividade do Edge. AWS OpsHub SiteWise APIs

31 de outubro de 2024

[Configurações de proxy configuráveis adicionadas para SiteWise o Edge APIs](#)

Foi adicionado o gerenciamento de informações do armazenamento confiável para habilitar o suporte de proxy HTTPS para gateways SiteWise Edge.

31 de outubro de 2024

<u>Habilite o CORS no Edge SiteWise APIs</u>	Foi adicionado suporte CORS para o SiteWise Edge APIs para permitir o acesso seguro a aplicativos web entre domínios.	30 de setembro de 2024
<u>Suporte a fontes de dados de parceiros do CloudRail e Litmus Edge</u>	Adição de suporte a fontes de dados de parceiros do CloudRail e do Litmus Edge.	5 de setembro de 2024
<u>Disponibilidade geral para executar o SiteWise Edge no Siemens Industrial Edge</u>	AWS IoT SiteWise agora suporta a disponibilidade geral da execução do SiteWise Edge em dispositivos Siemens Industrial Edge.	24 de julho de 2024
<u>Adição de suporte à configuração de carimbos de data/hora em fontes de dados OPC UA</u>	AWS IoT SiteWise agora suporta a configuração de timestamp para fontes de dados OPC UA.	24 de julho de 2024
<u>Adição de suporte à conversão do tipo de dados em fontes de dados OPC UA</u>	AWS IoT SiteWise agora suporta conversão de tipo de dados para tipos de dados OPC UA não suportados.	24 de julho de 2024
<u>Foi adicionado suporte para executar uma prévia do SiteWise Edge no Siemens Industrial Edge</u>	AWS IoT SiteWise agora suporta a execução de uma prévia do SiteWise Edge em dispositivos Siemens Industrial Edge.	26 de novembro de 2023

[Adição de suporte ao armazenamento de nível morno](#)

AWS IoT SiteWise agora oferece suporte ao armazenamento quente, um nível de armazenamento totalmente gerenciado que facilita para os clientes armazenar e acessar dados industriais com segurança.

15 de novembro de 2023

[Adição de suporte a identificadores exclusivos definidos pelo usuário](#)

AWS IoT SiteWise agora suporta o uso de identificadores exclusivos definidos pelo usuário para ativos, modelos de ativos, propriedades e hierarquias.

15 de novembro de 2023

[Adição de suporte à detecção de anomalias multivariadas em 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 equipamento com o Amazon Lookout for Equipment.

15 de novembro de 2023

[Adição de suporte à ingestão econômica e escalável de dados de séries temporais no 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

[Adição de suporte à 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

<u>Adição de suporte a componentes de modelos de ativo</u>	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
<u>Adição de suporte à aplicação do painel de IoT</u>	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
<u>Atualizou as funções vinculadas ao serviço para AWS IoT SiteWise</u>	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
<u>Marcação atualizada para recursos de fluxo AWS IoT SiteWise de dados</u>	Suporte adicionado para marcar recursos de fluxo de dados.	18 de agosto de 2022
<u>Gateways SiteWise Edge atualizados</u>	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
<u>Atualizou a AWS IoT SiteWise demonstração</u>	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

[Suporte adicionado 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 recursos foram adicionados

10 de agosto de 2021

- 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.

<u>Intervalo de tempo de métrica personalizado</u>	Suporte adicional para intervalos de tempo personalizados e compensações nas métricas.	3 de agosto de 2021
<u>Usando AWS IoT SiteWise na borda</u>	O recurso de processamento de bordas agora está disponível ao público em geral.	29 de julho de 2021
<u>Exportando dados para o Amazon S3</u>	AWS IoT SiteWise agora pode exportar dados para o Amazon S3.	27 de julho de 2021
<u>Endpoints da VPC (AWS PrivateLink)</u>	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
<u>Transformações</u>	As transformações agora podem inserir múltiplas variáveis de propriedade do ativo.	8 de julho de 2021
<u>Atualização da função time stamp()</u>	Nas transformações, você agora pode fornecer uma variável como argumento para a função timestamp() .	16 de junho de 2021
<u>Disponibilidade geral de alarmes</u>	Os recursos 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 adicionou suporte para ASCII, UTF8, e cadeias de caracteres de origem ISO8859 codificadas.

24 de maio de 2021

Service Quotas atualizadas

Foram adicionadas as seguintes cotas para a [GetInterpolatedAssetPropertyValues](#) API: taxa de GetInterpolatedAssetPropertyValues solicitações, número de resultados por GetInterpolatedAssetPropertyValues solicitação e número de dias entre a data de início no passado e a data de GetInterpolatedAssetPropertyValues hoje.

29 de abril de 2021

Expressões de fórmula atualizadas

Adição dos seguintes operadores e funções:

22 de abril de 2021

- 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' '.

<u>Endpoints da VPC (AWS PrivateLink)</u>	Foram adicionadas informações sobre como estabelecer uma conexão privada entre sua nuvem privada virtual (VPC) e o plano de AWS IoT SiteWise controle APIs criando uma interface VPC endpoint.	16 de março de 2021
<u>Federação do IAM</u>	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
<u>Lançamento regional</u>	Lançado AWS IoT SiteWise na China (Pequim).	3 de fevereiro de 2021
<u>Lançado o SiteWise conector IoT versão 10</u>	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
<u>Funções de data e hora</u>	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](#)

15 de dezembro de 2020

Agora você pode monitorar seus dados com alarmes, processar dados industriais na borda, usar o Modbus TCP e Ethernet/IP fontes para seu gateway SiteWise Edge, filtrar dados recebidos com faixas mortas e muito mais.

- Foi adicionada a seção [Monitorando dados com alarmes](#) para lhe permitir definir, configurar e responder aos alarmes no 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

SiteWise Edge a partir do servidor local industrial.

[AWS IoT SiteWise agora oferece suporte gerenciado pelo cliente CMKs.](#)

AWS IoT SiteWise agora oferece suporte à criptografia gerenciada pelo cliente CMKs.

24 de novembro de 2020

[Lançado o SiteWise conector IoT versão 8](#)

A versão 8 do SiteWise conector IoT está disponível. Esta versão melhora a estabilidade quando o conector vivencia conectividade de rede intermitente.

19 de novembro de 2020

[Uso de strings e condicionais em expressões de fórmula](#)

Foram adicionadas informações 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 informações 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 informações sobre como estabelecer uma conexão privada entre sua nuvem privada virtual (VPC) e os AWS IoT SiteWise dados APIs 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 disponível. 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 informações 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 recurso. Essa alteração reduz o número de etapas no tutorial.

4 de agosto de 2020

[Solução de problemas aprimorada do gateway SiteWise Edge](#)

Foram adicionadas informações 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 Amazon 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.

29 de abril de 2020

- 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 Amazon S3.
- Foi adicionada a seção [Configurando fontes de dados](#), que aprimora a documentação da fonte do gateway SiteWise Edge e inclui o novo gateway SiteWise APIs 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 EC2 seção Configurando um gateway SiteWise Edge na Amazon com um AWS CloudFormation modelo que você pode usar para configurar

rapidamente as dependências do gateway SiteWise Edge em uma instância da 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 Greengrass principal foram removidas do Guia AWS IoT SiteWise do usuário. O Guia do AWS IoT Greengrass Desenvolvedor oferece um script de configuração do dispositivo e instruções 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 informações 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 disponível. 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 de 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.

4 de fevereiro de 2020

- [Estados de ativos e modelos](#)
- [Gerencie fluxos de dados para AWS IoT SiteWise](#)
- [Atualizar valores de atributo](#)
- [Associar e desassociar ativos](#)
- [Atualizar ativos e modelos](#)
- [Exclua ativos e modelos em AWS IoT SiteWise](#)

[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 notificações 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. Reestruturação de Propriedades de ativos em tópicos separados, para cada tipo de propriedade.	7 de janeiro de 2020
Usar filtros de nó OPC UA	Foram adicionadas informações 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 informações 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 disponível. 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 segredos OPC UA.

10 de dezembro de 2019

[Criando painéis \(AWS CLI\)](#)

Foram adicionadas informações sobre como criar um painel AWS IoT SiteWise Monitor usando AWS CLI.

6 de dezembro de 2019

[AWS IoT SiteWise versão 2 lançada](#)

Prévia lançada para a versão 2 do AWS IoT SiteWise.

2 de dezembro de 2019

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 Monitor](#) seção 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 [Interaja com outros AWS serviços](#).
- Reformulação da seção [conceitos básicos](#) para corresponder à experiência de demonstração atualizada.

[AWS IoT SiteWise versão 1 lançada](#)

Lançada prévia inicial para a versão 1 do AWS IoT SiteWise.

25 de fevereiro de 2019

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.