Guide de l’utilisateur

AWS IoT SiteWise

AWS IoT SiteWise: Guide de l’utilisateur

Table of Contents

Qu'est-ce que c'est AWS IoT SiteWise ? 1
Comment ça marche 2
Ingérez des données industrielles 2
Modélisez les actifs pour contextualiser les données collectées 3
Analysez à l'aide de requêtes, d'alarmes et de prédictions 4
Visualisez les opérations 4
Stockez les données 5
Intégrer à d'autres services 5
Concepts 5
Cas d'utilisation 11
Fabrication 11
Alimentation et boissons 11
Énergie et services publics 12
Premiers pas 13
Prérequis 13
Configuration d'un Compte AWS 14
Inscrivez-vous pour un Compte AWS 14
Création d'un utilisateur doté d'un accès administratif 14
Utilisation de la démonstration de démarrage rapide 16
Création de la AWS IoT SiteWise démo 16
Supprimer la AWS IoT SiteWise démo 18
Didacticiels 20
Calcul de l'OEE en cours 20
Prérequis 20
Calcul de l'OEE 21
Ingestion de données provenant d'objets AWS IoT 23
Prérequis 24
Étape 1 : créer une politique 25
Étape 2 : créer un AWS IoT objet 27
Étape 3 : Création d'un modèle de ressource d'appareil 29
Étape 4 : créer un parc d'appareils 31
Étape 5 : Représenter un appareil 33
Étape 6 : Représenter le parc d'appareils 34
Étape 7 : Envoyer des données à l'appareil 35

Étape 8 : script client de l'appareil 38
Étape 9 : Nettoyer les ressources 45
Visualisation et partage de données dans Monitor SiteWise 47
Prérequis 48
Étape 1 : Création d'un portail 49
Étape 2 : Connectez-vous à un portail 53
Étape 3 : Créer un projet 55
Étape 4 : Création d'un tableau de bord 59
Étape 5 : Explorez le portail 66
Étape 6 : Nettoyage des ressources 67
Publication de mises à jour de la valeur des propriétés sur Amazon DynamoDB 70
Prérequis 70
Étape 1 : Configuration AWS IoT SiteWise pour publier les mises à jour de la valeur des propriétés 71
Étape 2 : création d'une règle 73
Étape 3 : Création d'une table DynamoDB 76
Étape 4 : Configuration de l'action des règles 78
Étape 5 : Explorez les données 79
Étape 6 : nettoyer les ressources 80
Ingestion de données pour AWS IoT SiteWise 84
Gestion des flux de données 85
Gestion des flux de données 86
Utilisation de l' AWS IoT SiteWise API 94
Utiliser des AWS IoT Core règles 97
Octroi de l'accès requis 97
Configuration de l'action de règle 99
Réduction des coûts grâce à l'ingestion de base 107
Utiliser des AWS IoT Events actions 108
Utilisation du gestionnaire de AWS IoT Greengrass flux 109
Utilisation de l' CreateBulkImportJob API 110
Création d'une tâche d'importation en bloc (AWS CLI) 112
Décrire une tâche d'importation en masse (AWS CLI) 115
Répertorier les tâches d'importation en bloc (AWS CLI) 116
Utilisation des passerelles SiteWise Edge 118
Prérequis 118
Prérequis 119

Création d'une passerelle SiteWise Edge 122
Création d'une passerelle SiteWise Edge 123
Installation du logiciel de passerelle SiteWise Edge sur votre appareil local 124
Permettre le traitement des données de pointe 127
Configuration de la fonctionnalité Edge 128
Traitement des données à la périphérie 130
Configuration de l'éditeur 132
Configuration des sources de données 135
Configuration d'une source OPC-UA 136
Configuration de l'authentification des sources de données 160
Choix d'une destination pour les données de votre serveur source 164
Ajouter des sources de données partenaires 167
Sécurité 168
Ajouter une source de données partenaire 168
Configurer docker sur votre passerelle Edge SiteWise 169
Sources de données partenaires 170
Utiliser des packs 171
Packs d'amélioration 171
Gestion des passerelles SiteWise Edge 172
Gestion de votre passerelle SiteWise Edge avec la AWS IoT SiteWise console 173
Gestion des passerelles SiteWise Edge à l'aide de AWS OpsHubAWS IoT SiteWise 174
Accès à votre passerelle SiteWise Edge à l'aide des informations d'identification du système d'exploitation local 176
Gestion du certificat de passerelle SiteWise Edge 178
Modification de la version des packs de composants de la passerelle SiteWise Edge 179
Running SiteWise Edge sur Siemens Industrial Edge 179
Prérequis 180
Sécurité 180
Créez le fichier de configuration 181
Résolution des problèmes 182
Nous contacter 183
Filtrer les actifs 184
Configuration du filtrage des bords 184
Utilisation des API 185
Toutes les API disponibles pour une utilisation avec les appareils de AWS IoT SiteWise pointe 185

API réservées aux périphériques 186
Tutoriel : Obtenir une liste de modèles d'actifs 189
Backup et restauration des passerelles SiteWise Edge 199
Sauvegardes quotidiennes des données métriques 199
Restaurer une passerelle SiteWise Edge 200
Restaurer AWS IoT SiteWise les données 201
Validez les sauvegardes et restaurations réussies 202
Configuration des passerelles SiteWise Edge ()AWS IoT Greengrass Version 1 204
Choix d'un AWS IoT Greengrass V1 SiteWise périphérique de passerelle Edge 205
Configuration d'une passerelle AWS IoT Greengrass V1 SiteWise Edge 206
Configuration des sources de données sur les passerelles AWS IoT Greengrass V1 SiteWise Edge 225
Modélisation des ressources industrielles 247
État des ressources et des modèles 249
Vérification de l'état d'une ressource 250
Vérification de l'état d'un modèle d'actif ou d'un modèle de composant 251
Modèles composites personnalisés (composants) 253
Modèles composites personnalisés en ligne 254
Modèles composites omponent-model-based personnalisés C 256
Utilisation de chemins pour référencer les propriétés de modèles composites personnalisés 258
Utilisation des identifiants d'objets 260
Utilisation des UUID d'objets 260
Utilisation d'identifiants externes 261
Création de modèles d'actifs et de modèles de composants 263
Création de modèles de ressources 263
Création de modèles de composants 279
Définition des propriétés des données 283
Création de modèles composites personnalisés (composants) 368
Création de ressources 372
Création d'une ressource (console) 372
Création d'un actif (AWS CLI) 373
Configuration d'une nouvelle ressource 375
Recherche de ressources 375
Prérequis 375
Recherche avancée sur Console AWS IoT SiteWise 375

Mappage des flux de données industrielles avec des propriétés de ressources 379
Définition d'un alias de propriété (console) 381
Définition d'un alias de propriété (AWS CLI) 381
Mise à jour des valeurs d'attribut 384
Association et dissociation de ressources 387
Association et dissociation de ressources (console) 387
Associer et dissocier des actifs ()AWS CLI 389
Mise à jour des ressources et des modèles 391
Mise à jour de ressources 391
Mise à jour des modèles d'actifs et des modèles de composants 393
Mise à jour de modèles composites personnalisés (composants) 398
Suppression des ressources et des modèles 401
Suppression de ressources 401
Suppression de modèles de ressource 403
Opérations groupées avec actifs et modèles 405
Concepts clés et terminologie 406
Fonctionnalités prises en charge 407
Prérequis pour les opérations en masse 407
Exécution d'une tâche d'importation en bloc 410
Exécution d'une tâche d'exportation groupée 412
Suivi de l'avancement des tâches et gestion des erreurs 416
Exemples d'importation de métadonnées 422
Exemples de métadonnées d'exportation 436
AWS IoT SiteWise schéma de tâche de transfert de métadonnées 439
Surveillance des données à l'aide d'alarmes 458
Types d'alarmes 458
États d'alarme 460
Propriétés de l'état de l'alarme 461
Définition des alarmes sur les modèles d'actifs 464
Définition des AWS IoT Events alarmes 467
Définition des alarmes externes 503
Configuration des alarmes sur les actifs 505
Configuration d'une valeur de seuil (console) 505
Configuration d'une valeur de seuil (AWS CLI) 506
Configuration des paramètres de notification (console) 508
Configuration des paramètres de notification (CLI) 508

Répondre aux alarmes 510
Répondre à une alarme (console) 511
Répondre à une alarme (API) 514
Ingestion de l'état d'alarme externe 515
Cartographie des flux d'état d'alarme externes 516
Ingestion des données d'état des alarmes 517
Surveillance des données avec des portails web 519
SiteWise Contrôler les rôles 520
Fédération SAML 522
SiteWise Concepts de surveillance 524
Premiers pas 525
Création d'un portail 526
Configuration de votre portail 527
Invitation des administrateurs 531
Ajout d'utilisateurs du portail 534
Création de tableaux de bord 538
Activation des alarmes pour vos portails 544
Activation de votre portail à la périphérie 547
Administration de vos portails 547
Modification des attributs d'un portail 549
Ajout ou suppression d'administrateurs du portail 549
Envoi d'invitations par e-mail aux administrateurs du portail 553
Ajout ou suppression d'utilisateurs du portail 553
Suppression d'un portail 556
Surveillance des données avec l'application de tableau de bord IoT 559
Interrogez les données de AWS IoT SiteWise 560
Rechercher les valeurs actuelles des actifs 561
Rechercher la valeur actuelle d'une propriété d'actif (console) 561
Rechercher la valeur actuelle d'une propriété d'actif (AWS CLI) 561
Rechercher les valeurs historiques des propriétés des actifs 563
Rechercher l'historique des valeurs d'une propriété d'actif (AWS CLI) 563
Rechercher des agrégats de propriétés d'actifs 564
Agrégats pour une propriété d'actif (API) 565
Agrégats pour une propriété d'actif ()AWS CLI 566
AWS IoT SiteWise langage de requête 567
Prérequis 568

Référence du langage de requête 569
Interaction avec d'autres services 577
Présentation des rubriques MQTT des propriétés de ressource 578
Utilisation des notifications relatives aux propriétés des actifs 578
Activation des notifications relatives aux propriétés de ressource (console) 579
Activation des notifications relatives aux propriétés des actifs (AWS CLI) 579
Interrogation des messages de notification de propriété de ressource 581
Exportation de données vers Amazon S3 584
Créez la AWS CloudFormation pile 586
Afficher vos données dans Amazon S3 587
Analyser les données exportées 589
Ressources de modèles créées 598
Intégration à Grafana 601
Intégration avec AWS IoT TwinMaker 603
Activation de l'intégration 604
Intégration d'AWS IoT SiteWise et de AWS IoT TwinMaker 604
Détecter les anomalies des équipements 605
Ajouter une définition de prédiction (console) 607
Entraînement d'une prédiction (console) 610
Démarrer ou arrêter l'inférence sur une prédiction (console) 611
Ajouter une définition de prédiction (CLI) 612
Entraînement d'une prédiction et démarrage de l'inférence (CLI) 615
Entraînement d'une prédiction (CLI) 617
Démarrer ou arrêter l'inférence sur une prédiction (CLI) 619
Gestion du stockage des données 622
Configuration des paramètres de stockage 623
Impact sur la conservation des données 624
Configurer les paramètres de stockage pour Warm Tier (console) 624
Configurer les paramètres de stockage pour Warm Tier (AWS CLI) 626
Configuration des paramètres de stockage pour le niveau froid (console) 629
Configurer les paramètres de stockage pour Cold Tier (AWS CLI) 632
Résoudre les problèmes liés aux paramètres de stockage 637
Erreur : le compartiment n'existe pas 637
Erreur : accès refusé au chemin Amazon S3 637
Erreur : l'ARN du rôle ne peut pas être assumé 638
Erreur : Impossible d'accéder au compartiment Amazon S3 interrégional 638

Chemins de fichiers et schémas de données enregistrés dans le niveau froid 638
Données relatives à l'équipement (mesures) 639
Métriques, transformations et agrégats 644
Métadonnées relatives aux actifs 649
Métadonnées de hiérarchie des actifs 653
Fichiers d'index des données de stockage 656
Sécurité 657
Protection des données 658
Confidentialité du trafic inter-réseau 659
Chiffrement des données 659
Chiffrement au repos 660
Chiffrement en transit 663
Gestion des clés 664
Gestion des identités et des accès 666
Public ciblé 667
Authentification par des identités 667
Comment AWS IoT SiteWise fonctionne avec IAM 671
Politiques gérées 691
Rôles liés à un service 695
Configuration des autorisations pour les alarmes 709
Prévention du problème de l'adjoint confus entre services 715
Résolution des problèmes 717
Validation de conformité 719
Résilience 720
Sécurité de l'infrastructure 721
Analyse de la configuration et des vulnérabilités 722
Points de terminaison d'un VPC 722
Opérations d'API prises en charge 723
Création d'un point de terminaison d'un VPC d'interface 726
Accès AWS IoT SiteWise via un point de terminaison VPC d'interface 726
Création d'une stratégie de point de terminaison de VPC 728
Bonnes pratiques de sécurité 729
Utiliser les informations d'identification d'authentification sur vos serveurs OPC-UA 729
Utiliser des modes de communication chiffrés pour vos serveurs OPC-UA 729
Maintenez vos composants à jour 730
Chiffrez le système de fichiers de votre passerelle SiteWise Edge 730

Accès sécurisé à votre configuration Edge 730
Accorder aux utilisateurs de SiteWise Monitor les autorisations minimales possibles 730
Ne pas exposer d'informations sensibles 731
Suivez les meilleures pratiques en matière de AWS IoT Greengrass sécurité 731
Consultez aussi 731
Journalisation et surveillance 732
Surveillance des journaux de service 733
Gestion de la connexion AWS IoT SiteWise 734
Exemple : entrées de fichier AWS IoT SiteWise journal 736
Surveillance des journaux de la passerelle SiteWise Edge 736
Utilisation d'Amazon CloudWatch Logs 737
Utilisation des journaux de service 738
Utilisation des journaux d'événements 740
Surveillance à l'aide des CloudWatch métriques Amazon 743
AWS IoT Greengrass Version 2 métriques de passerelle 744
AWS IoT Greengrass Version 1 métriques de passerelle 752
Journalisation des appels d'API avec AWS CloudTrail 758
AWS IoT SiteWise informations dans CloudTrail 758
AWS IoT SiteWise événements de données dans CloudTrail 759
AWS IoT SiteWise événements de gestion dans CloudTrail 762
Exemple : entrées de fichier AWS IoT SiteWise journal 762
Balisage de vos ressources 764
Utilisation de balises dans AWS IoT SiteWise 764
Marquage à l'aide du AWS Management Console 764
Marquage avec l'API AWS IoT SiteWise 765
Utilisation des balises avec des politiques IAM 766
Résolution des problèmes 768
Résolution des problèmes d'importation et d'exportation en masse 768
Résolution des problèmes liés à un portail 769
Les utilisateurs et les administrateurs ne peuvent pas accéder au AWS IoT SiteWise portail 769
Dépannage d'une passerelle 770
Configuration et accès aux journaux de la passerelle SiteWise Edge 771
Résolution des problèmes liés à la passerelle SiteWise Edge 771
AWS IoT Greengrass Problèmes de résolution des problèmes 775
Résolution des problèmes liés à une action de AWS IoT SiteWise règle 775

Configuration des AWS IoT Core journaux 775
Configuration d'une action d'erreur de republication 776
Résolution des problèmes 778
Résolution des problèmes d'une règle 780
Résolution des problèmes d'une règle 782
Points de terminaison et quotas 787
Points de terminaison 787
..... 787
..... 787
..... 788
..... 788
..... 788
..... 788
Quotas 789
Quotas pour la détection des anomalies 804
Historique de la documentation 805
Glossaire AWS 826
..... dcccxxvii

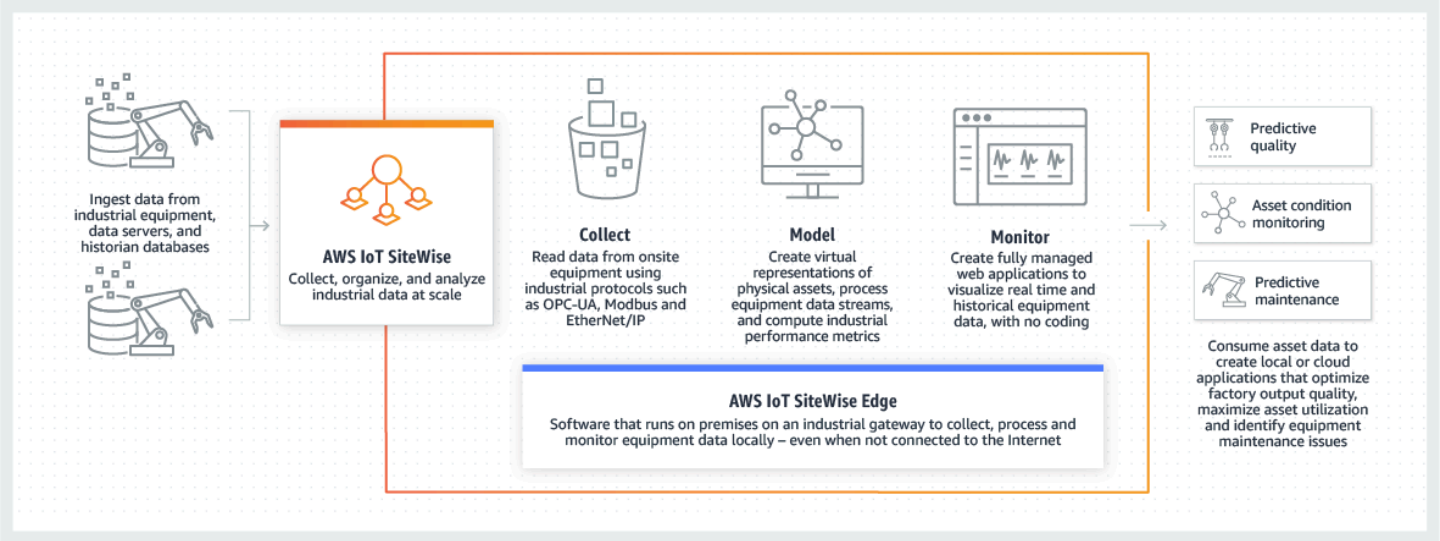
Qu'est-ce que c'est AWS IoT SiteWise ?

AWS IoT SiteWise est un service géré qui facilite la collecte, le stockage, l'organisation et le suivi des données provenant d'équipements industriels à grande échelle afin de vous aider à prendre de meilleures décisions basées sur les données. Vous pouvez l'utiliser AWS IoT SiteWise pour surveiller les opérations sur l'ensemble des installations, calculer rapidement les indicateurs de performance industrielle courants et créer des applications qui analysent les données des équipements industriels afin de prévenir les problèmes d'équipement coûteux et de réduire les écarts de production.

AWS IoT SiteWise Monitor permet à vos utilisateurs opérationnels de créer rapidement des applications Web pour visualiser et analyser vos données industrielles en temps réel. Vous pouvez obtenir des informations sur vos opérations industrielles en configurant et en surveillant des mesures telles que le temps moyen entre les pannes et l'efficacité globale de l'équipement (OEE).

AWS IoT SiteWise Edge est un composant AWS IoT SiteWise qui permet de collecter, de stocker et de traiter des données sur des appareils locaux. Cela est utile si vous avez un accès limité à Internet ou si vous devez préserver la confidentialité de vos données.

Le schéma suivant montre l'architecture de base de AWS IoT SiteWise :



Rubriques

- Comment AWS IoT SiteWise fonctionne
- AWS IoT SiteWise concepts
- Cas d'utilisation pour AWS IoT SiteWise

Comment AWS IoT SiteWise fonctionne

AWS IoT SiteWise propose un cadre de modélisation des ressources que vous pouvez utiliser pour créer des représentations de vos appareils, processus et installations industriels. Les représentations de votre équipement et de vos processus sont appelées modèles d'actifs dans AWS IoT SiteWise. Avec les modèles d'actifs, vous définissez les données brutes à consommer et la manière de les transformer en indicateurs utiles. Créez et visualisez des actifs et des modèles pour vos opérations industrielles dans la AWS IoT SiteWise console. Vous pouvez également configurer des modèles d'actifs pour collecter et traiter des données en périphérie ou dans le AWS cloud.

Rubriques

- Ingérez des données industrielles
- Modélisez les actifs pour contextualiser les données collectées
- Analysez à l'aide de requêtes, d'alarmes et de prédictions
- Visualisez les opérations
- Stockez les données
- Intégrer à d'autres services

Ingérez des données industrielles

Commencez à l'utiliser AWS IoT SiteWise en ingérant des données industrielles. L'ingestion de vos données s'effectue de différentes manières :

- Ingestion directe depuis les serveurs sur site : utilisez des protocoles tels que OPC-UA pour lire les données directement à partir des appareils sur site. Déployez le logiciel de passerelle SiteWise Edge, compatible avec AWS IoT Greengrass V2, sur un large éventail de plateformes telles que les passerelles industrielles courantes ou les serveurs virtuels. Vous pouvez connecter jusqu'à 100 serveurs OPC-UA à une seule AWS IoT SiteWise passerelle. Pour plus d'informations, consultez SiteWise Exigences relatives à la passerelle Edge.

  Notez que les protocoles tels que Modbus TCP et EtherNet/IP (EIP) sont pris en charge dans le cadre de notre partenariat avecDomatica. AWS IoT Greengrass V2
- Traitement des données Edge avec des packs : Améliorez votre passerelle SiteWise Edge en ajoutant des packs pour activer des fonctionnalités Edge complètes. Avec SiteWise Edge, disponible sur AWS IoT Greengrass V2, le traitement des données est exécuté directement sur site

avant d'être transmis de manière sécurisée vers le AWS Cloud via un AWS IoT Greengrass flux. Pour plus d'informations, consultez Utiliser des packs.

- Ingestion adaptative via Amazon S3 avec opérations en masse : lorsque vous travaillez avec un grand nombre de ressources ou de modèles d'actifs, utilisez des opérations en masse pour importer et exporter des ressources en masse depuis des compartiments Amazon S3. Pour plus d'informations, consultez Opérations groupées avec actifs et modèles.
- Messages MQTT avec règles de AWS IoT base : pour les appareils connectés à AWS IoT Core qui envoient des messages MQTT, utilisez le moteur de règles AWS IoT Core pour diriger ces messages vers AWS IoT SiteWise. Si vous avez des appareils connectés à AWS IoT Core qui envoient des messages MQTT, utilisez le moteur de règles AWS IoT Core pour acheminer ces messages vers. AWS IoT SiteWise Pour plus d'informations, consultez Ingestion de données à l'aide de règles AWS IoT Core.
- Ingestion de données déclenchée par un événement : utilisez AWS IoT Events des actions pour configurer l' SiteWise action IoT afin d' AWS IoT Events envoyer des données AWS IoT SiteWise lorsque des événements se produisent. Pour plus d'informations, consultez Ingestion de données provenant de AWS IoT Events.
- AWS IoT SiteWise API : vos applications en périphérie ou dans le cloud peuvent envoyer des données directement à AWS IoT SiteWise. Pour plus d'informations, consultez Ingestion de données à l'aide de l'API AWS IoT SiteWise.

Modélisez les actifs pour contextualiser les données collectées

Après avoir ingéré les données, vous pouvez les utiliser pour créer des représentations virtuelles de vos actifs, processus et installations en élaborant des modèles de vos opérations physiques. Un actif, représentant un appareil ou un processus, transmet des flux de données vers le AWS Cloud. Les actifs peuvent également signifier des groupements de périphériques logiques. Les hiérarchies sont formées en associant des actifs pour refléter des opérations complexes. Ces hiérarchies permettent aux actifs d'accéder aux données des actifs enfants associés. Les actifs sont créés à partir de modèles d'actifs. Les modèles d'actifs sont des structures déclaratives qui normalisent les formats des actifs. Réutilisez les composants des actifs pour l'organisation et la maintenabilité de vos modèles. Pour plus d'informations, consultez Modélisation des ressources industrielles.

Avec AWS IoT SiteWise, vous pouvez configurer vos actifs pour transformer les données entrantes en mesures et transformations contextuelles.

- Transforme le travail lors de la réception des données de l'équipement.

- Les mesures sont calculées à des intervalles que vous définissez.

Les métriques et les transformations s'appliquent à la fois à des actifs individuels ou à plusieurs actifs.AWS IoT SiteWise calcule automatiquement les agrégats statistiques couramment utilisés tels que la moyenne, la somme et le nombre, sur différentes périodes pertinentes pour les données, les métriques et les transformations de votre équipement.

Les actifs peuvent être synchronisés à l'aide AWS IoT TwinMaker de. Pour plus d'informations, consultez Intégration d'AWS IoT SiteWise et de AWS IoT TwinMaker.

Analysez à l'aide de requêtes, d'alarmes et de prédictions

Analysez les données recueillies AWS IoT SiteWise en exécutant des requêtes et en configurant des alarmes. Vous pouvez également utiliser Amazon Lookout pour détecter automatiquement les anomalies dans les métriques et identifier leurs causes profondes.

- Définissez des alarmes spécifiques pour alerter votre équipe lorsque l'équipement ou les processus s'écartent des performances optimales, garantissant ainsi une identification et une résolution rapides des problèmes. Pour plus d'informations, consultez Surveillance des données à l'aide d'alarmes.
- Utilisez les opérations de l' AWS IoT SiteWise API pour interroger les valeurs actuelles, les valeurs historiques et les agrégats des propriétés de vos actifs sur des intervalles de temps spécifiques. Pour plus d'informations, consultez Interrogez les données de AWS IoT SiteWise.
- Utilisez la détection des anomalies avec Amazon Lookout for Equipment pour identifier et visualiser les modifications de l'équipement ou des conditions de fonctionnement. Grâce à la détection des anomalies, vous pouvez déterminer les mesures de maintenance préventive pour vos opérations. Cette intégration permet aux clients de synchroniser les données entre Amazon Lookout for AWS IoT SiteWise Equipment et Amazon Lookout for Equipment. Pour plus d'informations, consultez Détecter les anomalies des équipements avec Amazon Lookout for Equipment.

Visualisez les opérations

Configurez SiteWise Monitor pour créer des applications Web pour vos employés opérationnels. Les applications Web aident les employés à visualiser vos opérations. Gérez différents niveaux d'accès pour vos employés à l'aide d'IAM Identity Center ou IAM. Configurez des connexions et des autorisations uniques pour chaque employé afin de consulter des sous-ensembles spécifiques de

l'ensemble d'une opération industrielle. AWS IoT SiteWise fournit un guide d'application permettant à ces employés d'apprendre à utiliser SiteWise Monitor.

Pour plus d'informations sur la visualisation de vos opérations, consultezSurveillance des données avec AWS IoT SiteWise Monitor.

Stockez les données

Vous pouvez intégrer le stockage de séries chronologiques à votre lac de données industriel. AWS IoT SiteWise dispose de trois niveaux de stockage pour les données industrielles :

- Un niveau de stockage à chaud optimisé pour les applications en temps réel.
- Un niveau de stockage à chaud optimisé pour les charges de travail analytiques.
- Un niveau de stockage à froid géré par le client utilisant Amazon S3 pour les applications de données opérationnelles avec une tolérance de latence élevée.

AWS IoT SiteWise vous aide à gérer les coûts de stockage en conservant les données récentes dans le niveau de stockage à chaud. Vous définissez ensuite des politiques de conservation des données pour déplacer les données historiques vers un stockage à chaud ou à froid. Pour plus d'informations, consultez Gestion du stockage des données.

Vous pouvez également importer et exporter les métadonnées des actifs. Pour plus d'informations, consultez Métadonnées relatives aux actifs.

Intégrer à d'autres services

AWS IoT SiteWise s'intègre à plusieurs AWS services pour développer une AWS IoT solution complète dans le AWS Cloud. Pour plus d'informations, voir Interaction avec d'autres AWS services.

AWS IoT SiteWise concepts

Les concepts de base suivants sont les AWS IoT SiteWise suivants :

Regrouper

Les agrégats sont des métriques fondamentales, ou mesures, qui sont calculées AWS IoT SiteWise automatiquement pour toutes les données de séries chronologiques. Pour plus d'informations, consultez Interrogation des agrégats de propriétés d'actif.

Ressource

Lorsque vous saisissez ou ingérez des données AWS IoT SiteWise provenant de votre équipement industriel, vos appareils, équipements et processus sont tous présentés comme des actifs. Chaque actif est associé à des données. Par exemple, un équipement peut avoir un numéro de série, un emplacement, une marque et un modèle, ainsi qu'une date d'installation. Il peut également contenir des séries chronologiques pour la disponibilité, les performances, la qualité, la température, la pression, etc. Regroupez les actifs en hiérarchies pour permettre aux actifs d'accéder aux données stockées dans leurs actifs enfants. Pour plus d'informations, consultez Modélisation des ressources industrielles.

Hiérarchie des ressources

Définissez des hiérarchies d'actifs pour créer des représentations logiques de vos opérations industrielles. Pour ce faire, définissez une hiérarchie dans un modèle d'actifs et associez les actifs créés à partir de ce modèle à la hiérarchie spécifiée. Les indicateurs des actifs parents peuvent combiner les données issues des propriétés des actifs enfants, ce qui vous permet de calculer des indicateurs qui fournissent des informations sur l'ensemble de vos opérations ou sur une partie spécifique de celles-ci. Pour plus d'informations, consultez Définition de hiérarchies de modèles d'actifs.

Modèle de ressource

Chaque actif est créé à l'aide d'un modèle d'actif. Les modèles d'actifs sont des structures qui définissent et normalisent le format de vos actifs. Ils garantissent la cohérence des informations sur plusieurs actifs du même type, ce qui vous permet de gérer les données dans des actifs qui représentent des groupes d'appareils. Dans chaque modèle d'immobilisation, vous pouvez définir des attributs, des entrées de séries chronologiques (mesures), des transformations de séries chronologiques (transformations), des agrégations de séries chronologiques (métriques) et des hiérarchies de ressources. Pour plus d'informations, consultez Modélisation des ressources industrielles.

Décidez où les propriétés de votre modèle d'actifs sont traitées en configurant votre modèle d'actif pour la périphérie. Utilisez cette fonctionnalité pour gérer et surveiller les données relatives aux actifs sur vos appareils locaux.

Propriété de la ressource

Les propriétés des actifs sont les structures de chaque actif qui contiennent des données industrielles. Chaque propriété possède un type de données et peut également avoir une unité.

Une propriété peut être un attribut, une mesure, une transformation, ou une métrique. Pour plus d'informations, consultez Définition des propriétés des données.

Configurez les propriétés des actifs à calculer à la périphérie. Pour plus d'informations sur le traitement des données en périphérie, consultezthe section called "Permettre le traitement des données de pointe".

Attribut

Les attributs sont des propriétés d'un actif qui restent généralement constantes, comme le fabricant ou l'emplacement de l'appareil. Les attributs peuvent avoir des valeurs prédéfinies. Chaque actif créé à partir d'un modèle d'actif inclut les valeurs par défaut des attributs définis dans ce modèle. Pour plus d'informations, consultez Définition de données statiques (attributs).

Tableau de bord

Chaque projet contient un ensemble de tableaux de bord. Les tableaux de bord fournissent un ensemble de visualisations pour les valeurs d'un ensemble de ressources. Les propriétaires de projet créent les tableaux de bord et les visualisations qu'il contient. Lorsqu'un propriétaire de projet est prêt à partager l'ensemble de tableaux de bord, il peut inviter des utilisateurs dans le projet, ce qui leur donne accès à tous les tableaux de bord correspondants. Si vous souhaitez affecter différents groupes d'utilisateurs à différents tableaux de bord, vous devez diviser les tableaux de bord entre plusieurs projets. Lorsque les utilisateurs consultent les tableaux de bord, ils peuvent personnaliser la plage horaire pour examiner des données spécifiques.

Flux de données

Entrez ou ingérez des données industrielles avant AWS IoT SiteWise même de créer des modèles d'actifs et des actifs. AWS IoT SiteWise génère automatiquement des flux de données pour collecter des flux de données brutes provenant de votre équipement.

Alias de flux de données

Les alias de flux de données vous permettent d'identifier facilement un flux de données. Par exemple, l'alias `server1-windfarm/3/turbine/7/temperature` indique les valeurs de température provenant de la turbine #7 du parc éolien #3. Le terme `server1` est le nom de la source de données qui permet d'identifier le serveur OPC-UA. `server1-` Il s'agit d'un préfixe attaché à tous les flux de données signalés par ce serveur OPC-UA.

Association de flux de données

Après avoir créé des modèles d'actifs et des actifs, associez les flux de données aux propriétés des actifs définies dans vos actifs pour structurer vos données. AWS IoT SiteWise peut ensuite

utiliser des modèles d'actifs et des actifs pour gérer les données entrantes provenant de vos flux de données. Vous pouvez également dissocier les flux de données des propriétés des actifs. Pour plus d'informations, consultez Gestion des flux de données.

Formule

Chaque propriété de transformation et de métrique est associée à une formule qui décrit la manière dont la propriété transforme ou agrège les données. Ces formules incluent les entrées de propriétés, les opérateurs et les fonctions proposés par AWS IoT SiteWise. Pour plus d'informations, consultez Utilisation d'expressions de formule.

Mesure

Les mesures sont des propriétés d'un actif qui représentent les flux de données chronologiques bruts d'un capteur provenant d'un appareil ou d'un équipement. Pour plus d'informations, consultez Définition des flux de données provenant des équipements (mesures).

Métrique

Les métriques sont des propriétés d'un actif qui représentent des données de séries chronologiques agrégées. Chaque métrique est accompagnée d'une expression mathématique (formule) qui décrit comment agréger des points de données et un intervalle de temps pour le calcul de cette agrégation. Les métriques génèrent un point de données unique pour chaque intervalle de temps spécifié. Pour plus d'informations, consultez Agrégation de données provenant de propriétés et d'autres actifs (métriques).

Packages

SiteWise Les passerelles Edge utilisent des packs pour déterminer comment collecter, traiter et acheminer les données. Actuellement, AWS IoT SiteWise prend en charge le pack de collecte de données et le pack de traitement des données. Pour plus d'informations sur les packs disponibles pour votre passerelle SiteWise Edge, consultezthe section called "Utiliser des packs".

Pack de collecte de données

Utilisez le pack de collecte de données afin que votre passerelle SiteWise Edge puisse collecter vos données industrielles et les acheminer vers la AWS destination de votre choix. Ce pack est automatiquement ajouté à votre passerelle SiteWise Edge et ne peut pas être supprimé.

Pack de traitement de données

Utilisez le pack de traitement des données pour traiter vos données en périphérie et les conserver pendant 30 jours pour les utiliser dans des applications locales.

Portal

Un AWS IoT SiteWise Monitor portail est une application Web que vous pouvez utiliser pour visualiser et partager vos AWS IoT SiteWise données. Un portail compte un ou plusieurs administrateurs et contient zéro ou plusieurs projets.

Administrateur du portail

Chaque portail SiteWise Monitor possède un ou plusieurs administrateurs de portail. Les administrateurs du portail utilisent ce dernier pour créer des projets contenant des collections de ressources et de tableaux de bord. Ils attribuent ensuite des ressources et des propriétaires à chaque projet. En contrôlant l'accès au projet, les administrateurs de portail spécifient les ressources que les propriétaires et les utilisateurs de projet peuvent voir.

Projet

Chaque portail SiteWise Monitor contient un ensemble de projets. Chaque projet est associé à un sous-ensemble de vos ressources AWS IoT SiteWise . Les propriétaires de projet créent un ou plusieurs tableaux de bord pour fournir un moyen cohérent de visualiser les données liées à ces ressources. Ils peuvent inviter des utilisateurs standard dans le projet pour leur permettre d'en consulter les ressources et les tableaux de bord. Le projet est l'unité de base du partage au sein de SiteWise Monitor. Les propriétaires de projets peuvent inviter les utilisateurs auxquels l' AWS administrateur a donné accès au portail. Tout utilisateur doit avoir accès à un portail avant qu'un projet de ce portail puisse être partagé avec lui.

Propriétaire du projet

Chaque projet SiteWise Monitor a des propriétaires. Ces propriétaires créent des visualisations sous la forme de tableaux de bord afin de représenter les données opérationnelles de manière cohérente. Lorsque les tableaux de bord sont prêts à être partagés, tout propriétaire du projet peut inviter des utilisateurs. Les propriétaires de projet peuvent également affecter d'autres propriétaires au projet. Les propriétaires de projets peuvent configurer des seuils et des paramètres de notification pour les alarmes.

Utilisateur de projet

Chaque projet SiteWise Monitor possède des spectateurs. Les utilisateurs de projet peuvent se connecter au portail pour consulter les tableaux de bord créés par les propriétaires de projet. Dans chaque tableau de bord, les utilisateurs du projet peuvent ajuster la plage de temps pour mieux comprendre les données opérationnelles. Les utilisateurs de projet ne peuvent afficher que les tableaux de bord des projets auxquels ils ont accès. Les spectateurs du projet peuvent accuser réception des alarmes et les suspendre.

Alias de propriété

Vous avez la possibilité de créer des alias sur les propriétés des actifs, tels que le chemin du flux de données du serveur OPC-UA (par exemple, /company/windfarm/3/turbine/7/temperature), afin de simplifier l'identification d'une propriété d'actif lors de l'ingestion ou de la récupération des données des actifs. Lorsque vous utilisez une passerelle SiteWise Edge pour ingérer des données provenant de serveurs, les alias de vos propriétés doivent correspondre aux chemins de vos flux de données brutes. Pour plus d'informations, consultez Mappage des flux de données industrielles avec des propriétés de ressources.

Notification de propriété

Lorsque vous activez les notifications de propriété pour une propriété d'actif, AWS IoT SiteWise publie un message MQTT AWS IoT Core chaque fois que cette propriété reçoit une nouvelle valeur. La charge utile du message inclut des détails sur la mise à jour de cette valeur de propriété. Utilisez les notifications relatives à la valeur des propriétés pour créer des solutions qui connectent vos données industrielles AWS IoT SiteWise à d'autres AWS services. Pour plus d'informations, consultez Interaction avec d'autres AWS services.

SiteWise Passerelle Edge

Une passerelle SiteWise Edge est située dans les locaux du client pour collecter, traiter et diriger les données. Une passerelle SiteWise Edge se connecte à vos sources de données industrielles via le protocole OPC-UA pour collecter et traiter les données, puis les envoyer vers le AWS cloud. SiteWise Les passerelles Edge peuvent également se connecter aux sources de données partenaires. SiteWise Les passerelles Edge utilisent des packs pour la collecte de données, le traitement Edge, etc. Pour plus d'informations sur les packs disponibles, consultezthe section called "Utiliser des packs".

Vous avez la possibilité de créer une passerelle SiteWise Edge sur n'importe quel appareil ou plate-forme capable de fonctionner AWS IoT Greengrass. Pour plus d'informations, consultez Utilisation des passerelles SiteWise Edge.

Transformation

Les transformations sont des propriétés d'un actif qui représentent des données de séries chronologiques transformées. Chaque transformation est accompagnée d'une expression mathématique (formule) qui indique comment convertir les points de données d'un formulaire à un autre. Les points de données transformés entretiennent une one-to-one relation avec les points de données d'entrée. Pour plus d'informations, consultez Transformation des données (transformations).

Visualisation

Dans chaque tableau de bord, les propriétaires de projet décident comment afficher les propriétés et les alarmes des actifs associés au projet. La disponibilité peut être représentée sous forme de graphique linéaire, tandis que d'autres valeurs peuvent être affichées sous forme de diagrammes à barres ou d'indicateurs de performance clés (KPI). Il est préférable d'afficher les alarmes sous forme de grilles d'état et de chronologies d'état. Les propriétaires de projet personnalisent chaque visualisation pour fournir une compréhension optimale des données de la ressource concernée.

Cas d'utilisation pour AWS IoT SiteWise

AWS IoT SiteWise est utilisé dans de nombreux secteurs pour de nombreuses applications de collecte et d'analyse de données industrielles.

Collectez des données de manière cohérente auprès de toutes vos sources afin de résoudre rapidement les problèmes. AWS IoT SiteWise propose une surveillance à distance pour collecter les données directement sur site ou à partir de sources multiples dans de nombreuses installations. AWS IoT SiteWise fournit la flexibilité nécessaire aux solutions de données IoT industrielles.

Fabrication

AWS IoT SiteWise peut simplifier le processus de collecte et d'utilisation des données de votre équipement afin d'identifier et de minimiser les inefficiences, améliorant ainsi les opérations industrielles. AWS IoT SiteWise vous aide à collecter des données sur les chaînes de fabrication et les équipements. Vous pouvez ainsi transférer les données vers le AWS cloud et créer des indicateurs de performance pour vos équipements et processus spécifiques. AWS IoT SiteWise Vous pouvez utiliser les indicateurs produits pour comprendre l'efficacité globale de vos opérations et identifier les opportunités d'innovation et d'amélioration. Vous pouvez également consulter votre processus de fabrication et identifier les défaillances des équipements et des processus, les écarts de production ou les défauts du produit.

Alimentation et boissons

Les installations du secteur de l'alimentation et des boissons gèrent une large variété d'opérations de transformation des aliments, notamment la mouture du grain en farine, le découpage et l'emballage de la viande, ainsi que l'assemblage, la préparation et la congélation de plats micro-ondables. Les usines de transformation des aliments s'étendent souvent sur plusieurs sites, les opérateurs d'usine et d'équipement étant centralisés pour surveiller les processus et les équipements. Par exemple,

les unités de réfrigération évaluent la manipulation et l'expiration des ingrédients. Ils surveillent la création de déchets dans les installations pour garantir l'efficacité opérationnelle. Vous pouvez ainsi regrouper les flux de données de capteurs provenant de plusieurs sites par ligne de production et par installation afin que vos ingénieurs de procédé puissent mieux comprendre et apporter des améliorations à l'ensemble des installations. AWS IoT SiteWise

Énergie et services publics

Avec AWS IoT SiteWise, vous pouvez résoudre les problèmes d'équipement plus facilement et plus efficacement. Vous pouvez surveiller les performances des actifs à distance et en temps réel. Accédez aux données historiques des équipements où que vous soyez pour identifier les problèmes potentiels, affecter des ressources précises et prévenir et résoudre les problèmes plus rapidement.

Commencer avec AWS IoT SiteWise

Avec AWS IoT SiteWise, vous pouvez collecter, organiser, analyser et visualiser vos données.

AWS IoT SiteWise fournit une démonstration que vous pouvez utiliser pour explorer le service sans configurer une véritable source de données. Pour plus d'informations, consultez Utilisation de la AWS IoT SiteWise démo.

Vous pouvez suivre les didacticiels suivants pour découvrir certaines fonctionnalités de AWS IoT SiteWise :

- Ingestion de données provenant d'objets AWS IoT
- Visualisation et partage des données des parcs éoliens dans Monitor SiteWise
- Publication de mises à jour de la valeur des propriétés sur Amazon DynamoDB

Consultez les rubriques suivantes pour en savoir plus sur AWS IoT SiteWise :

- Ingestion de données pour AWS IoT SiteWise
- Modélisation des ressources industrielles
- Permettre le traitement des données de pointe
- Surveillance des données avec AWS IoT SiteWise Monitor
- Interrogez les données de AWS IoT SiteWise
- Interaction avec d'autres AWS services

Rubriques

- Prérequis
- Configuration d'un Compte AWS
- Utilisation de la AWS IoT SiteWise démo

Prérequis

Vous devez avoir un Compte AWS pour commencer AWS IoT SiteWise. Si vous n'en avez pas, veuillez consulter Configuration d'un Compte AWS.

Utilisez une région où elle AWS IoT SiteWise est disponible. Pour plus d'informations, consultez Points de terminaison et quotas AWS IoT SiteWise. Vous pouvez utiliser le sélecteur de région dans le AWS Management Console pour passer à l'une de ces régions.

Configuration d'un Compte AWS

Rubriques

- Inscrivez-vous pour un Compte AWS
- Création d'un utilisateur doté d'un accès administratif

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. Pour des raisons de sécurité, attribuez un accès administratif à un utilisateur et utilisez uniquement l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Après vous être inscrit à un Compte AWS, sécurisez Utilisateur racine d'un compte AWS AWS IAM Identity Center, activez et créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, voir Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, accordez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connectez-vous en tant qu'utilisateur disposant d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribuer l'accès à des utilisateurs supplémentaires

1. Dans IAM Identity Center, créez un ensemble d'autorisations conforme aux meilleures pratiques en matière d'application des autorisations du moindre privilège.

Pour obtenir des instructions, voir Création d'un ensemble d'autorisations dans le guide de AWS IAM Identity Center l'utilisateur.

2. Affectez des utilisateurs à un groupe, puis attribuez un accès d'authentification unique au groupe.

   Pour obtenir des instructions, voir Ajouter des groupes dans le guide de AWS IAM Identity Center l'utilisateur.

Utilisation de la AWS IoT SiteWise démo

Vous pouvez facilement explorer AWS IoT SiteWise en utilisant la AWS IoT SiteWise démo. AWS IoT SiteWise fournit la démo sous forme de AWS CloudFormation modèle que vous pouvez déployer pour créer des modèles d'actifs, des actifs et un portail de SiteWise surveillance, et générer des exemples de données pendant une semaine au maximum.

> **Important**
>
> Une fois que vous aurez créé la démo, les ressources créées et consommées par cette démo vous seront facturées.

Rubriques

- Création de la AWS IoT SiteWise démo
- Supprimer la AWS IoT SiteWise démo

Création de la AWS IoT SiteWise démo

Vous pouvez créer la AWS IoT SiteWise démo depuis la AWS IoT SiteWise console.

> **Note**
>
> La démo crée des fonctions Lambda, une règle d' CloudWatch événements et les rôles AWS Identity and Access Management (IAM) requis pour la démonstration. Vous trouverez peut-être ces ressources dans votre Compte AWS. Nous vous recommandons de conserver ces

ressources jusqu'à ce que vous ayez terminé la démo. Si vous supprimez les ressources, la démo risque de ne plus fonctionner correctement.

Pour créer la démo dans la AWS IoT SiteWise console

1. Accédez à la AWS IoT SiteWise console et trouvez la SiteWise démo dans le coin supérieur droit de la page.
2. (Facultatif) Sous SiteWise démo, modifiez le champ Jours pendant lesquels vous souhaitez conserver les ressources de démonstration pour spécifier le nombre de jours pendant lesquels vous devez conserver la démo avant de la supprimer.
3. (Facultatif) Pour créer un portail de SiteWise surveillance afin de surveiller des échantillons de données, procédez comme suit.

   > **Note**
   >
   > Les ressources du SiteWise moniteur créées et consommées par cette démo vous seront facturées. Pour plus d'informations, voir SiteWise Surveiller dans la section AWS IoT SiteWise Tarification.

   a. Choisissez Monitor Resources.
   b. Choisissez Autorisation.
   c. Choisissez un rôle IAM existant qui accorde à vos utilisateurs IAM fédérés l'accès au portail.

      > **Important**
      >
      > Votre rôle IAM doit disposer des autorisations suivantes.

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

Pour plus d'informations sur l'utilisation de SiteWise Monitor, voir Qu'est-ce que c'est AWS IoT SiteWise Monitor ? dans le guide de AWS IoT SiteWise Monitor candidature.

4. Choisissez Créer une démonstration.

   La démonstration prend environ 3 minutes à créer. Si la création de la démonstration échoue, votre compte peut ne pas disposer d'autorisations suffisantes. Basculez vers un compte disposant d'autorisations administratives ou suivez les étapes suivantes pour supprimer la démo et réessayez :

   a. Choisissez Delete demo (Supprimer la démo).

      La suppression de la démonstration prend environ 15 minutes.

   b. Si la démo n'est pas supprimée, ouvrez la AWS CloudFormation console, choisissez la pile nommée IoT SiteWiseDemoAssets, puis choisissez Supprimer dans le coin supérieur droit.

   c. Si la démo ne parvient pas à être supprimée à nouveau, suivez les étapes de la AWS CloudFormation console pour ignorer les ressources qui n'ont pas pu être supprimées, puis réessayez.

5. Une fois la démo créée avec succès, vous pouvez explorer les ressources et les données de démonstration dans la AWS IoT SiteWise console.

Supprimer la AWS IoT SiteWise démo

La AWS IoT SiteWise démo se supprime d'elle-même au bout d'une semaine, ou après le nombre de jours que vous avez choisi si vous avez créé la pile de démonstration depuis la AWS CloudFormation console. Vous pouvez supprimer la démo avant si vous avez fini d'utiliser les ressources de

démonstration. Vous pouvez également supprimer la démo si la démo ne parvient pas à créer. Suivez les étapes suivantes pour supprimer manuellement la démo.

Pour supprimer la AWS IoT SiteWise démo

1. Accédez à la console AWS CloudFormation.
2. Choisissez IoTSiteWiseDemoAssets dans la liste Stacks (Piles).
3. Sélectionnez Delete (Supprimer).

   Lorsque vous supprimez la pile, toutes les ressources créées pour la démonstration sont supprimées.
4. Dans la boîte de dialogue de confirmation, choisissez Delete (Supprimer).

   La suppression de la pile prend environ 15 minutes. Si la suppression de la démonstration échoue, choisissez à nouveau Delete (Supprimer) dans le coin supérieur droit. Si la démo ne parvient pas à être supprimée à nouveau, suivez les étapes de la AWS CloudFormation console pour ignorer les ressources qui n'ont pas pu être supprimées, puis réessayez.

AWS IoT SiteWise tutoriels

Bienvenue sur la page des AWS IoT SiteWise tutoriels. Cette collection croissante de didacticiels vous permet d'acquérir les connaissances et les compétences nécessaires pour naviguer dans les subtilités de. AWS IoT SiteWise Ces didacticiels proposent un large éventail de sujets de base adaptés à vos besoins. En parcourant les didacticiels, découvrez des informations précieuses sur divers aspects de AWS IoT SiteWise.

Chaque tutoriel utilise un exemple d'équipement spécifique. Ces didacticiels sont destinés aux environnements de test et utilisent des noms de sociétés, des modèles, des actifs, des propriétés fictifs, etc. Leur objectif consiste à fournir des instructions générales. Les didacticiels ne sont pas destinés à être utilisés directement dans un environnement de production sans un examen minutieux et une adaptation pour répondre aux besoins uniques de votre organisation.

Rubriques

- Calcul de l'OEE dans AWS IoT SiteWise
- Ingestion de données provenant d'objets AWS IoT
- Visualisation et partage des données des parcs éoliens dans Monitor SiteWise
- Publication de mises à jour de la valeur des propriétés sur Amazon DynamoDB

Calcul de l'OEE dans AWS IoT SiteWise

Ce didacticiel fournit un exemple de la façon de calculer l'efficacité globale d'équipement (OEE) pour un processus de fabrication. Pour cette raison, vos calculs ou formules d'OEE peuvent être différents de ceux illustrés ici. En général, l'OEE est définie comme `Availability * Quality * Performance`. Pour en savoir plus sur le calcul de l'OEE, veuillez consulter Efficacité globale de l'équipement sur Wikipédia.

Prérequis

Pour terminer ce didacticiel, vous devez configurer l'ingestion de données pour un appareil qui possède les trois flux de données suivants :

- `Equipment_State`— Code numérique qui représente l'état de la machine, tel que le ralenti, le défaut, l'arrêt planifié ou le fonctionnement normal.

- `Good_Count`— Un flux de données dans lequel chaque point de données contient le nombre d'opérations réussies depuis le dernier point de données.
- `Bad_Count`— Un flux de données dans lequel chaque point de données contient le nombre d'opérations infructueuses depuis le dernier point de données.

Pour configurer l'ingestion de données, veuillez consulter Ingestion de données pour AWS IoT SiteWise. Si vous n'avez pas d'opération industrielle disponible, vous pouvez écrire un script qui génère et télécharge des exemples de données via l'API AWS IoT SiteWise .

Calcul de l'OEE

Dans ce didacticiel, vous créez un modèle de ressource qui calcule l'OEE à partir de trois flux d'entrée de données : `Equipment_State`, `Good_Count` et `Bad_Count`. Dans cet exemple, considérez une machine d'emballage générique, telle qu'une machine utilisée pour l'emballage du sucre, des chips ou de la peinture. Dans la AWS IoT SiteWise console, créez un modèle AWS IoT SiteWise d'actif avec les mesures, transformations et métriques suivantes. Ensuite, vous pouvez créer un actif pour représenter la machine d'emballage et observer comment l'OEE est AWS IoT SiteWise calculée.

Définissez les mesures suivantes pour représenter les flux de données brutes de la machine de conditionnement.

Mesures

- `Equipment_State`— Un flux de données (ou mesure) qui fournit l'état actuel de la machine d'emballage sous forme de codes numériques :
  - `1024`— La machine est inactive.
  - `1020`— Un défaut, tel qu'une erreur ou un retard.
  - `1000`— Un arrêt planifié.
  - `1111`— Un fonctionnement normal.
- `Good_Count`— Un flux de données dans lequel chaque point de données contient le nombre d'opérations réussies depuis le dernier point de données.
- `Bad_Count`— Un flux de données dans lequel chaque point de données contient le nombre d'opérations infructueuses depuis le dernier point de données.

À l'aide du flux de données de mesure `Equipment_State` et des codes qu'il contient, définissez les transformations (ou mesures dérivées) suivantes. Les transformations ont une one-to-one relation avec les mesures brutes.

Transformations

- `Idle = eq(Equipment_State, 1024)`— Un flux de données transformé qui contient l'état inactif de la machine.
- `Fault = eq(Equipment_State, 1020)`— Un flux de données transformé qui contient l'état de défaillance de la machine.
- `Stop = eq(Equipment_State, 1000)`— Un flux de données transformé qui contient l'état d'arrêt prévu de la machine.
- `Running = eq(Equipment_State, 1111)`— Un flux de données transformé qui contient l'état de fonctionnement normal de la machine.

À l'aide des mesures brutes et transformées, définissez les métriques suivantes qui regroupent les données machine sur des intervalles de temps spécifiés. Choisissez le même intervalle de temps pour chaque métrique lorsque vous définissez les métriques dans cette section.

Métriques

- `Successes = sum(Good_Count)`— Le nombre de colis remplis avec succès au cours de l'intervalle de temps spécifié.
- `Failures = sum(Bad_Count)`— Le nombre de colis remplis sans succès au cours de l'intervalle de temps spécifié.
- `Idle_Time = statetime(Idle)`— Durée totale d'inactivité de la machine (en secondes) par intervalle de temps spécifié.
- `Fault_Time = statetime(Fault)`— Durée totale de panne de la machine (en secondes) par intervalle de temps spécifié.
- `Stop_Time = statetime(Stop)`— Le temps d'arrêt total prévu de la machine (en secondes) par intervalle de temps spécifié.
- `Run_Time = statetime(Running)`— Durée totale (en secondes) de fonctionnement de la machine sans problème par intervalle de temps spécifié.
- `Down_Time = Idle_Time + Fault_Time + Stop_Time`— Le temps d'arrêt total de la machine (en secondes) sur l'intervalle de temps spécifié, calculé comme la somme des états de la machine autres que`Run_Time`.

- `Availability = Run_Time / (Run_Time + Down_Time)`— Temps de disponibilité de la machine ou pourcentage du temps prévu pendant lequel la machine est disponible pour fonctionner pendant l'intervalle de temps spécifié.
- `Quality = Successes / (Successes + Failures)`— Le pourcentage de colis remplis avec succès par la machine sur les intervalles de temps spécifiés.
- `Performance = ((Successes + Failures) / Run_Time) / Ideal_Run_Rate`— Les performances de la machine sur l'intervalle de temps spécifié, en pourcentage par rapport à la cadence de fonctionnement idéale (en secondes) pour votre processus.

  Par exemple, `Ideal_Run_Rate` peut être de 60 paquets par minute (1 paquet par seconde). Si votre `Ideal_Run_Rate` valeur est exprimée par minute ou par heure, vous devez la diviser par le facteur de conversion unitaire approprié, car il `Run_Time` est exprimé en secondes.
- `OEE = Availability * Quality * Performance`— L'efficacité globale de l'équipement de la machine sur l'intervalle de temps spécifié. Cette formule calcule l'OEE comme une fraction de 1.

Ingestion de données provenant d'objets AWS IoT

Découvrez comment intégrer des données à AWS IoT SiteWise partir d'un parc d' AWS IoT objets en utilisant les ombres des appareils dans ce didacticiel. Les ombres de périphérique sont des objets JSON qui stockent les informations d'état actuel d'un AWS IoT appareil. Pour plus d'informations, voir Device Shadow Service dans le Guide du AWS IoT développeur.

Après avoir terminé ce didacticiel, vous pouvez configurer une opération en AWS IoT SiteWise fonction AWS IoT des éléments. En utilisant AWS IoT des objets, vous pouvez intégrer vos opérations à d'autres fonctionnalités utiles de AWS IoT. Par exemple, vous pouvez configurer les AWS IoT fonctionnalités pour effectuer les tâches suivantes :

- Configurez des règles supplémentaires pour diffuser des données vers Amazon DynamoDB AWS IoT Events, etc. Services AWS Pour plus d'informations, consultez la section Règles du guide du AWS IoT développeur.
- Indexez, recherchez et agrégez les données de vos appareils grâce au service d'indexation de AWS IoT flotte. Pour plus d'informations, consultez la section Service d'indexation de flotte dans le Guide du AWS IoT développeur.
- Auditez et sécurisez vos appareils avec AWS IoT Device Defender. Pour plus d'informations, consultez AWS IoT Device Defender dans le Guide du développeur AWS IoT .

Dans ce didacticiel, vous allez apprendre à ingérer des données depuis les zones d'ombre AWS IoT des appareils vers les actifs qu'ils contiennent. AWS IoT SiteWise Pour ce faire, vous créez un ou plusieurs AWS IoT éléments et exécutez un script qui met à jour l'ombre du périphérique de chaque élément avec les données d'utilisation du processeur et de la mémoire. Vous utiliserez les données d'utilisation de l'UC et de la mémoire dans ce didacticiel pour imiter des données de capteur réalistes. Ensuite, vous créez une règle avec une AWS IoT SiteWise action qui envoie ces données à un actif AWS IoT SiteWise chaque fois que le device shadow d'un objet est mis à jour. Pour plus d'informations, consultez Ingestion de données à l'aide de règles AWS IoT Core.

Rubriques

- Prérequis
- Étape 1 : Création d'une AWS IoT politique
- Étape 2 : Création et configuration d'un AWS IoT objet
- Étape 3 : Création d'un modèle de ressource d'appareil
- Étape 4 : Création d'un modèle d'actifs de parc d'appareils
- Étape 5 : Création et configuration d'un actif de terminal
- Étape 6 : Création et configuration d'un parc d'appareils
- Étape 7 : Création d'une règle dans AWS IoT Core pour envoyer des données aux actifs de l'appareil
- Étape 8 : Exécution du script client de l'appareil
- Étape 9 : Nettoyage des ressources après le didacticiel

Prérequis

Pour suivre ce didacticiel, vous aurez besoin des éléments suivants :

- Un Compte AWS. Si vous n'en avez pas, veuillez consulter Configuration d'un Compte AWS.
- Un ordinateur de développement exécutant WindowsmacOS,Linux, ou Unix permettant d'accéder au AWS Management Console. Pour plus d'informations, consultez Démarrer avec le AWS Management Console.
- Un utilisateur AWS Identity and Access Management (IAM) doté d'autorisations d'administrateur.
- Python3 installé sur votre ordinateur de développement ou installé sur l'appareil que vous souhaitez enregistrer en tant qu' AWS IoT objet.

Étape 1 : Création d'une AWS IoT politique

Dans cette procédure, créez une AWS IoT politique permettant à vos AWS IoT objets d'accéder aux ressources utilisées dans ce didacticiel.

Pour créer une AWS IoT politique

1. Connectez-vous à la AWS Management Console.
2. Passez en revue les AWS régions dans lesquelles le AWS IoT SiteWise support est pris en charge. Basculez vers l'une de ces régions prises en charge, si nécessaire.
3. Accédez à la console AWS IoT. Si un bouton Connect device apparaît, choisissez-le.
4. Dans le volet de navigation de gauche, choisissez Security, puis Policies.
5. Choisissez Créer.
6. Entrez le nom de la AWS IoT politique (par exemple,**`SiteWiseTutorialDevicePolicy`**).
7. Sous Document de stratégie, choisissez JSON pour saisir la politique suivante au format JSON. Remplacez *`la région`* et l'*`identifiant du compte`* par votre région et votre numéro de compte, tels que **`us-east-1`** et. **`123456789012`**

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

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

Cette politique permet à vos AWS IoT appareils d'établir des connexions et de communiquer avec leurs ombres à l'aide de messages MQTT. Pour plus d'informations sur les messages MQTT, consultez Qu'est-ce que MQTT ? . Pour interagir avec les ombres des appareils, vos AWS IoT objets publient et reçoivent des messages MQTT sur des sujets commençant `$aws/things/`*`thing-name`*`/shadow/` par. Cette politique intègre une variable de politique d'objets connue sous le nom de`${iot:Connection.Thing.ThingName}`. Cette variable remplace le nom de l'objet connecté dans chaque rubrique. L'`iot:Connect`instruction définit des limites quant aux appareils autorisés à établir des connexions, en veillant à ce que la variable thing policy ne puisse remplacer que les noms commençant par`SiteWiseTutorialDevice`.

Pour plus d'informations, consultez la section Variables de politique des objets dans le manuel du AWS IoT développeur.

> **Note**
>
> Cette stratégie s'applique aux objets dont le nom commence par `SiteWiseTutorialDevice`. Pour utiliser un nom différent pour vos objets, vous devez mettre à jour la stratégie en conséquence.

8. Sélectionnez Create (Créer).

Étape 2 : Création et configuration d'un AWS IoT objet

Dans cette procédure, vous créez et configurez n'importe quel AWS IoT objet. Vous pouvez désigner votre ordinateur de développement comme n'importe quel AWS IoT objet. Au fur et à mesure que vous progressez, n'oubliez pas que les principes que vous apprenez ici peuvent être appliqués à des projets réels. Vous avez la flexibilité de créer et de configurer des AWS IoT éléments sur n'importe quel appareil capable d'exécuter un AWS IoT SDK, y compris AWS IoT Greengrass FreeRTOS. Pour plus d'informations, consultez la section AWS IoT SDK dans le guide du AWS IoT développeur.

Pour créer et configurer n'importe quel AWS IoT objet

1. Ouvrez une ligne de commande et exécutez la commande suivante pour créer un répertoire pour ce didacticiel.

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

2. Exécutez la commande suivante pour créer un répertoire pour les certificats de l'objet.

```
mkdir device1
```

   Si vous créez des objets supplémentaires, incrémentez le nombre en conséquence dans le nom du répertoire pour pouvoir déterminer quel certificat appartient à quel objet.

3. Accédez à la console AWS IoT.
4. Dans le volet de navigation de gauche, choisissez Tous les appareils dans la section Gérer. Ensuite, choisissez Things (Objets).
5. Si une boîte de dialogue You don't have any things yet (Vous n'avez pas encore d'objet) s'affiche, choisissez Create a thing (Créer un objet). Sinon, choisissez Create things.
6. Sur la page Création d'objets, choisissez Créer un objet unique, puis cliquez sur Suivant.
7. Sur la page Spécifier les propriétés de l'objet, entrez le nom de votre AWS IoT objet (par exemple,**`SiteWiseTutorialDevice1`**) puis choisissez Suivant. Si vous créez des objets supplémentaires, incrémentez le nombre en conséquence dans le nom de l'objet.

   > **Important**
   >
   > Le nom de l'objet doit correspondre au nom utilisé dans la politique que vous avez créée à l'étape 1 : Création d'une AWS IoT politique. Dans le cas contraire, votre appareil ne pourra pas se connecter à AWS IoT.

8. Sur la page Configurer le certificat de l'appareil - facultatif, choisissez Générer automatiquement un nouveau certificat (recommandé) puis cliquez sur Suivant. Les certificats permettent AWS IoT d'identifier vos appareils en toute sécurité.
9. Sur la page facultative Attacher des politiques au certificat, sélectionnez la politique que vous avez créée à l'étape 1 : Création d'une AWS IoT politique, puis choisissez Créer un objet.
10. Dans la boîte de dialogue Télécharger les certificats et les clés, procédez comme suit :

    a. Choisissez les liens Télécharger pour télécharger le certificat, la clé publique et la clé privée de votre objet. Enregistrez les trois fichiers dans le répertoire que vous avez créé pour les certificats de l'objet (par exemple, `iot-sitewise-rule-tutorial/device1`).

> **Important**
>
> Il s'agit de l'unique fois où vous pouvez télécharger le certificat et les clés de l'objet, sans lesquels votre appareil ne pourra pas se connecter à AWS IoT.

b. Cliquez sur le lien Télécharger pour télécharger un certificat CA racine. Enregistrez le certificat d'autorité de certification racine dans `iot-sitewise-rule-tutorial`. Nous vous recommandons de télécharger Amazon Root CA 1.

11. Sélectionnez Exécuté.

Vous avez maintenant enregistré AWS IoT quelque chose sur votre ordinateur. Procédez à l'une des étapes suivantes :

- Passez à l'étape 3 : Création d'un modèle de ressource d'appareil sans créer d' AWS IoT éléments supplémentaires. Vous pouvez réaliser ce didacticiel avec un seul objet.
- Répétez les étapes de cette section sur un autre ordinateur ou périphérique pour créer d'autres objets AWS IoT . Pour ce didacticiel, nous vous recommandons de suivre cette étape afin que vous puissiez ingérer des données d'utilisation d'UC et de mémoire uniques à partir de plusieurs appareils.
- Répétez les étapes de cette section sur le même périphérique (ordinateur) pour créer davantage d'objets AWS IoT . Chaque AWS IoT appareil reçoit des données d'utilisation du processeur et de la mémoire similaires de votre ordinateur. Utilisez cette approche pour démontrer l'ingestion de données non uniques provenant de plusieurs appareils.

Étape 3 : Création d'un modèle de ressource d'appareil

Dans cette procédure, vous créez un modèle d'actif AWS IoT SiteWise pour représenter vos appareils qui diffusent des données d'utilisation du processeur et de la mémoire. Pour traiter les données des actifs qui représentent des groupes d'appareils, les modèles d'actifs appliquent des informations cohérentes sur plusieurs actifs du même type. Pour plus d'informations, consultez Modélisation des ressources industrielles.

Pour créer un modèle de ressource qui représente un périphérique

1. Accédez à la console AWS IoT SiteWise.
2. Dans le volet de navigation de gauche, choisissez Models (Modèles).

3. Sélectionnez Create model.
4. Sous Détails du modèle, entrez le nom de votre modèle. Par exemple, **`SiteWise Tutorial Device Model`**.
5. Sous Measurement definitions (Définitions de mesure), procédez comme suit :

   a. Pour Name (Nom), entrez **`CPU Usage`**.

   b. Pour Unit (Unité), saisissez **`%`**.

   c. Conservez le type de données Double.

   Les propriétés de mesure représentent les flux de données brutes d'un périphérique. Pour plus d'informations, consultez Définition des flux de données provenant des équipements (mesures).
6. Choisissez Ajouter une nouvelle mesure pour ajouter une deuxième propriété de mesure.
7. Dans la deuxième ligne sous Measurement definitions (Définitions de mesure), procédez comme suit :

   a. Pour Name (Nom), entrez **`Memory Usage`**.

   b. Pour Unit (Unité), saisissez **`%`**.

   c. Conservez le type de données Double.
8. Sous Metric definitions (Définitions de métrique), procédez comme suit :

   a. Pour Name (Nom), entrez **`Average CPU Usage`**.

   b. Pour Formula (Formule), saisissez **`avg(CPU Usage)`**. Choisissez CPU Usage dans la liste de saisie semi-automatique lorsqu'elle apparaît.

   c. Dans Time interval (Intervalle de temps), entrez **`5 minutes`**.

   Les propriétés de métrique définissent les calculs d'agrégation qui traitent tous les points de données en entrée sur un intervalle et qui produisent un point de données unique par intervalle. Cette propriété de métrique calcule l'utilisation moyenne de l'UC de chaque périphérique toutes les 5 minutes. Pour plus d'informations, consultez Agrégation de données provenant de propriétés et d'autres actifs (métriques).
9. Choisissez Ajouter une nouvelle métrique pour ajouter une deuxième propriété de métrique.
10. Dans la deuxième ligne sous Metric definitions (Définitions de métrique), procédez comme suit :

    a. Pour Name (Nom), entrez **`Average Memory Usage`**.

b. Pour Formula (Formule), saisissez **`avg(Memory Usage)`**. Choisissez Memory Usage dans la liste de saisie semi-automatique lorsqu'elle apparaît.

c. Dans Time interval (Intervalle de temps), entrez **`5 minutes`**.

Cette propriété de métrique calcule l'utilisation moyenne de la mémoire de chaque périphérique toutes les 5 minutes.

11. (Facultatif) Ajoutez les autres métriques que vous souhaitez calculer pour chaque périphérique. Certaines fonctions intéressantes comprennent `min` et `max`. Pour plus d'informations, consultez Utilisation d'expressions de formule. À l'étape 4 : Création d'un modèle d'actifs de parc d'appareils, vous créez un actif parent capable de calculer des mesures à l'aide des données de l'ensemble de votre parc d'appareils.
12. Sélectionnez Create model.

Étape 4 : Création d'un modèle d'actifs de parc d'appareils

Dans cette procédure, vous créez un modèle de ressource AWS IoT SiteWise pour symboliser votre collection d'appareils. Dans ce modèle d'actifs, vous établissez une structure qui vous permet de relier de nombreux équipements à un actif de flotte global. Ensuite, vous définissez les mesures du modèle d'actifs du parc afin de consolider les données de tous les actifs des appareils connectés. Cette approche vous fournit des informations complètes sur les performances collectives de l'ensemble de votre flotte.

Pour créer un modèle de ressource qui représente un parc de périphériques

1. Accédez à la console AWS IoT SiteWise.
2. Dans le volet de navigation de gauche, choisissez Models (Modèles).
3. Sélectionnez Create model.
4. Sous Détails du modèle, entrez le nom de votre modèle. Par exemple, **`SiteWise Tutorial Device Fleet Model`**.
5. Sous Hierarchy definitions (Définitions de hiérarchie), procédez comme suit :

   a. Dans Hierarchy name (Nom de la hiérarchie), entrez **`Device`**.

   b. Dans Hierarchy model (Modèle de hiérarchie), choisissez votre modèle de ressource de périphérique (**`SiteWise Tutorial Device Model`**).

Une hiérarchie définit une relation entre un modèle de ressource parent (parc) et un modèle de ressource enfant (périphérique). Les ressources parents peuvent accéder aux données de propriété des ressources enfants. Lorsque vous créerez des ressources par la suite, vous devrez associer des ressources enfants aux ressources parents selon une définition de hiérarchie dans le modèle de ressource parent. Pour plus d'informations, consultez Définition de hiérarchies de modèles d'actifs.

6. Sous Metric definitions (Définitions de métrique), procédez comme suit :

   a. Pour Name (Nom), entrez **`Average CPU Usage`**.

   b. Pour Formula (Formule), saisissez **`avg(Device | Average CPU Usage)`**. Lorsque la liste de saisie semi-automatique apparaît, choisissez Device pour sélectionner une hiérarchie, puis choisissez Average CPU Usage pour sélectionner la métrique à partir de la ressource de périphérique que vous avez créée précédemment.

   c. Dans Time interval (Intervalle de temps), entrez **`5 minutes`**.

   Cette propriété de métrique calcule l'utilisation moyenne de l'UC de toutes les ressources de périphériques associées à une ressource de parc via la hiérarchie **`Device`**.

7. Choisissez Ajouter une nouvelle métrique pour ajouter une deuxième propriété de métrique.

8. Dans la deuxième ligne sous Metric definitions (Définitions de métrique), procédez comme suit :

   a. Pour Name (Nom), entrez **`Average Memory Usage`**.

   b. Pour Formula (Formule), saisissez **`avg(Device | Average Memory Usage)`**. Lorsque la liste de saisie semi-automatique apparaît, choisissez Device pour sélectionner une hiérarchie, puis choisissez Average Memory Usage pour sélectionner la métrique à partir de la ressource de périphérique que vous avez créée précédemment.

   c. Dans Time interval (Intervalle de temps), entrez **`5 minutes`**.

   Cette propriété de métrique calcule l'utilisation moyenne de la mémoire de toutes les ressources de périphériques associées à une ressource de parc via la hiérarchie **`Device`**.

9. (Facultatif) Ajoutez les autres métriques que vous souhaitez calculer pour l'ensemble de votre parc de périphériques.

10. Sélectionnez Create model.

Étape 5 : Création et configuration d'un actif de terminal

Dans cette procédure, vous générez un actif d'appareil basé sur le modèle d'actif de votre appareil. Ensuite, vous définirez des alias de propriété pour chaque propriété de mesure. Un alias de propriété est une chaîne unique qui identifie la propriété d'un actif. Plus tard, vous pourrez identifier une propriété pour le téléchargement des données en utilisant les alias au lieu de l'ID de ressource et de l'ID de propriété. Pour plus d'informations, consultez Mappage des flux de données industrielles avec des propriétés de ressources.

Pour créer une ressource de périphérique et définir des alias de propriété

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation de gauche, choisissez Assets (Ressources).
3. Choisissez Create asset (Créer une ressource).
4. Sous Informations sur le modèle, choisissez le modèle de ressource de votre appareil,**`SiteWise Tutorial Device Model`**.
5. Sous Informations sur l'actif, entrez le nom de votre actif. Par exemple, **`SiteWise Tutorial Device 1`**.
6. Choisissez Create asset (Créer une ressource).
7. Pour la nouvelle ressource de périphérique, choisissez Edit (Modifier).
8. Sous CPU Usage, entrez **`/tutorial/device/SiteWiseTutorialDevice1/cpu`** comme alias de propriété. Vous incluez le nom de l' AWS IoT objet dans l'alias de propriété, afin de pouvoir ingérer les données de tous vos appareils à l'aide d'une seule AWS IoT règle.
9. Sous Memory Usage, entrez **`/tutorial/device/SiteWiseTutorialDevice1/memory`** comme alias de propriété.
10. Choisissez Enregistrer.

Si vous avez créé plusieurs AWS IoT éléments précédemment, répétez les étapes 3 à 10 pour chaque appareil, puis incrémentez le numéro dans le nom de l'actif et les alias de propriété en conséquence. Par exemple, le nom de la deuxième ressource de périphérique doit être **`SiteWise Tutorial Device 2`**, et ses alias de propriété doivent être **`/tutorial/device/SiteWiseTutorialDevice2/cpu`** et **`/tutorial/device/SiteWiseTutorialDevice2/memory`**.

Étape 6 : Création et configuration d'un parc d'appareils

Dans cette procédure, vous créez un actif de parc d'appareils dérivé de votre modèle d'actifs de parc d'appareils. Ensuite, vous associez les actifs de vos appareils individuels à l'actif du parc. Cette association permet aux propriétés métriques de l'actif du parc de compiler et d'analyser les données provenant de plusieurs appareils. Ces données vous fournissent une vue consolidée des performances collectives de l'ensemble de la flotte.

Pour créer une ressource de parc de périphériques et associer des ressources de périphérique

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation de gauche, choisissez Assets (Ressources).
3. Choisissez Create asset (Créer une ressource).
4. Sous Informations sur le modèle, choisissez le modèle d'actif de votre parc d'appareils,**`SiteWise Tutorial Device Fleet Model`**.
5. Sous Informations sur l'actif, entrez le nom de votre actif. Par exemple, **`SiteWise Tutorial Device Fleet 1`**.
6. Choisissez Create asset (Créer une ressource).
7. Pour la nouvelle ressource de parc de périphériques, choisissez Edit (Modifier).
8. Sous Ressources associées à cette ressource, choisissez Ajouter une ressource associée et procédez comme suit :

   a. Sous Hierarchy (Hiérarchie), choisissez Device. Cette hiérarchie identifie la relation hiérarchique entre les ressources de périphériques et de parc de périphériques. Vous avez défini cette hiérarchie dans le modèle de ressource de parc de périphériques précédemment dans ce didacticiel.

   b. Sous Asset (Ressource), sélectionnez votre ressource de périphérique, SiteWise Tutorial Device 1.
9. (Facultatif) Si vous avez créé plusieurs actifs d'appareil précédemment, répétez les étapes 8 à 10 pour chaque actif d'appareil que vous avez créé.
10. Choisissez Enregistrer.

    Vous devriez maintenant voir les ressources de votre périphérique organisées sous forme de hiérarchie.

Étape 7 : Création d'une règle dans AWS IoT Core pour envoyer des données aux actifs de l'appareil

Dans cette procédure, vous établissez une règle dans AWS IoT Core. La règle est conçue pour interpréter les messages de notification provenant des ombres de l'appareil et pour transmettre les données aux actifs de votre appareil en AWS IoT SiteWise.Chaque fois que le shadow de votre appareil est mis à jour, un AWS IoT message MQTT est envoyé. Vous pouvez créer une règle qui effectue des actions spécifiques lorsque les ombres de périphérique changent en fonction du message MQTT. Dans ce cas, l'objectif est de gérer le message de mise à jour, d'extraire les valeurs des propriétés et de les transmettre aux actifs de votre appareil dans AWS IoT SiteWise.

Pour créer une règle avec une AWS IoT SiteWise action

1. Accédez à la console AWS IoT.
2. Dans le volet de navigation de gauche, choisissez Routage des messages, puis sélectionnez Règles.
3. Choisissez Créer une règle.
4. Entrez un nom et une description pour votre règle, puis choisissez Next.
5. Entrez l'instruction SQL suivante, puis choisissez Next.

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

   Cette instruction de requête de règle fonctionne, car le service d'ombres de périphérique publie les mises à jour des ombres vers `$aws/things/thingName/shadow/update/accepted`. Pour plus d'informations sur le Device Shadow, voir Device Shadow Service dans le Guide du AWS IoT développeur.

   Dans la clause `WHERE`, cette instruction de requête de règle utilise la fonction `topic(3)` pour obtenir le nom de l'objet à partir du troisième segment de la rubrique. Ensuite, l'instruction filtre les périphériques dont les noms ne correspondent pas à ceux des périphériques du didacticiel. Pour plus d'informations sur le AWS IoT SQL, consultez la référence AWS IoT SQL dans le Guide du AWS IoT développeur.

6. Sous Actions de règle, choisissez Envoyer les données des messages aux propriétés des actifs dans AWS IoT SiteWise et procédez comme suit :

   a. Choisissez By property alias (Par alias de propriété).

   b. Dans Property alias (Alias de propriété), entrez **`/tutorial/device/${topic(3)}/cpu`**.

      La `${...}` syntaxe est un modèle de substitution. AWS IoT évalue le contenu à l'intérieur des bretelles. Ce modèle de substitution extrait le nom de l'objet à partir de la rubrique pour créer un alias spécifique à chaque objet. Pour plus d'informations, consultez la section Modèles de substitution dans le Guide du AWS IoT développeur.

      > **Note**
      >
      > Comme une expression dans un modèle de substitution est évaluée séparément de l'instruction `SELECT`, vous ne pouvez pas utiliser un modèle de substitution pour référencer un alias créé à l'aide d'une clause `AS`. Vous pouvez référencer uniquement les informations présentes dans la charge utile d'origine, en plus des fonctions et opérateurs pris en charge.

   c. Dans Numéro d'entrée - facultatif, entrez**`${concat(topic(3), "-cpu-", floor(state.reported.timestamp))}`**.

      Les ID d'entrée identifient de manière unique chaque tentative d'entrée de valeur. Si une entrée renvoie une erreur, vous pouvez trouver son ID dans l'erreur générée pour résoudre le problème. Le modèle de substitution de cet ID d'entrée combine le nom de l'objet et l'horodatage signalé du périphérique. Par exemple, l'ID d'entrée généré peut ressembler à `SiteWiseTutorialDevice1-cpu-1579808494`.

   d. Dans Time in seconds (Délai en secondes), entrez **`${floor(state.reported.timestamp)}`**.

      Ce modèle de substitution calcule le délai en secondes à compter de l'horodatage signalé du périphérique. Dans ce didacticiel, les périphériques signalent l'horodatage en secondes au format d'heure Unix epoch sous la forme d'un nombre à virgule flottante.

   e. Dans Décalage en nanos - facultatif, entrez**`${floor((state.reported.timestamp % 1) * 1E9)}`**.

      Ce modèle de substitution calcule le décalage en nanoseconde à compter du délai en secondes en convertissant la partie décimale de l'horodatage signalé du périphérique.

> **Note**
>
> AWS IoT SiteWise nécessite que vos données aient un horodatage actuel en temps réel à l'époque Unix. Si vos périphériques n'indiquent pas l'heure avec précision, vous pouvez obtenir l'heure actuelle à partir du moteur de règles AWS IoT avec timestamp(). Cette fonction signale le délai en millisecondes. Vous devez donc remplacer les paramètres de délai de l'action de règle par les valeurs suivantes :
>
> - Dans Time in seconds (Délai en secondes), entrez **`${floor(timestamp() / 1E3)}`**.
> - Dans Offset in nanos (Décalage en nanosecondes), entrez **`${(timestamp() % 1E3) * 1E6}`**.

f. Dans Data type (Type de données), choisissez Double.

   Ce type de données doit correspondre au type de données de la propriété de ressource que vous avez définie dans le modèle de ressource.

g. Dans Value (Valeur), entrez **`${state.reported.cpu}`**. Dans les modèles de substitution, vous utilisez l'opérateur **`.`** pour récupérer une valeur à partir d'une structure JSON.

h. Choisissez Add entry (Ajouter une entrée) pour ajouter une entrée pour la propriété d'utilisation de la mémoire et suivez à nouveau les étapes ci-dessous pour cette propriété :

   i. Choisissez By property alias (Par alias de propriété).

   ii. Dans Property alias (Alias de propriété), entrez **`/tutorial/device/${topic(3)}/memory`**.

   iii. Dans Numéro d'entrée - facultatif, entrez**`${concat(topic(3), "-memory-", floor(state.reported.timestamp))}`**.

   iv. Dans Time in seconds (Délai en secondes), entrez **`${floor(state.reported.timestamp)}`**.

   v. Dans Décalage en nanos - facultatif, entrez**`${floor((state.reported.timestamp % 1) * 1E9)}`**.

   vi. Dans Data type (Type de données), choisissez Double.

   vii. Dans Value (Valeur), entrez **`${state.reported.memory}`**.

i. Sous Rôle IAM, choisissez Créer un nouveau rôle pour créer un rôle IAM pour cette action de règle. Ce rôle permet AWS IoT de transférer les données vers les propriétés de votre parc d'appareils et de sa hiérarchie d'actifs.

j. Entrez un nom de rôle et choisissez Create.

7. (Facultatif) Configurez une action d'erreur que vous pouvez utiliser pour dépanner la règle. Pour plus d'informations, consultez Résolution des problèmes d'une règle.
8. Choisissez Suivant.
9. Vérifiez les paramètres et choisissez Créer pour créer la règle.

Étape 8 : Exécution du script client de l'appareil

Dans le cadre de ce didacticiel, vous n'utilisez pas un appareil réel pour communiquer des données. Au lieu de cela, vous exécutez un script pour mettre à jour l'ombre AWS IoT de l'appareil en fonction de l'utilisation du processeur et de la mémoire afin d'imiter les données réelles des capteurs. Pour exécuter le script, vous devez d'abord installer les Python packages requis. Dans cette procédure, vous installez les Python packages requis, puis vous exécutez le script client de l'appareil.

Pour configurer et exécuter le script client de périphérique

1. Accédez à la console AWS IoT.
2. En bas du volet de navigation de gauche, choisissez Settings (Paramètres).
3. Enregistrez le point de terminaison personnalisé pour l'utiliser avec le script client de périphérique. Vous utiliserez ce point de terminaison pour interagir avec les ombres de votre objet. Ce point de terminaison est unique à votre compte dans la région actuelle.

   Le point de terminaison personnalisé devrait ressembler à l'exemple suivant.

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

4. Ouvrez une ligne de commande et exécutez la commande suivante pour accéder au répertoire du didacticiel que vous avez créé précédemment.

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

5. Exécutez la commande suivante pour installer le kit Kit SDK des appareils AWS IoT pour Python.

   ```
   pip3 install AWSIoTPythonSDK
   ```

Pour plus d'informations, consultez Kit SDK des appareils AWS IoT pour Pythonle guide du AWS IoT développeur

6. Exécutez la commande suivante pour installer psutil, bibliothèque d'utilitaires système et de processus multiplateformes.

```
pip3 install psutil
```

Pour plus d'informations, consultez psutil dans l'index des packages Python.

7. Créez un fichier appelé `thing_performance.py` dans le répertoire `iot-sitewise-rule-tutorial`, puis copiez le code Python suivant dans le fichier.

```
import AWSIoTPythonSDK.MQTTLib as AWSIoTPyMQTT

import json
import psutil
import argparse
import logging
import time


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

```
        "-c",
        "--cert",
        action="store",
        required=True,
        dest="certificatePath",
        help="Certificate file path",
    )
    parser.add_argument(
        "-k",
        "--key",
        action="store",
        required=True,
        dest="privateKeyPath",
        help="Private key file path",
    )
    parser.add_argument(
        "-p",
        "--port",
        action="store",
        dest="port",
        type=int,
        default=8883,
        help="Port number override",
    )
    parser.add_argument(
        "-n",
        "--thingName",
        action="store",
        required=True,
        dest="thingName",
        help="Targeted thing name",
    )
    parser.add_argument(
        "-d",
        "--requestDelay",
        action="store",
        dest="requestDelay",
        type=float,
        default=1,
        help="Time between requests (in seconds)",
    )
    parser.add_argument(
        "-v",
        "--enableLogging",
```

```
        action="store_true",
        dest="enableLogging",
        help="Enable logging for the AWS IoT Device SDK for Python",
    )
    return parser


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

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

        print("Running performance shadow client for {}...
\n".format(self.thingName))
        while True:
            performance = self.readPerformance()
            print("[{}]".format(self.thingName))
```

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

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

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

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


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

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

8. Exécutez `thing_performance.py` depuis la ligne de commande avec les paramètres suivants :

   - `-n`, `--thingName` — Le nom de votre objet, tel que**`SiteWiseTutorialDevice1`**.
   - `-e`, `--endpoint` — Votre point de AWS IoT terminaison personnalisé que vous avez enregistré plus tôt dans cette procédure.
   - `-r`, `--rootCA` — Le chemin d'accès à votre certificat CA AWS IoT racine.
   - `-c`, `--cert` — Le chemin d'accès à votre certificat d' AWS IoT objet.
   - `-k`, `--key` — Le chemin d'accès à la clé privée de votre certificat d' AWS IoT objet.
   - `-d`, `--requestDelay` — (Facultatif) Temps d'attente en secondes entre chaque mise à jour instantanée de l'appareil. Par défaut, il correspond à 1 seconde.
   - `-v`, `--enableLogging` — (Facultatif) Si ce paramètre est présent, le script imprime des messages de débogage à partir du Kit SDK des appareils AWS IoT pour Python.

   La commande doit être similaire à l'exemple suivant :

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

```
  --key device1/thing-id-private.pem.key
```

Si vous exécutez le script pour d'autres AWS IoT éléments, mettez à jour le nom de l'objet et le répertoire des certificats en conséquence.

9. Essayez d'ouvrir et de fermer des programmes sur votre appareil pour voir comment évolue l'utilisation de l'UC et de la mémoire. Le script imprime chaque lecture de l'utilisation de l'UC et de la mémoire. Si le script charge des données vers le service d'ombres de périphérique avec succès, la sortie du script doit ressembler à l'exemple suivant.

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

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

10. Procédez comme suit pour vérifier que le script met à jour l'ombre du périphérique :

    a. Accédez à la console AWS IoT.

    b. Dans le volet de navigation de gauche, choisissez Tous les appareils, puis Objets.

    c. Choisissez votre truc, SiteWiseTutorialDevice.

    d. Choisissez l'onglet Device Shadows, choisissez Classic Shadow et vérifiez que l'état Shadow ressemble à l'exemple suivant.

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

    Si l'état fantôme de votre objet est vide ou ne ressemble pas à celui de l'exemple précédent, vérifiez que le script est en cours d'exécution et que vous y êtes connecté correctement AWS IoT. Si le script continue à expirer lors de la connexion à AWS IoT, vérifiez que votre politique d'objets est configurée conformément à ce didacticiel.

11. Procédez comme suit pour vérifier que l'action de règle envoie des données à AWS IoT SiteWise :

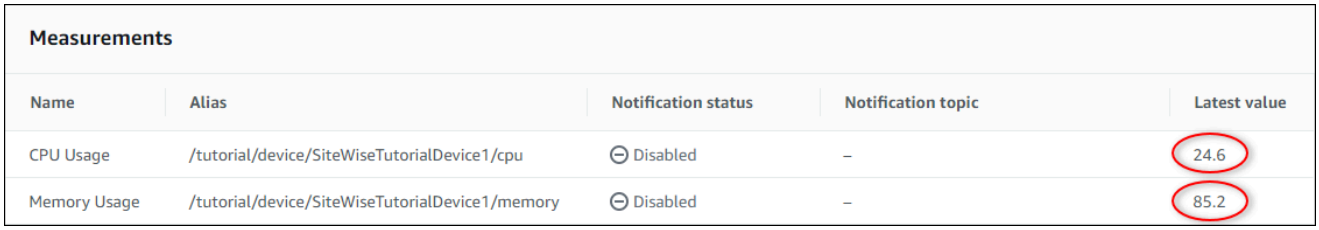
a. Accédez à la console AWS IoT SiteWise.

b. Dans le panneau de navigation de gauche, choisissez Assets (Ressources).

c. Sélectionnez la flèche en regard de votre parc de périphériques (SiteWise Tutorial Device Fleet 1 1) pour développer sa hiérarchie de ressources, puis choisissez votre ressource de périphérique (SiteWise Tutorial Device 1).

d. Choisissez Measurements (Mesures).

e. Vérifiez que les cellules Latest value (Valeur la plus récente) ont des valeurs pour les propriétés CPU Usage et Memory Usage.



f. Si les propriétés CPU Usage et Memory Usage n'ont pas les dernières valeurs, actualisez la page. Si aucune ligne n'apparaît après quelques minutes, consultez Résolution des problèmes d'une règle.

12. Vous avez terminé ce didacticiel. Si vous souhaitez explorer les visualisations en direct de vos données, vous pouvez configurer un portail dans AWS IoT SiteWise Monitor. Pour plus d'informations, consultez Surveillance des données avec AWS IoT SiteWise Monitor. Sinon, vous pouvez appuyer sur CTRL+C dans votre invite de commandes pour arrêter le script client du périphérique. Il est peu probable que le programme Python envoie suffisamment de messages pour générer des frais, mais il est recommandé d'arrêter le programme une fois que vous avez terminé.

Étape 9 : Nettoyage des ressources après le didacticiel

Après avoir terminé le didacticiel sur l'ingestion de données provenant d' AWS IoT objets, nettoyez vos ressources pour éviter d'encourir des frais supplémentaires.

Pour supprimer des actifs hiérarchiques dans AWS IoT SiteWise

1. Accédez à la AWS IoT SiteWise console
2. Dans le panneau de navigation de gauche, choisissez Assets (Ressources).
3. Lorsque vous supprimez des actifs AWS IoT SiteWise, vous devez d'abord les dissocier.

Procédez comme suit pour dissocier les ressources de périphérique de votre parc de périphériques :

a. Choisissez l'actif de votre parc d'appareils (SiteWise Tutorial Device Fleet 1).
b. Choisissez Modifier.
c. Sous Assets associated to this asset (Ressources associées à cette ressource), choisissez Disassociate (Dissocier) pour chaque ressource de périphérique associée à cette ressource de parc de périphériques.
d. Choisissez Enregistrer.

   Désormais, les ressources de votre périphérique ne devraient plus être organisées sous forme de hiérarchie.

4. Choisissez votre ressource de périphérique (SiteWise Tutorial Device 1).
5. Sélectionnez Delete (Supprimer).
6. Dans le champ de confirmation, entrez, **`Delete`**, puis choisissez Delete (Supprimer).
7. Répétez les étapes 4 à 6 pour chaque actif de l'appareil et pour le parc d'appareils (SiteWise Tutorial Device Fleet 1).

Pour supprimer des modèles d'actifs hiérarchiques dans AWS IoT SiteWise

1. Accédez à la console AWS IoT SiteWise.
2. Si vous ne l'avez pas déjà fait, supprimez vos périphériques et les ressources de votre parc de périphériques. Pour plus d'informations, consultez la procédure précédente. Vous ne pouvez pas supprimer un modèle s'il existe des ressources créées à partir de ce modèle.
3. Dans le volet de navigation de gauche, choisissez Models (Modèles).
4. Choisissez votre modèle de ressource de parc de périphériques (SiteWise Tutorial Device Fleet Model).

   Lorsque vous supprimez des modèles d'actifs hiérarchiques, commencez par supprimer d'abord le modèle d'actif parent.

5. Sélectionnez Delete (Supprimer).
6. Dans le champ de confirmation, entrez, **`Delete`**, puis choisissez Delete (Supprimer).
7. Répétez les étapes 4 à 6 pour le modèle de ressource de périphérique (SiteWise Tutorial Device Model Model).

Pour désactiver ou supprimer une règle dans AWS IoT Core

1. Accédez à la console AWS IoT.
2. Dans le volet de navigation de gauche, choisissez Routage des messages, puis Règles.
3. Sélectionnez votre règle, puis cliquez sur Supprimer.
4. Dans la boîte de dialogue de confirmation, entrez le nom de la règle, puis choisissez Supprimer.

Visualisation et partage des données des parcs éoliens dans Monitor SiteWise

Ce didacticiel explique comment visualiser et partager des données industrielles par le biais d'applications Web gérées, appelées portails. AWS IoT SiteWise Monitor Chaque portail englobe des projets, ce qui vous donne la possibilité de choisir les données accessibles au sein de chaque projet. Spécifiez ensuite les personnes de votre organisation qui peuvent accéder à chaque portail. Vos utilisateurs se connectent aux portails à l'aide de AWS IAM Identity Center comptes, afin que vous puissiez utiliser votre magasin d'identités existant ou un magasin géré par AWS.

Vous, ainsi que vos utilisateurs disposant d'autorisations suffisantes, pouvez créer des tableaux de bord dans chaque projet pour visualiser vos données industrielles de manière significative. Ensuite, vos utilisateurs peuvent consulter ces tableaux de bord pour obtenir rapidement des informations sur vos données et surveiller votre fonctionnement. Vous pouvez configurer des autorisations administratives ou en lecture seule pour chaque projet pour chaque utilisateur de votre entreprise. Pour plus d'informations, consultez Surveillance des données avec AWS IoT SiteWise Monitor.

Tout au long du didacticiel, vous améliorez la AWS IoT SiteWise démo en fournissant un exemple de jeu de données pour un parc éolien. Vous configurez un portail dans SiteWise Monitor, vous créez un projet et des tableaux de bord pour visualiser les données du parc éolien. Le didacticiel couvre également la création d'utilisateurs supplémentaires, ainsi que l'attribution d'autorisations pour posséder ou consulter le projet et ses tableaux de bord associés.

> **Note**
>
> Lorsque vous utilisez SiteWise Monitor, vous êtes facturé par utilisateur qui se connecte à un portail (par mois). Dans ce didacticiel, vous créez trois utilisateurs, mais vous ne devez vous connecter qu'avec un seul utilisateur. Après avoir terminé ce didacticiel, vous encourez des frais pour un utilisateur. Pour plus d'informations, consultez Tarification d'AWS IoT SiteWise.

Rubriques

- Prérequis
- Étape 1 : créer un portail dans SiteWise Monitor
- Étape 2 : Connectez-vous à un portail
- Étape 3 : Création d'un projet de parc éolien
- Étape 4 : Création d'un tableau de bord pour visualiser les données du parc éolien
- Étape 5 : Explorez le portail
- Étape 6 : Nettoyer les ressources après le didacticiel

Prérequis

Pour suivre ce didacticiel, vous aurez besoin des éléments suivants :

- Un Compte AWS. Si vous n'en avez pas, veuillez consulter Configuration d'un Compte AWS.
- Un ordinateur de développement exécutant WindowsmacOS,Linux, ou Unix permettant d'accéder au AWS Management Console. Pour plus d'informations, consultez Démarrer avec le AWS Management Console.
- Un utilisateur AWS Identity and Access Management (IAM) doté d'autorisations d'administrateur.
- Une démonstration de AWS IoT SiteWise parc éolien en cours d'exécution. Lorsque vous configurez la démo, elle définit les modèles et les actifs AWS IoT SiteWise et leur transmet des données pour représenter un parc éolien. Pour plus d'informations, consultez Utilisation de la AWS IoT SiteWise démo.
- Si vous avez activé IAM Identity Center dans votre compte, connectez-vous à votre compte AWS Organizations de gestion. Pour plus d'informations, veuillez consulter la rubrique Terminologie et concepts AWS Organizations. Si vous n'avez pas activé IAM Identity Center, vous allez l'activer dans ce didacticiel et définir votre compte comme compte de gestion.

  Si vous ne parvenez pas à vous connecter à votre compte de AWS Organizations gestion, vous pouvez suivre partiellement le didacticiel tant que votre organisation compte un utilisateur IAM Identity Center. Dans ce cas, vous pouvez créer le portail et les tableaux de bord, mais vous ne pouvez pas créer de nouveaux utilisateurs IAM Identity Center à affecter à des projets.

Étape 1 : créer un portail dans SiteWise Monitor

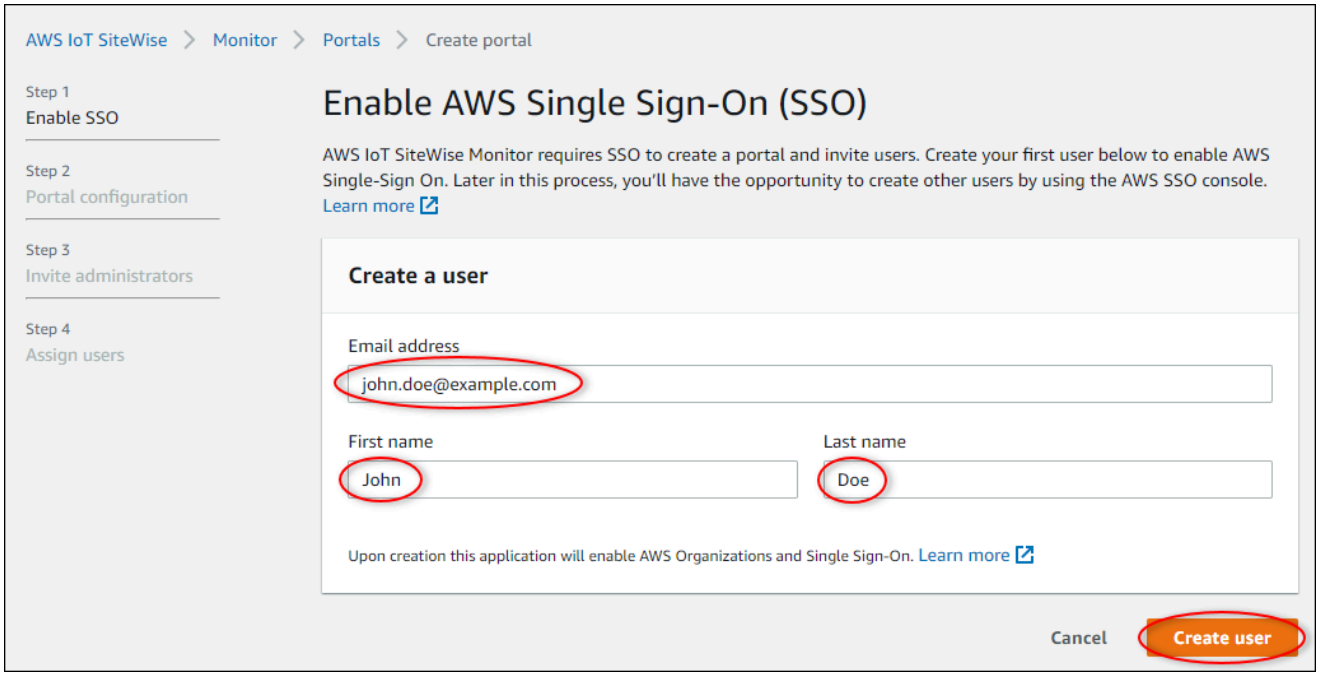
Dans cette procédure, vous créez un portail dans AWS IoT SiteWise Monitor. Chaque portail est une application Web gérée à laquelle vous et vos utilisateurs pouvez vous connecter à l'aide de AWS IAM Identity Center comptes. Avec IAM Identity Center, vous pouvez utiliser le magasin d'identités existant de votre entreprise ou en créer un géré par AWS. Les employés de votre entreprise peuvent se connecter sans créer de compte distinct Comptes AWS.

Pour créer un portail

1. Connectez-vous à la console AWS IoT SiteWise.
2. Passez en revue les AWS IoT SiteWise points de terminaison et les quotas pris en charge et changez de région, si nécessaire. AWS IoT SiteWise Vous devez exécuter la AWS IoT SiteWise démo dans la même région.
3. Dans le volet de navigation de gauche, choisissez Portals (Portails).
4. Choisissez Créer un portail.
5. Si vous avez déjà activé IAM Identity Center, passez à l'étape 6. Dans le cas contraire, procédez comme suit pour activer IAM Identity Center :

   a. Sur la page Activer AWS IAM Identity Center (SSO), entrez votre adresse e-mail, votre prénom et votre nom de famille pour créer un utilisateur IAM Identity Center en tant qu'administrateur du portail. Utilisez une adresse e-mail à laquelle vous pouvez accéder afin de recevoir un e-mail afin de définir un mot de passe pour votre nouvel utilisateur IAM Identity Center.

      Dans un portail, l'administrateur du portail crée des projets et affecte des utilisateurs à des projets. Vous pouvez créer plus d'utilisateurs ultérieurement.



b. Choisissez Create user (Créer un utilisateur).

6. Sur la page Portal configuration (Configuration du portail), procédez comme suit :

   a. Entrez un nom pour votre portail, tel que **`WindFarmPortal`**.

   b. (Facultatif) Saisissez une description pour votre portail. Si vous avez plusieurs portails, utilisez des descriptions significatives pour vous aider à suivre ce que contient chaque portail.

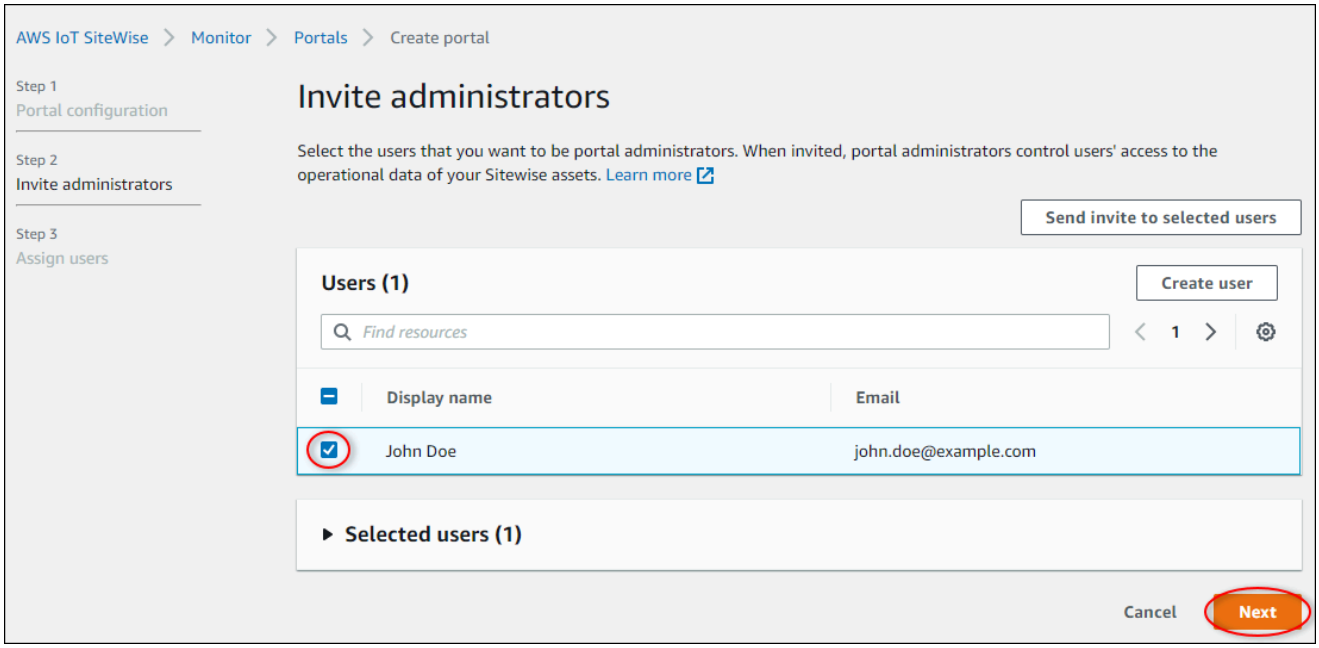
   c. (Facultatif) Téléchargez une image à afficher sur le portail.

   d. Entrez une adresse e-mail que les utilisateurs du portail peuvent contacter en cas de problème avec le portail et qu'ils ont besoin de l'aide de l' AWS administrateur de votre entreprise pour le résoudre.

   e. Choisissez Créer un portail.

7. Sur la page Inviter des administrateurs, vous pouvez affecter des utilisateurs d'IAM Identity Center au portail en tant qu'administrateurs. Les administrateurs du portail gèrent les autorisations et les projets au sein d'un portail. Sur cette page, effectuez les opérations suivantes :

   a. Sélectionnez un utilisateur comme administrateur du portail. Si vous avez activé IAM Identity Center plus tôt dans ce didacticiel, sélectionnez l'utilisateur que vous avez créé.



b. (Facultatif) Choisissez Envoyer l'invitation aux utilisateurs sélectionnés. Votre client de messagerie s'ouvre et une invitation apparaît dans le corps du message. Vous pouvez personnaliser l'e-mail avant de l'envoyer aux administrateurs de votre portail. Vous pouvez également envoyer l'e-mail aux administrateurs de votre portail ultérieurement. Si vous essayez SiteWise Monitor pour la première fois et que vous êtes l'administrateur du portail, vous n'avez pas besoin de vous envoyer un e-mail.

c. Choisissez Suivant.

8. Sur la page Attribuer des utilisateurs, vous pouvez attribuer des utilisateurs d'IAM Identity Center au portail. Les administrateurs du portail peuvent ultérieurement désigner ces utilisateurs en tant que propriétaires ou spectateurs du projet. Les propriétaires de projets peuvent créer des tableaux de bord dans les projets. Les visionneurs de projets ont un accès en lecture seule aux projets qui leur sont assignés. Sur cette page, vous pouvez créer des utilisateurs IAM Identity Center à ajouter au portail.

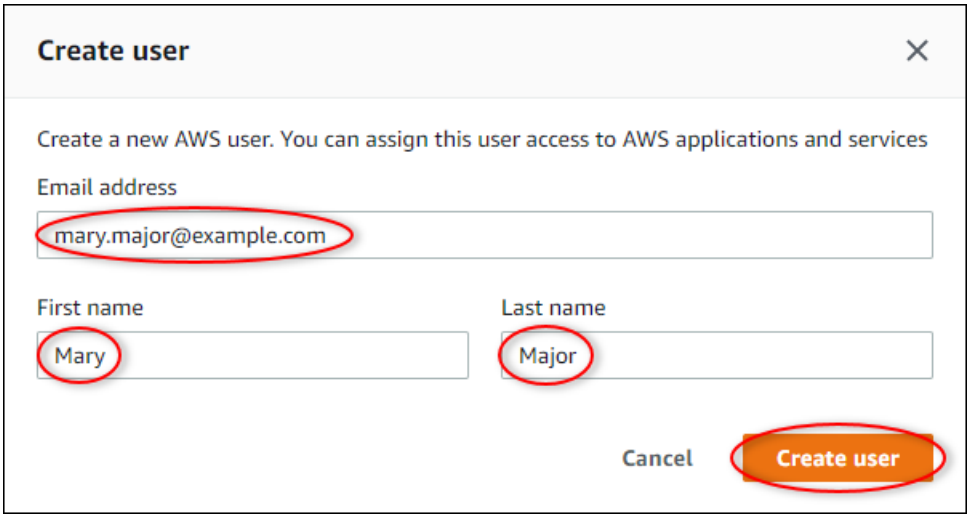
> **Note**
>
> Si vous n'êtes pas connecté à votre compte AWS Organizations de gestion, vous ne pouvez pas créer d'utilisateurs IAM Identity Center. Choisissez Affecter des utilisateurs pour créer le portail sans utilisateurs du portail, puis ignorez cette étape.

Sur cette page, effectuez les opérations suivantes :

a. Effectuez deux fois les étapes suivantes pour créer deux utilisateurs IAM Identity Center :

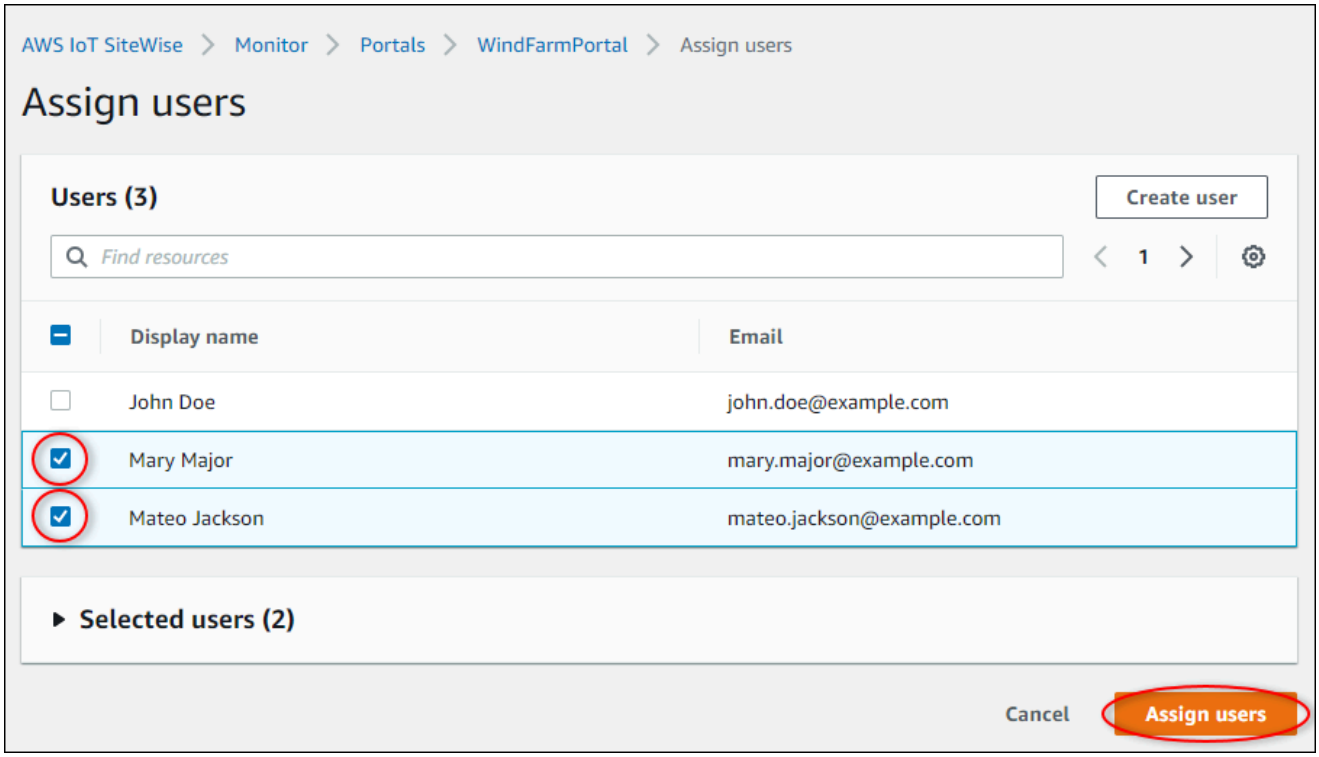
   i. Choisissez Créer un utilisateur pour ouvrir une boîte de dialogue dans laquelle vous entrez les informations relatives au nouvel utilisateur.

   ii. Entrez l'adresse e-mail, le prénom et le nom de famille du nouvel utilisateur. IAM Identity Center envoie un e-mail à l'utilisateur pour qu'il définisse son mot de passe. Si vous souhaitez vous connecter au portail en tant que ces utilisateurs, choisissez une adresse e-mail à laquelle vous pouvez accéder. Chaque adresse e-mail doit être unique. Vos utilisateurs se connectent au portail en utilisant leur adresse e-mail comme nom d'utilisateur.



   iii. Choisissez Create user (Créer un utilisateur).

b. Sélectionnez les deux utilisateurs IAM Identity Center que vous avez créés à l'étape précédente.



c. Choisissez Affecter des utilisateurs pour ajouter ces utilisateurs au portail.

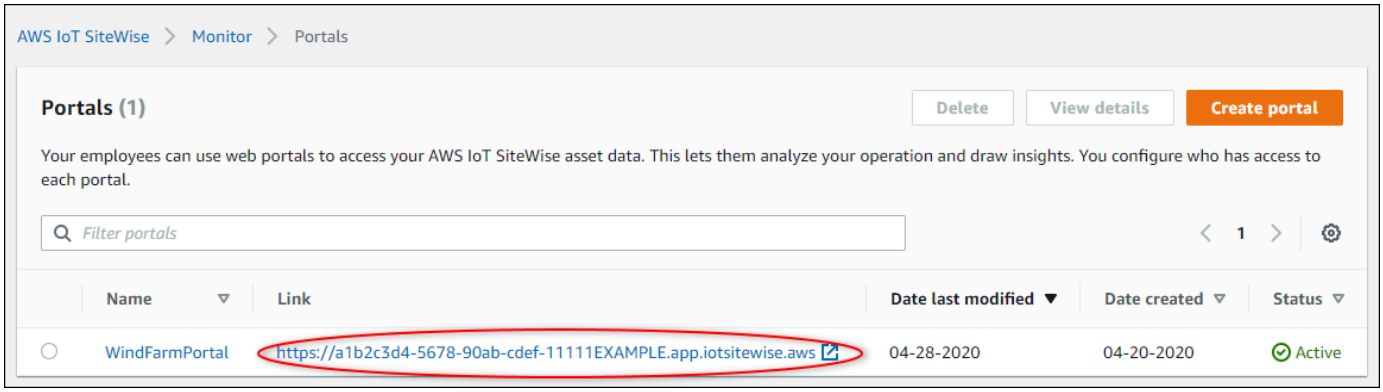
La page des portails s'ouvre avec votre nouveau portail répertorié.

Étape 2 : Connectez-vous à un portail

Dans cette procédure, vous vous connectez à votre nouveau portail en utilisant l' AWS IAM Identity Center utilisateur que vous avez ajouté au portail.

Pour vous connecter à un portail

1. Sur la page Portails choisissez le lien de votre nouveau portail pour ouvrir votre portail dans un nouvel onglet.



2. Si vous avez créé votre premier utilisateur IAM Identity Center plus tôt dans le didacticiel, suivez les étapes ci-dessous pour créer un mot de passe pour votre utilisateur :

   a. Vérifiez votre e-mail pour la ligne d'objet Invitation to join AWS IAM Identity Center.

   b. Ouvrez cet e-mail d'invitation et choisissez Accept invitation.

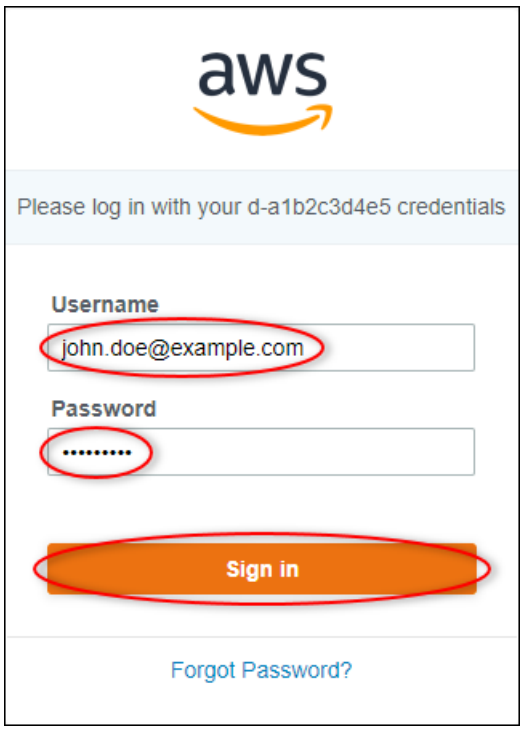
   c. Dans la nouvelle fenêtre, définissez un mot de passe pour votre utilisateur IAM Identity Center.

   Si vous souhaitez vous connecter ultérieurement au portail en tant que deuxième et troisième utilisateurs d'IAM Identity Center que vous avez créés précédemment, vous pouvez également suivre ces étapes pour définir des mots de passe pour ces utilisateurs.

   > **Note**
   >
   > Si vous n'avez pas reçu d'e-mail, vous pouvez générer un mot de passe pour votre utilisateur dans la console IAM Identity Center. Pour plus d'informations, voir Réinitialiser un mot de passe utilisateur dans le Guide de AWS IAM Identity Center l'utilisateur.

3. Entrez votre centre d'identité IAM Usernameet. Password Si vous avez créé votre utilisateur IAM Identity Center plus tôt dans ce didacticiel, Usernameil s'agit de l'adresse e-mail de l'utilisateur administrateur du portail que vous avez créé.

   Tous les utilisateurs du portail, y compris l'administrateur du portail, doivent se connecter à l'aide de leurs informations d'identification d'utilisateur IAM Identity Center. Ces informations d'identification ne sont généralement pas les mêmes que celles que vous utilisez pour vous connecter au AWS Management Console.



4. Sélectionnez Sign in.

   Votre portail s'ouvre.

Étape 3 : Création d'un projet de parc éolien

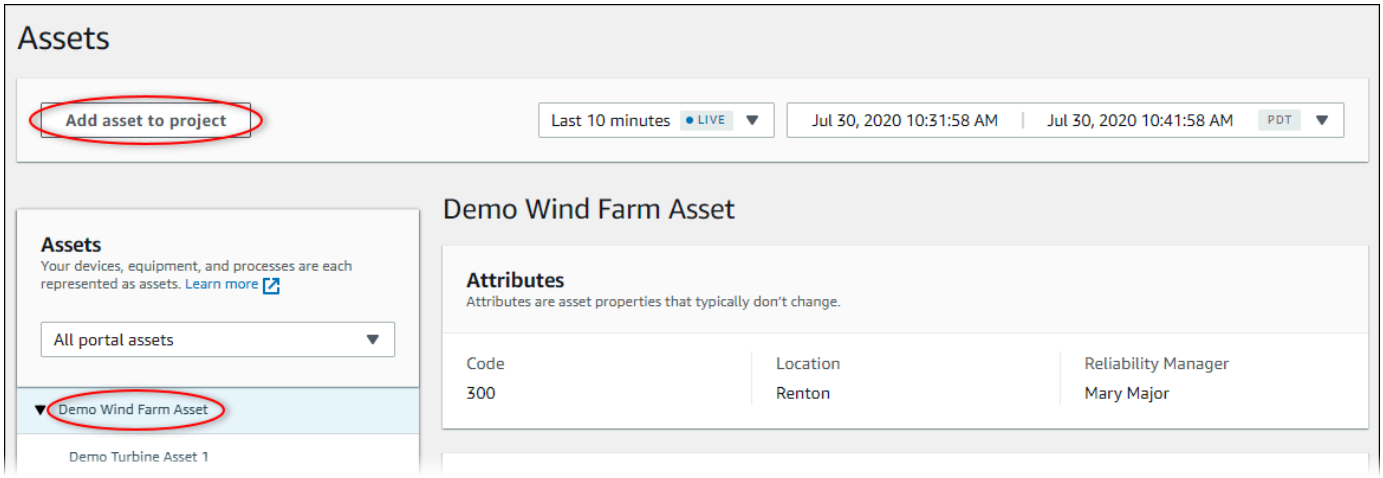
Dans cette procédure, vous créez un projet dans votre portail. Les projets sont des ressources qui définissent un ensemble d'autorisations, d'actifs et de tableaux de bord, que vous pouvez configurer pour visualiser les données des actifs dans ce projet. Avec les projets, vous définissez les personnes ayant accès aux sous-ensembles de votre opération et comment les données de ces sous-ensembles sont visualisées. Vous pouvez attribuer aux utilisateurs du portail les propriétaires ou les visualisateurs de chaque projet. Les propriétaires de projet peuvent créer des tableaux de bord pour visualiser les données et partager le projet avec d'autres utilisateurs. Les utilisateurs du projet peuvent afficher les tableaux de bord, mais pas les modifier. Pour plus d'informations sur les rôles dans SiteWise Monitor, consultezSiteWise Contrôler les rôles.

Pour créer un projet de parc éolien

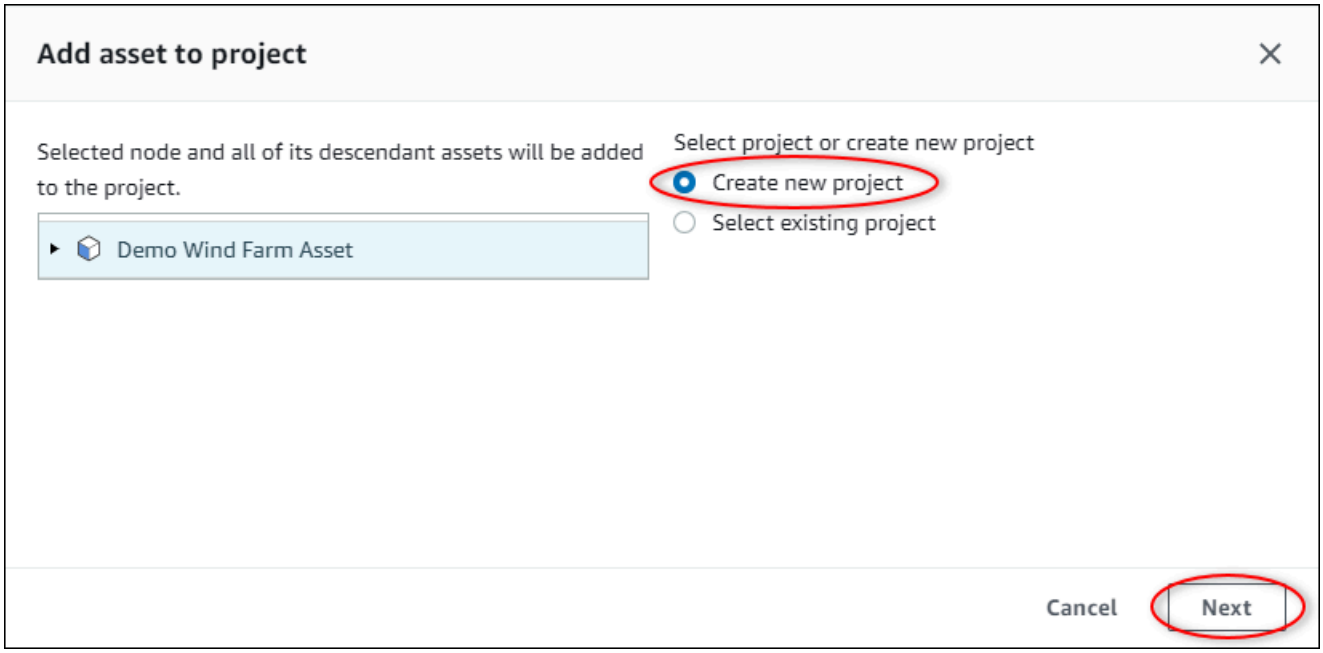
1. Dans le volet de navigation de gauche de votre portail, choisissez l'onglet Ressources. Sur la page Ressources, vous pouvez explorer toutes les ressources disponibles sur le portail et ajouter des ressources aux projets.

2. Dans le navigateur de ressources, choisissez Demo Wind Farm Asset. Lorsque vous choisissez un actif, vous pouvez explorer les données en temps réel et historiques de cet actif. Vous pouvez également appuyer Shift pour sélectionner plusieurs actifs et comparer leurs données side-by-side.

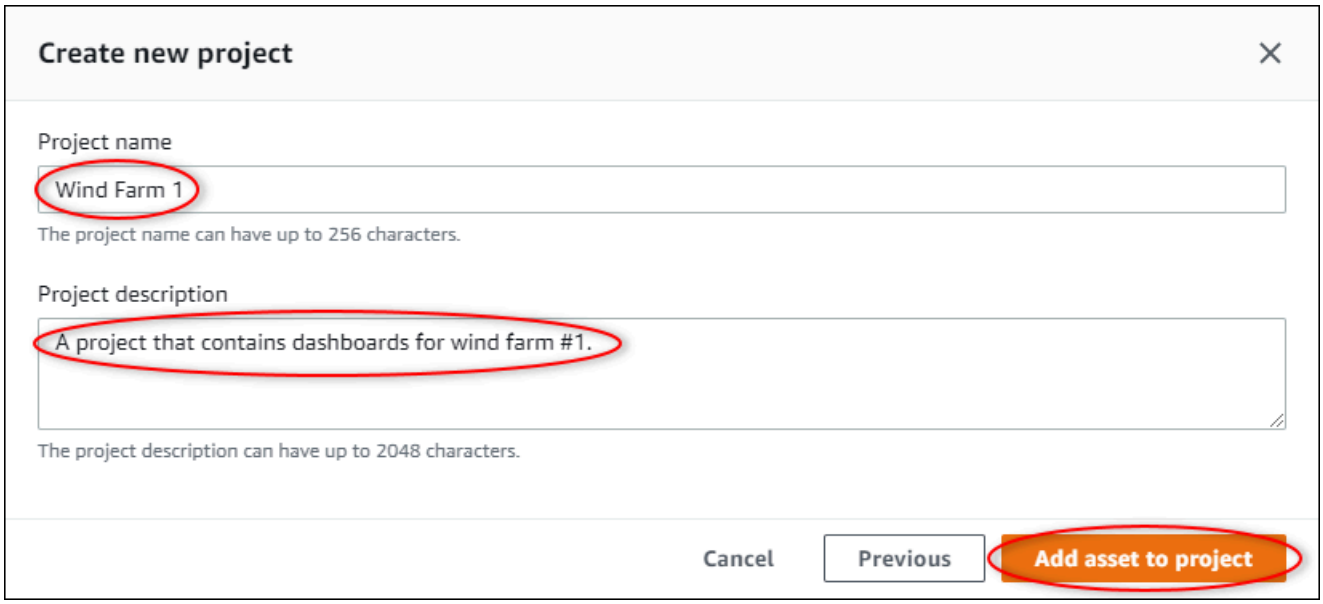
3. Choisissez Ajouter un actif au projet en haut à gauche. Les projets contiennent des tableaux de bord que les utilisateurs de votre portail peuvent consulter pour explorer vos données. Chaque projet a accès à un sous-ensemble de vos actifs dans AWS IoT SiteWise. Lorsque vous ajoutez un actif à un projet, tous les utilisateurs ayant accès à ce projet peuvent également accéder aux données de cet actif et de ses enfants.



4. Dans la boîte de dialogue Ajouter un actif au projet, choisissez Créer un nouveau projet, puis cliquez sur Suivant.



5. Dans la boîte de dialogue Créer un nouveau projet, entrez le nom et la description du projet pour votre projet, puis choisissez Ajouter un actif au projet.



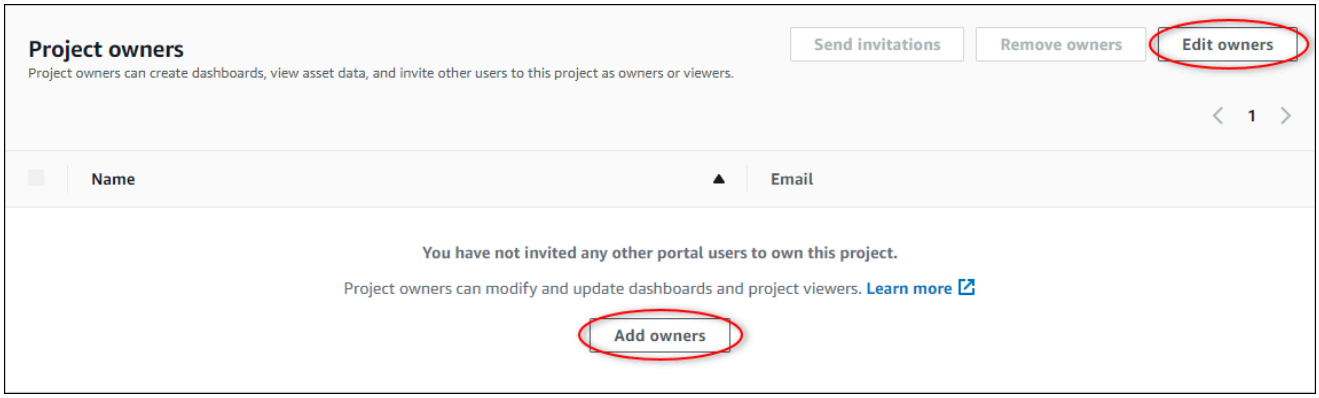
La page de votre nouveau projet s'ouvre.

6. Sur la page du projet, vous pouvez ajouter des utilisateurs du portail en tant que propriétaires ou spectateurs de ce projet.

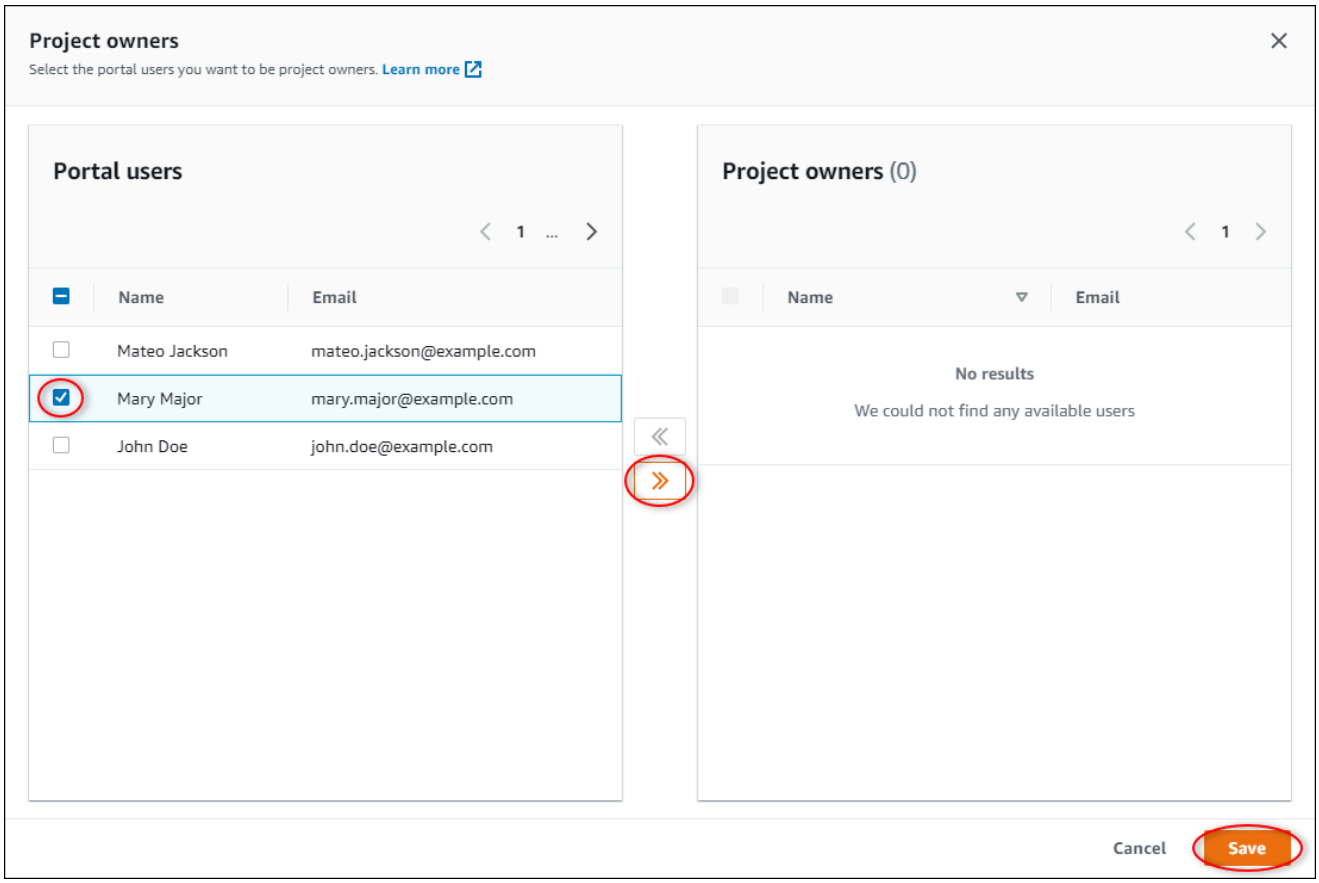
> **Note**
>
> Si vous n'êtes pas connecté à votre compte de AWS Organizations gestion, il se peut que vous n'ayez pas d'utilisateurs du portail à affecter à ce projet. Vous pouvez donc ignorer cette étape.

Sur cette page, effectuez les opérations suivantes :

a. Sous Propriétaires du projet, choisissez Ajouter des propriétaires ou Modifier des utilisateurs.



b. Choisissez l'utilisateur à ajouter en tant que propriétaire de projet (par exemple,Mary Major), puis choisissez l'icône >> .



c. Choisissez Enregistrer.

Votre utilisateur IAM Identity Center Mary Majorpeut se connecter à ce portail pour modifier les tableaux de bord de ce projet et partager ce projet avec d'autres utilisateurs de ce portail.

d. Sous Visionneuses de projet, choisissez Ajouter des visionneuses ou Modifier des utilisateurs.

e. Choisissez l'utilisateur à ajouter en tant que visionneur de projet (par exemple, Mateo Jackson), puis cliquez sur l'icône **>>**.

f. Choisissez Enregistrer.

L'utilisateur de votre IAM Identity Center Mateo Jacksonpeut se connecter à ce portail pour consulter, mais pas pour modifier, les tableaux de bord du projet de parc éolien.

Étape 4 : Création d'un tableau de bord pour visualiser les données du parc éolien

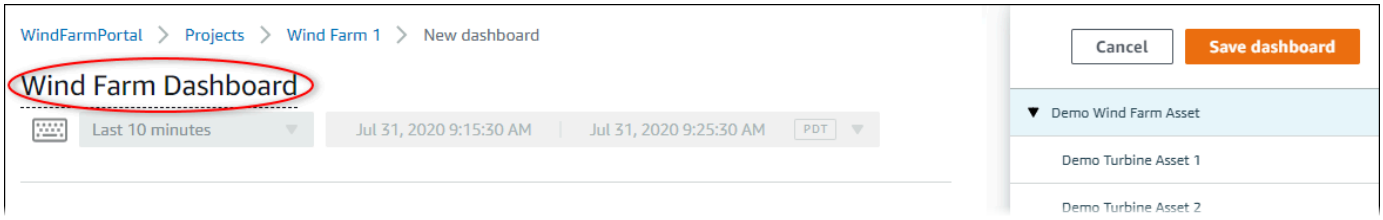
Dans cette procédure, vous créez des tableaux de bord pour visualiser les données du parc éolien de la démonstration. Les tableaux de bord contiennent les visualisations personnalisables des données de ressources de votre projet. Chaque visualisation peut avoir un type différent, tel qu'un graphique linéaire, un graphique à barres ou un affichage d'indicateurs de performance clés (KPI). Vous pouvez choisir le type de visualisation qui convient le mieux à vos données. Les propriétaires de projets peuvent modifier les tableaux de bord, tandis que les personnes qui consultent les projets ne peuvent consulter les tableaux de bord que pour obtenir des informations.

Pour créer un tableau de bord avec des visualisations

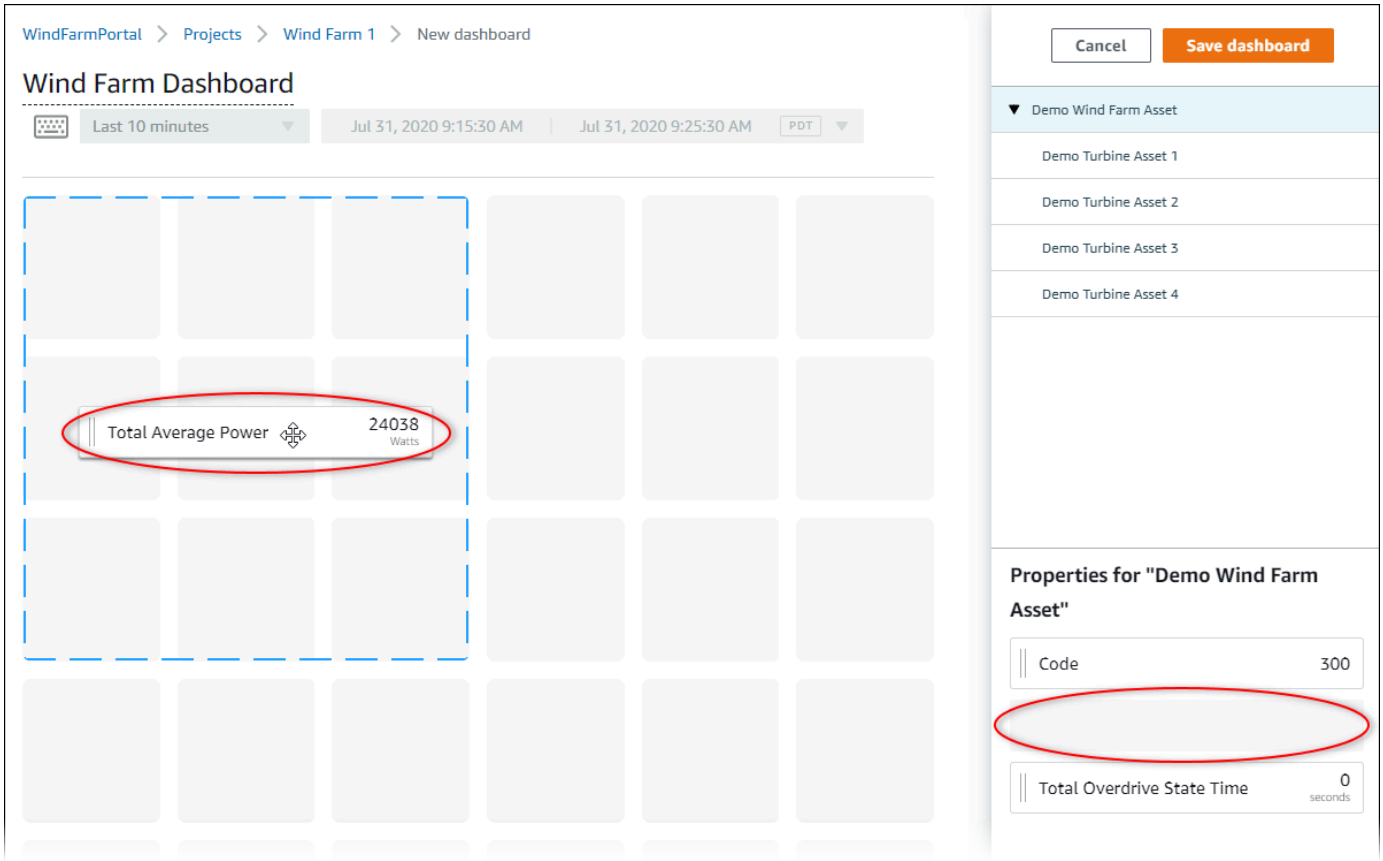
1. Sur la page de votre nouveau projet, choisissez Créer un tableau de bord pour créer un tableau de bord et ouvrir sa page de modification.

   Dans la page de modification d'un tableau de bord, vous pouvez faire glisser les propriétés des ressources de la hiérarchie des ressources vers le tableau de bord pour créer des visualisations. Vous pouvez ensuite modifier le titre, les titres de légende, le type, la taille et l'emplacement de chaque visualisation dans le tableau de bord.

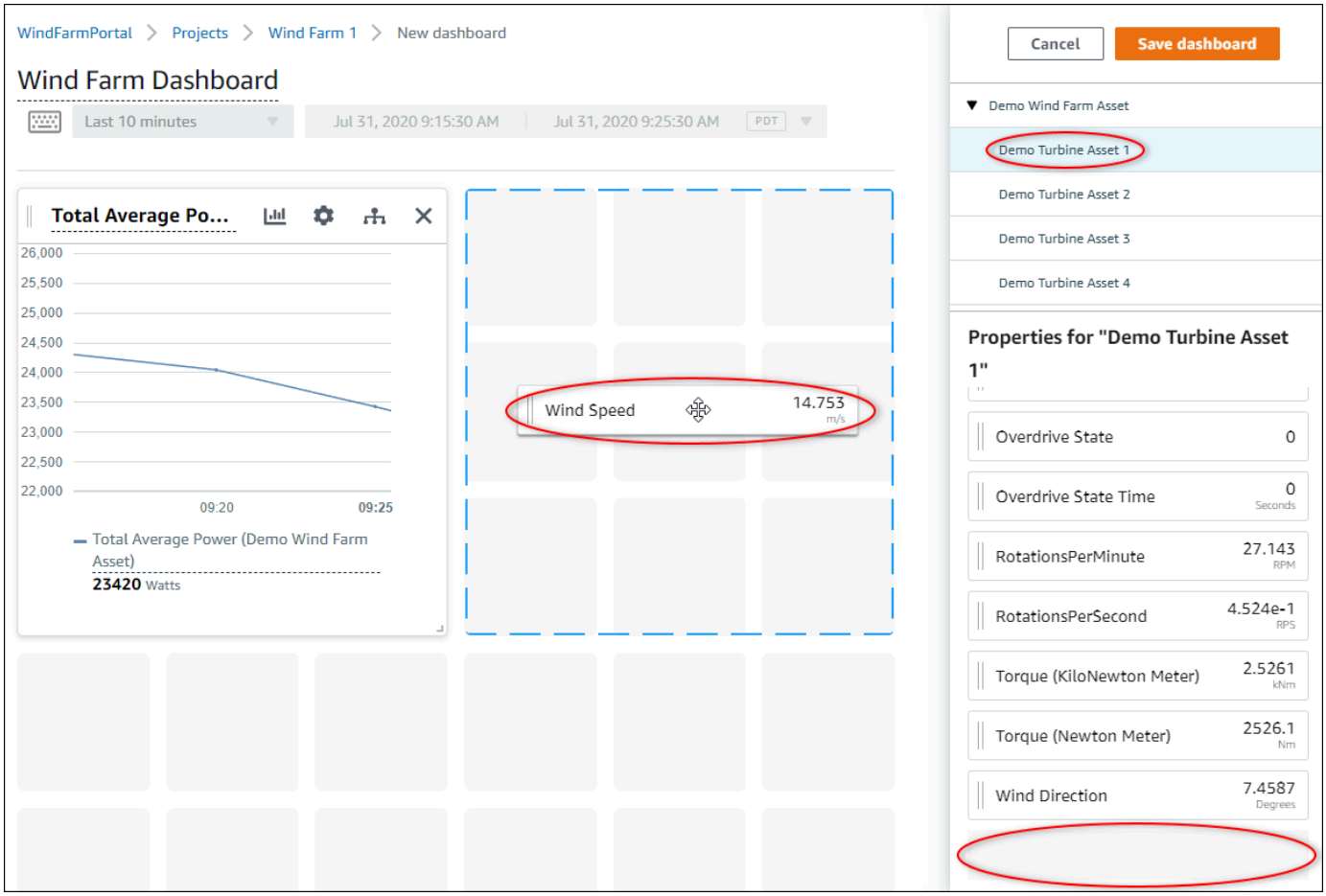
2. Donnez un nom à votre tableau de bord.



3. Faites glisser Total Average Power depuis la Demo Wind Farm Asset vers le tableau de bord pour créer une visualisation.

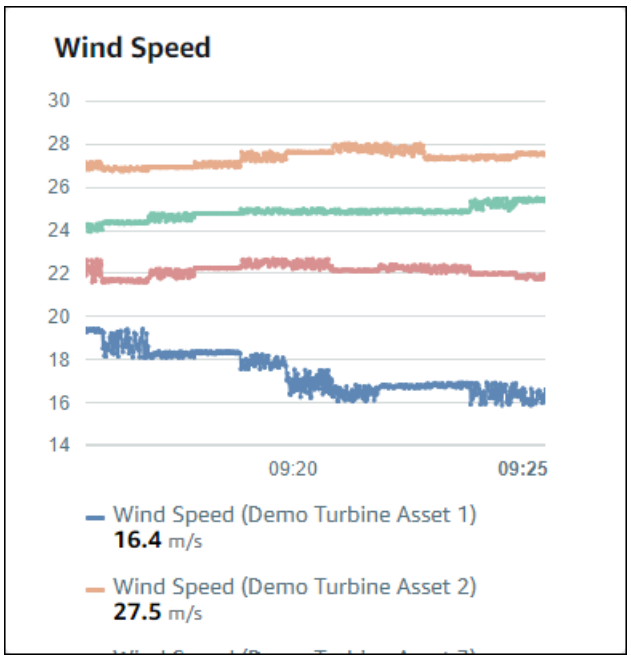


4. Choisissez Demo Turbine Asset 1d'afficher les propriétés de cet actif, puis faites glisser le pointeur Wind Speedvers le tableau de bord pour créer une visualisation de la vitesse du vent.

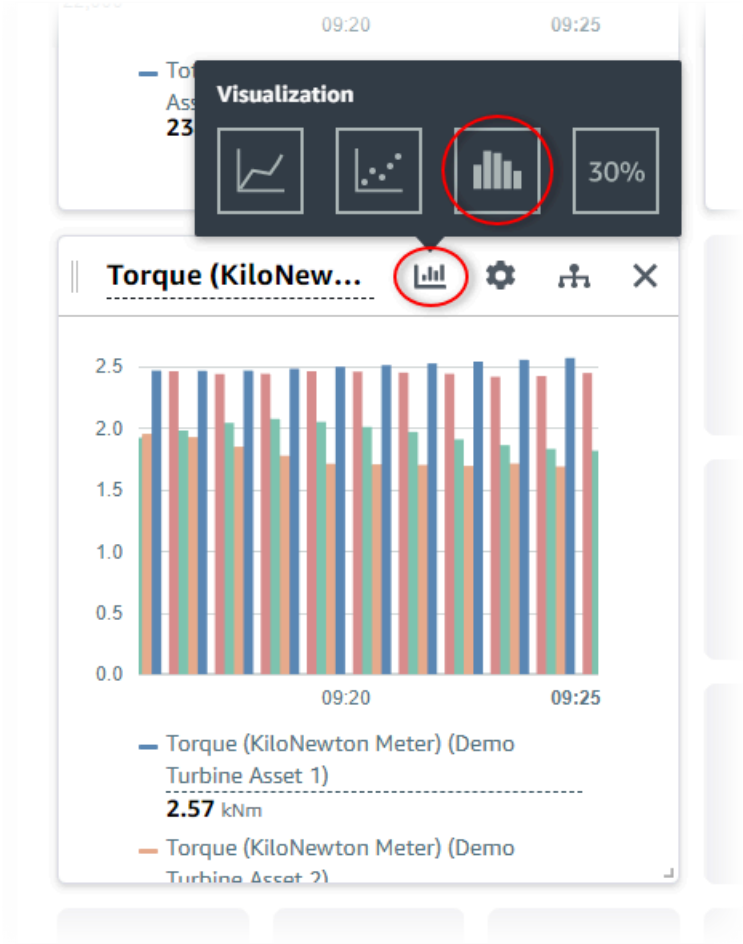


5. Ajoutez Wind Speed à la nouvelle visualisation de la vitesse du vent pour chaque Demo Turbine Asset 2, 3, et 4 (dans cet ordre).

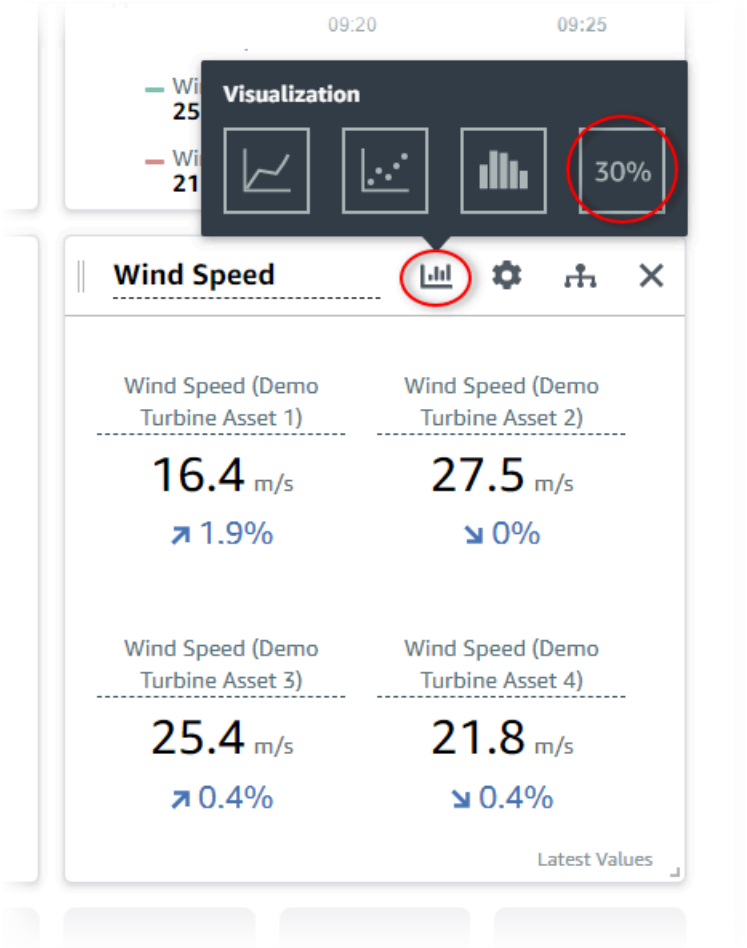
   Votre visualisation Wind Speed doit ressembler à la capture d'écran suivante.



6. Répétez les étapes 4 et 5 pour les Torque (KiloNewton Meter)propriétés des éoliennes afin de créer une visualisation du couple des éoliennes.
7. Choisissez l'icône de type de visualisation pour la visualisation Torque (KiloNewton Meter), puis choisissez l'icône du graphique à barres.

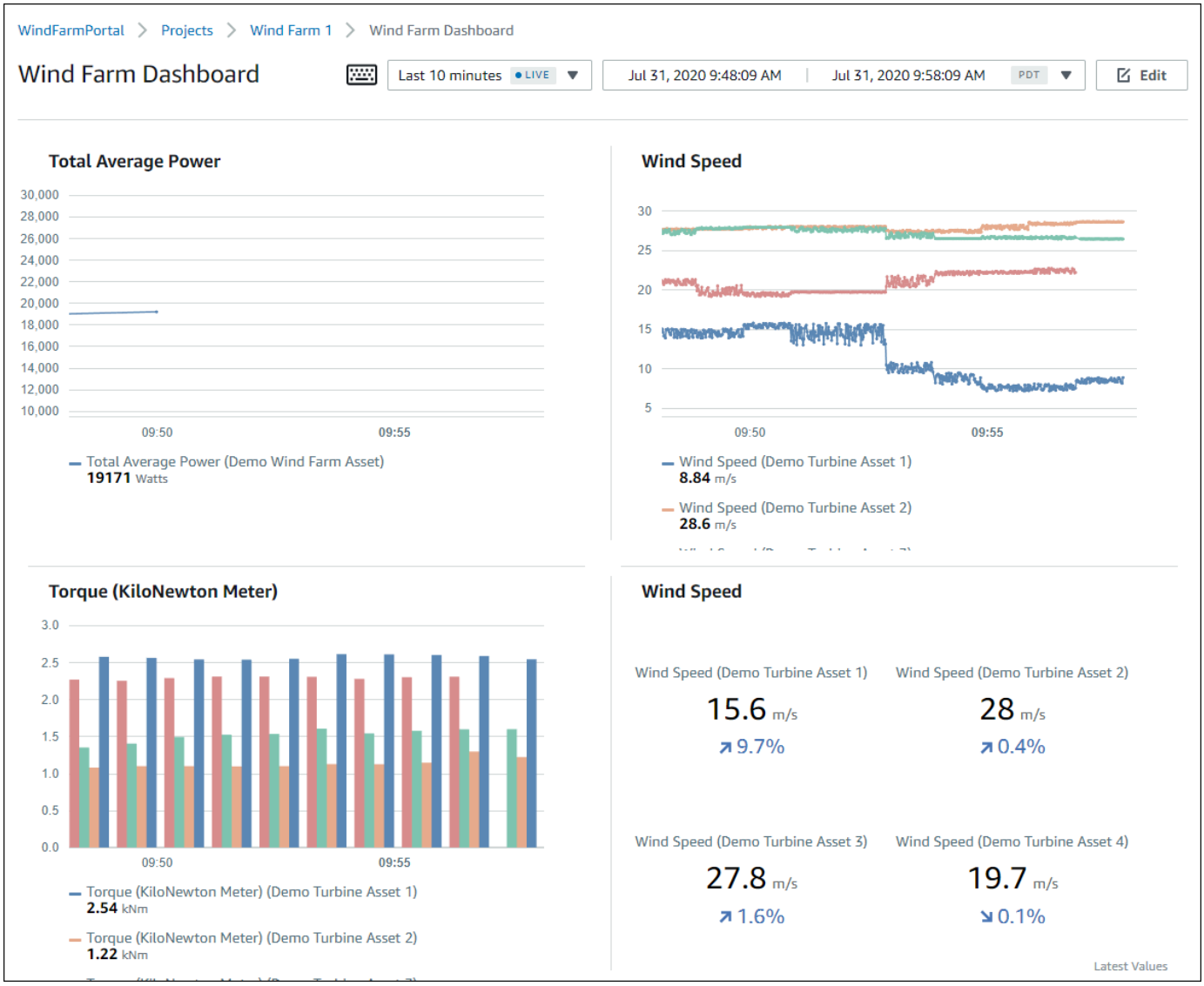


8. Répétez les étapes 4 et 5 pour les Wind Directionpropriétés des éoliennes afin de créer une visualisation de la direction du vent.
9. Choisissez l'icône du type de visualisation pour la visualisation Wind Direction, puis choisissez l'icône de graphique KPI (30%).



10. (Facultatif) Apportez d'autres modifications au titre de la visualisation, aux titres de légende, au type, à la taille et à l'emplacement, si nécessaire.
11. Choisissez Enregistrer le tableau de bord en haut à droite pour enregistrer votre tableau de bord.

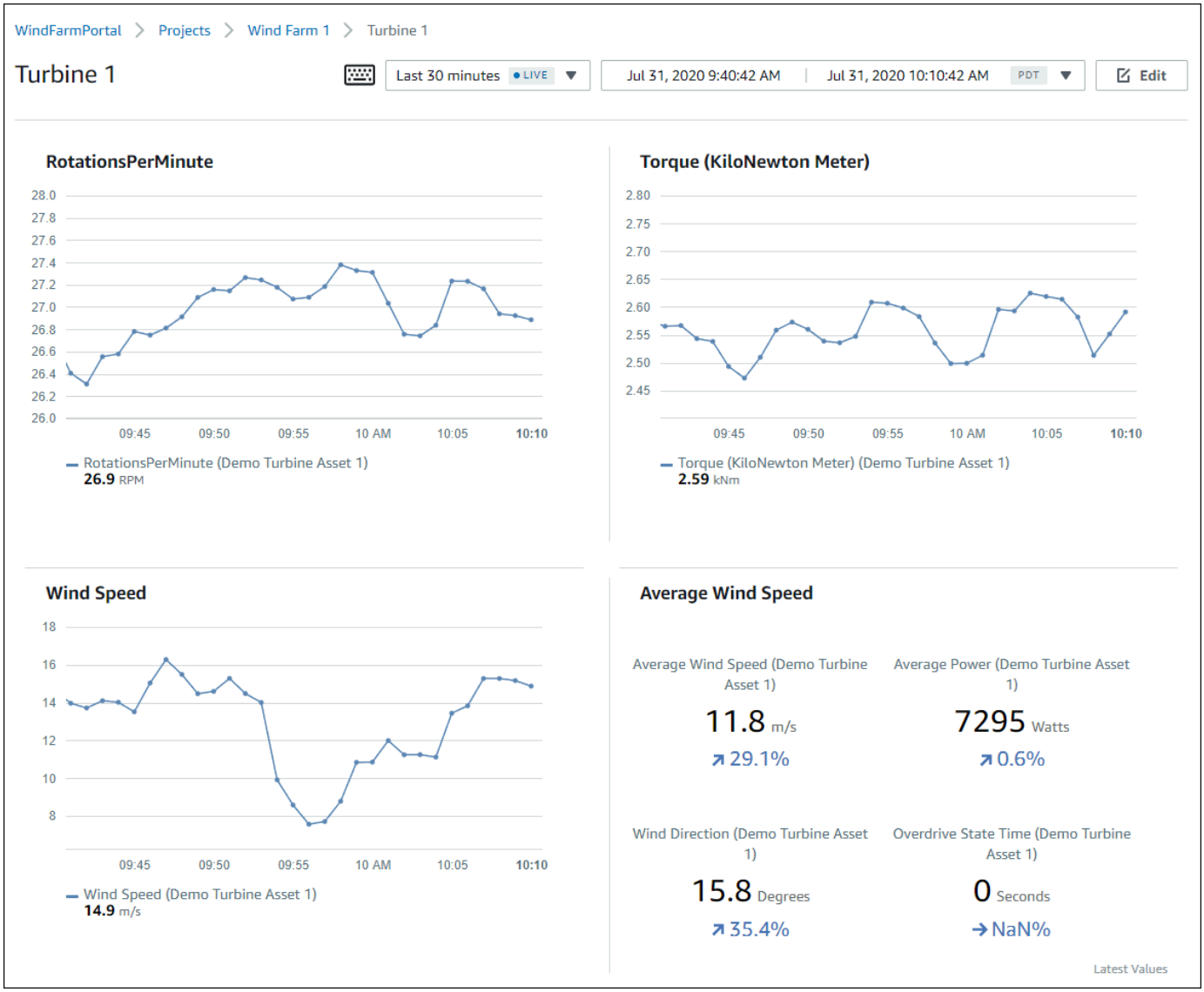
    Votre tableau de bord devrait ressembler à la capture d'écran suivante.



12. (Facultatif) Créez un tableau de bord supplémentaire pour chaque ressource éolienne.

    À titre de bonne pratique, nous vous recommandons de créer un tableau de bord pour chaque ressource afin que les utilisateurs de votre projet puissent examiner tous les problèmes liés à chaque ressource. Vous ne pouvez ajouter que 5 ressources à chaque visualisation. Vous devez donc créer plusieurs tableaux de bord pour vos ressources hiérarchiques dans de nombreux scénarios.

    Un tableau de bord pour une éolienne de démonstration pourrait ressembler à la capture d'écran suivante.



13. (Facultatif) Modifiez la chronologie ou sélectionnez des points de données sur une visualisation pour explorer les données de votre tableau de bord. Pour plus d'informations, consultez la section Affichage des tableaux de bord dans le Guide de AWS IoT SiteWise Monitor l'application.

Étape 5 : Explorez le portail

Dans cette procédure, vous pouvez explorer le portail en tant qu'utilisateur disposant de moins d'autorisations qu'en tant qu'administrateur AWS IoT SiteWise du portail.

Pour explorer le portail et terminer le didacticiel

- (Facultatif) Si vous avez ajouté d'autres utilisateurs au projet en tant que propriétaires ou spectateurs, vous pouvez vous connecter au portail en tant que ces utilisateurs. Cela vous

permet d'explorer le portail en tant qu'utilisateur disposant de moins d'autorisations qu'en tant qu'administrateur du portail.

> **Important**
>
> Vous êtes facturé pour chaque utilisateur qui se connecte à un portail. Pour plus d'informations, consultez Tarification d'AWS IoT SiteWise.

Pour explorer le portail en tant qu'autre utilisateur, procédez comme suit :

a. Choisissez Déconnexion en bas à gauche du portail pour quitter l'application Web.
b. Choisissez Se déconnecter dans le coin supérieur droit du portail de l'application IAM Identity Center pour vous déconnecter de votre utilisateur IAM Identity Center.
c. Connectez-vous au portail en tant qu'utilisateur IAM Identity Center que vous avez désigné en tant que propriétaire ou visionneur de projet. Pour plus d'informations, consultez Étape 2 : Connectez-vous à un portail.

Vous avez terminé le didacticiel. Lorsque vous aurez fini d'explorer votre parc éolien de démonstration dans SiteWise Monitor, suivez la procédure suivante pour nettoyer vos ressources.

Étape 6 : Nettoyer les ressources après le didacticiel

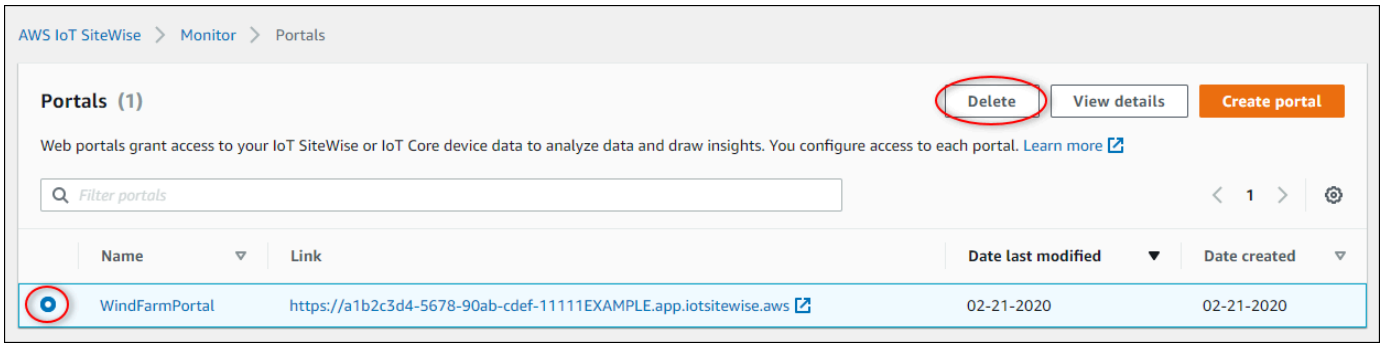
Après avoir terminé le didacticiel, vous pouvez nettoyer vos ressources. Vous n'êtes pas facturé pour AWS IoT SiteWise si les utilisateurs ne se connectent pas à votre portail, mais vous pouvez supprimer votre portail et les utilisateurs Répertoire AWS IAM Identity Center . Vos ressources de parc éolien de démonstration sont supprimées à la fin de la durée que vous avez choisie lors de la création de la démo, ou vous pouvez supprimer la démo manuellement. Pour plus d'informations, consultez Supprimer la AWS IoT SiteWise démo.

Suivez les procédures suivantes pour supprimer les utilisateurs de votre portail et de l'IAM Identity Center.

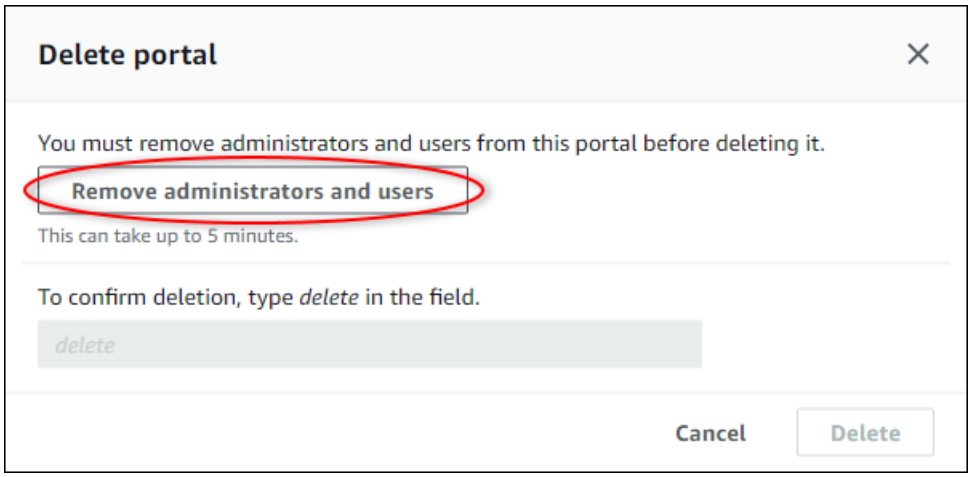
Pour supprimer un portail

1. Accédez à la console AWS IoT SiteWise.
2. Dans le volet de navigation de gauche, choisissez Portals (Portails).
3. Choisissez votre portail WindFarmPortal, puis sélectionnez Supprimer.

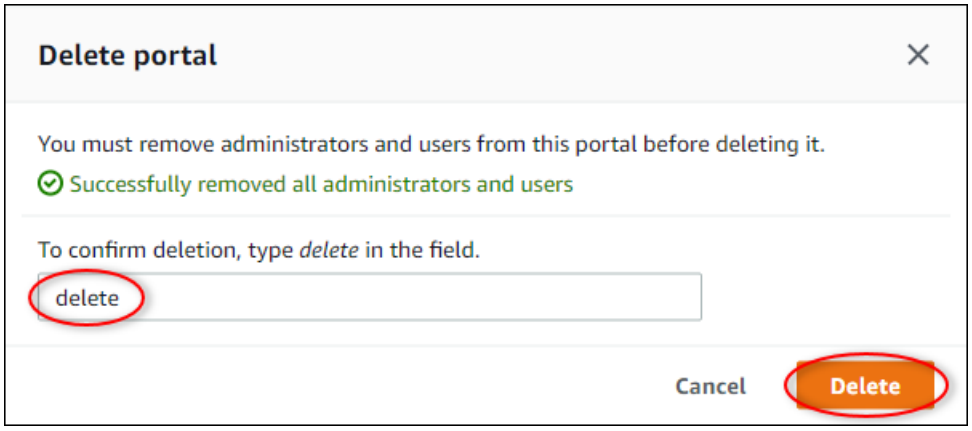
Lorsque vous supprimez un portail ou un projet, les ressources associées aux projets supprimés ne sont pas affectées.



4. Dans la boîte de dialogue Supprimer le portail, choisissez Supprimer les administrateurs et les utilisateurs.

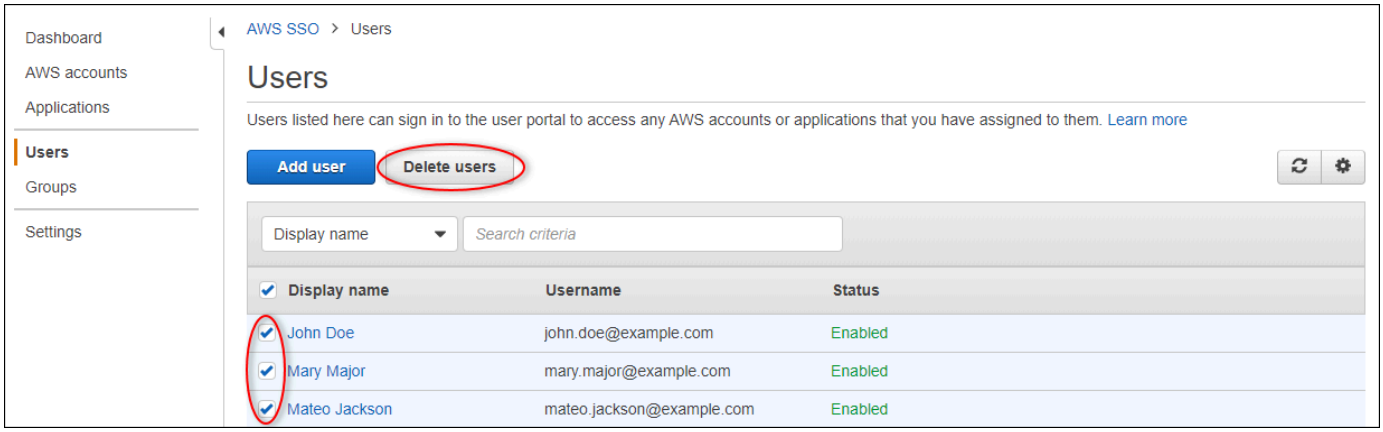


5. Entrez **`delete`** pour confirmer la suppression, puis choisissez Supprimer.

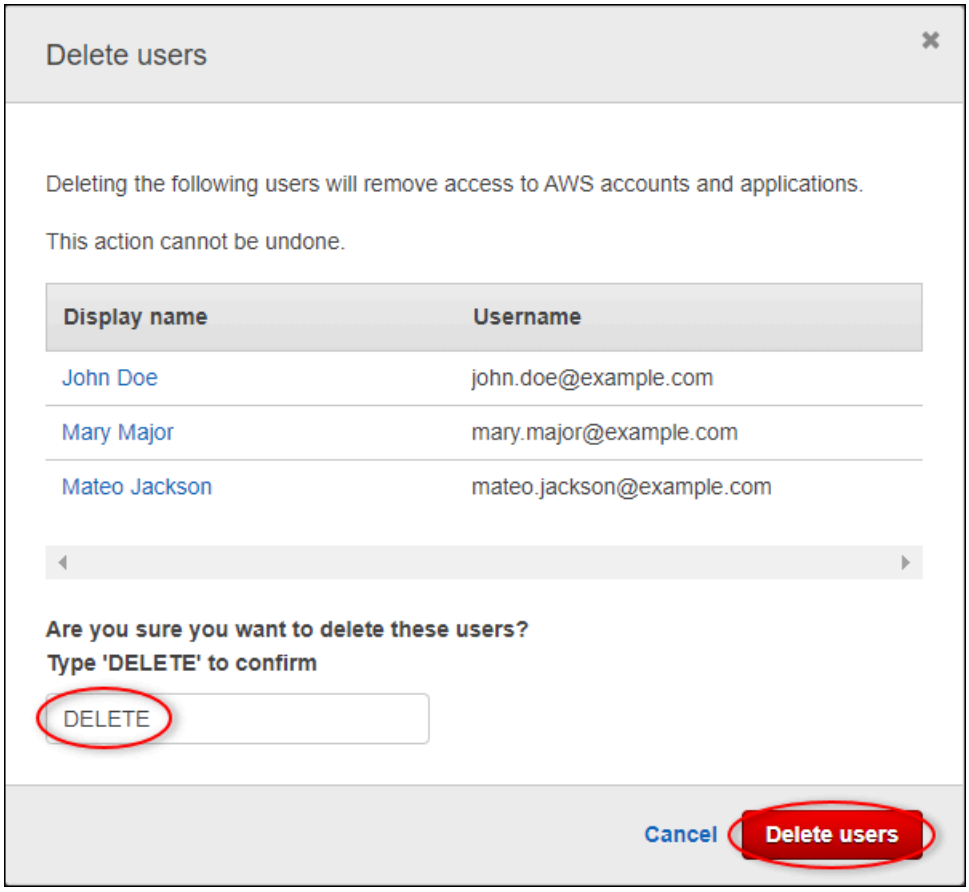


Pour supprimer des utilisateurs d'IAM Identity Center

1. Accédez à la console IAM Identity Center.
2. Dans le volet de navigation de gauche, choisissez Utilisateurs.
3. Activez la case à cocher pour chaque utilisateur à supprimer, puis choisissez Delete users (Supprimer les utilisateurs).



4. Dans la boîte de dialogue Supprimer les utilisateurs, entrez**DELETE**, puis choisissez Supprimer les utilisateurs.



Publication de mises à jour de la valeur des propriétés sur Amazon DynamoDB

Ce didacticiel présente un moyen pratique de stocker vos données à l'aide d'Amazon DynamoDB, afin de faciliter l'accès aux données historiques des actifs sans avoir à interroger l'API à plusieurs reprises. AWS IoT SiteWise Une fois ce didacticiel terminé, vous pouvez créer un logiciel personnalisé qui utilise les données de vos actifs, comme une carte en temps réel de la vitesse et de la direction du vent sur l'ensemble d'un parc éolien. Si vous souhaitez surveiller et visualiser vos données sans implémenter de solution logicielle personnalisée, consultezSurveillance des données avec AWS IoT SiteWise Monitor.

Dans ce didacticiel, vous vous appuierez sur la AWS IoT SiteWise démo qui fournit un exemple de jeu de données pour un parc éolien. Vous configurez les mises à jour de la valeur des propriétés à partir de la démonstration du parc éolien pour envoyer des données, via des règles de AWS IoT base, à une table DynamoDB que vous créez. Lorsque vous activez les mises à jour de la valeur des propriétés, AWS IoT SiteWise envoie vos données AWS IoT Core dans des messages MQTT. Définissez ensuite des règles de AWS IoT base qui exécutent des actions, telles que l'action DynamoDB, en fonction du contenu de ces messages. Pour plus d'informations, consultez Interaction avec d'autres AWS services.

Rubriques

- Prérequis
- Étape 1 : Configuration AWS IoT SiteWise pour publier les mises à jour de la valeur des propriétés
- Étape 2 : créer une règle dans AWS IoT Core
- Étape 3 : Création d'une table DynamoDB
- Étape 4 : Configuration de l'action de la règle DynamoDB
- Étape 5 : explorer les données dans DynamoDB
- Étape 6 : Nettoyer les ressources après le didacticiel

Prérequis

Pour suivre ce didacticiel, vous aurez besoin des éléments suivants :

- Un AWS compte. Si vous n'en avez pas, veuillez consulter Configuration d'un Compte AWS.

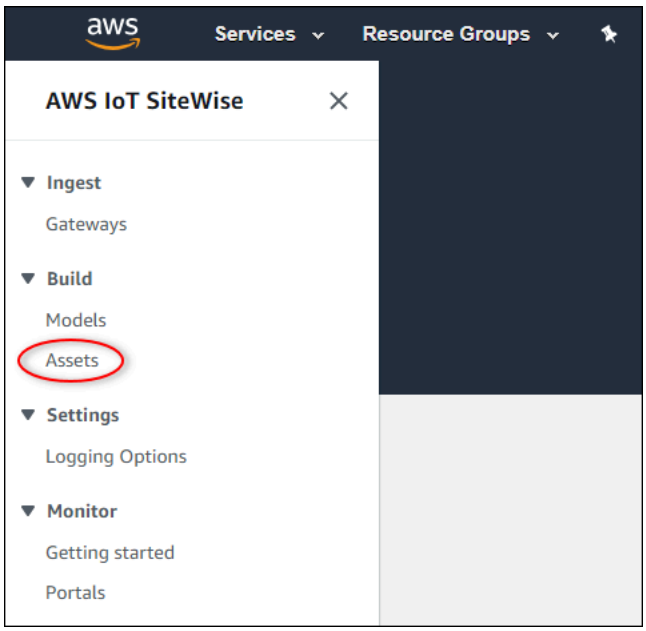
- Un ordinateur de développement exécutant Windows, macOS, Linux ou Unix pour accéder au AWS Management Console. Pour plus d'informations, consultez Démarrer avec le AWS Management Console.
- Utilisateur IAM possédant des autorisations de niveau administrateur.
- Une démonstration de AWS IoT SiteWise parc éolien en cours d'exécution. Lorsque vous configurez la démo, elle définit les modèles et les actifs AWS IoT SiteWise et leur transmet des données pour représenter un parc éolien. Pour plus d'informations, consultez Utilisation de la AWS IoT SiteWise démo.

Étape 1 : Configuration AWS IoT SiteWise pour publier les mises à jour de la valeur des propriétés

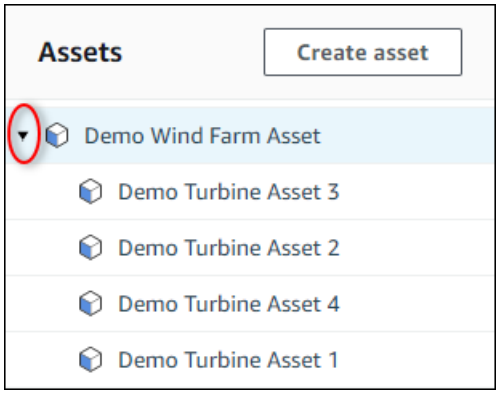
Dans cette procédure, vous activez les notifications de valeur de propriété au niveau des propriétés Wind Speed des ressources des éoliennes de la démonstration. Après avoir activé les notifications de valeur de propriété, AWS IoT SiteWise publie chaque mise à jour de valeur dans un message MQTT envoyé à AWS IoT Core.

Pour activer les notifications de mise à jour de valeur des propriétés de ressources

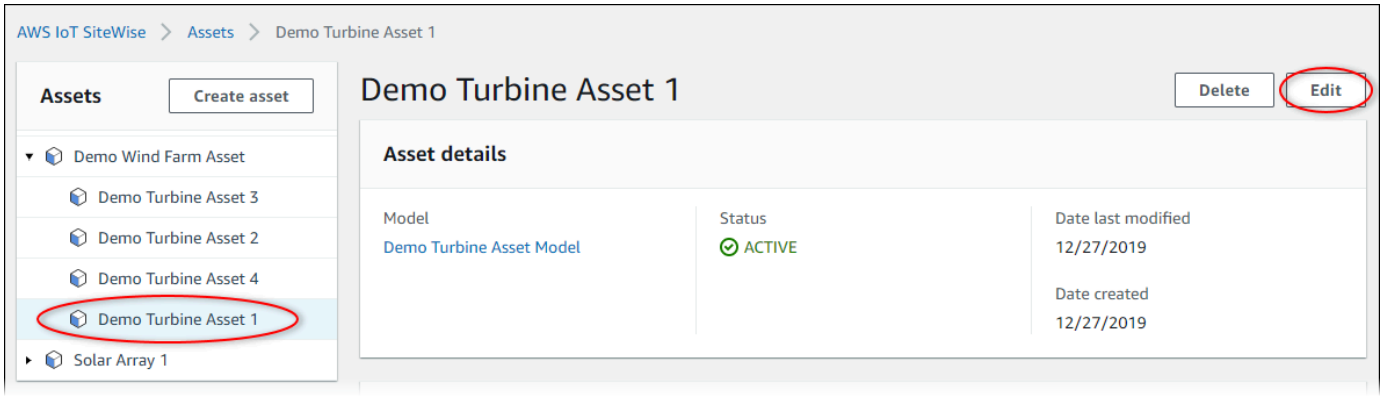
1. Connectez-vous à la console AWS IoT SiteWise.
2. Passez en revue les AWS IoT SiteWise points de terminaison et les quotas pris en charge et changez de AWS région, si nécessaire. AWS IoT SiteWise Basculez vers la région dans laquelle vous exécutez la AWS IoT SiteWise démo.
3. Dans le panneau de navigation de gauche, choisissez Assets (Ressources).



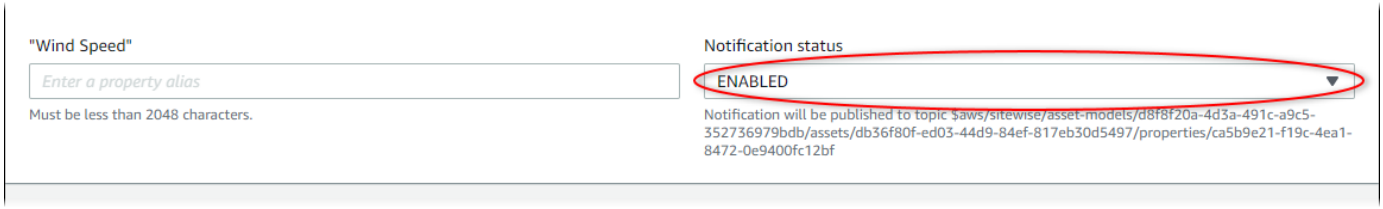
4. Sélectionnez la flèche en regard de Demo Wind Farm Asset pour développer la hiérarchie de la ressource du parc éolien.



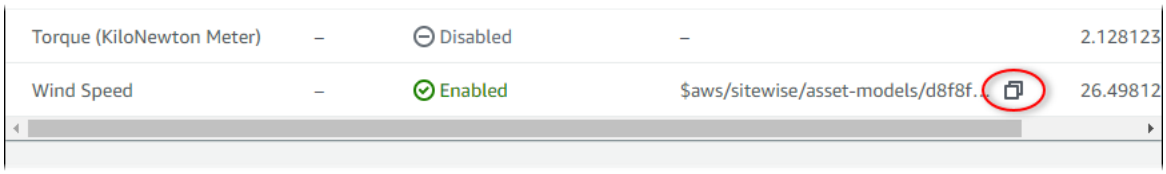
5. Choisissez une éolienne de démonstration et choisissez Edit (Modifier).



6. Mettez à jour le statut de notification de la Wind Speedpropriété sur ENABLED.



7. En bas de la page, choisissez Save asset (Enregistrer la ressource).
8. Répétez les étapes 5 à 7 pour chaque ressource d'éolienne de démonstration.
9. Choisissez une turbine de démonstration (par exemple, Demo Turbine Asset 1).
10. Choisissez Measurements (Mesures).
11. Choisissez l'icône de copie en regard de la propriété Wind Speed pour copier la rubrique de notification dans votre presse-papiers. Enregistrez la rubrique de notification qui sera utilisée ultérieurement dans ce didacticiel. Vous avez seulement besoin d'enregistrer la rubrique de notification d'une éolienne.



La rubrique de notification doit ressembler à l'exemple suivant.

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

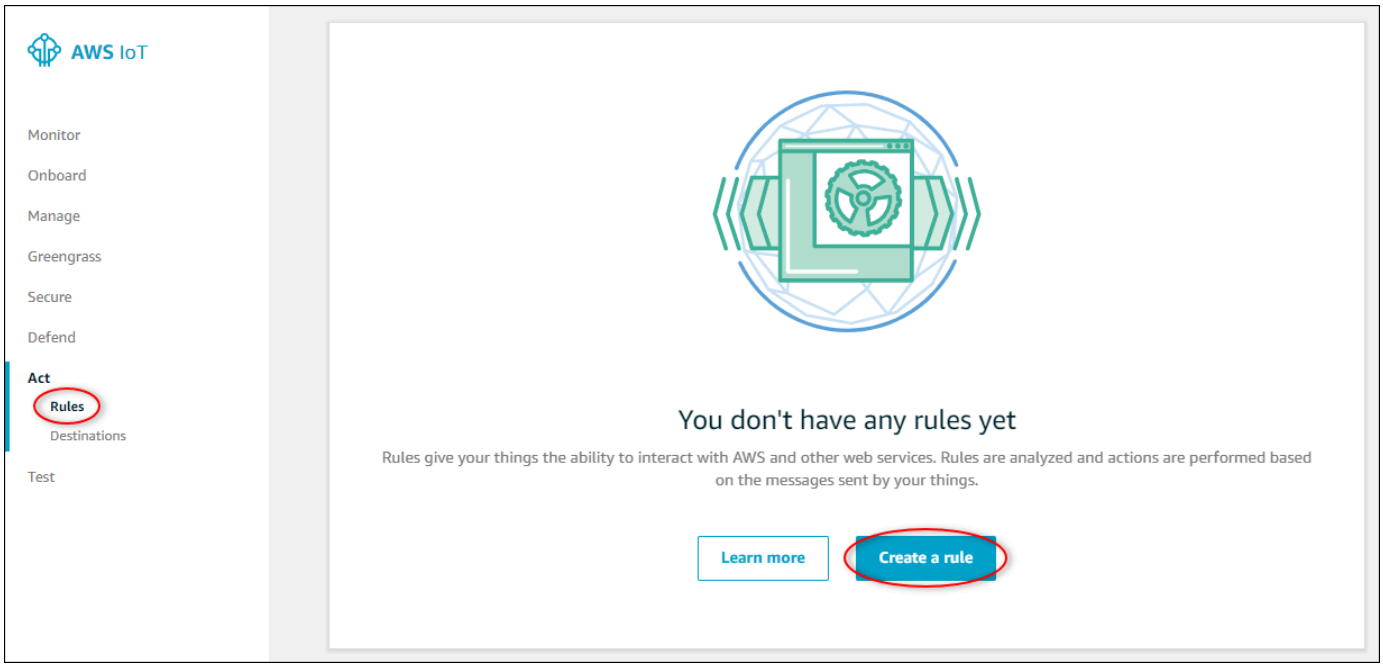
Étape 2 : créer une règle dans AWS IoT Core

Dans cette procédure, vous créez une règle dans AWS IoT Core qui analyse les messages de notification relatifs à la valeur de la propriété et insère des données dans une table Amazon DynamoDB. AWS IoT Les règles de base analysent les messages MQTT et exécutent des actions en fonction du contenu et du sujet de chaque message. Vous créez ensuite une règle avec une action DynamoDB pour insérer des données dans une table DynamoDB que vous créez dans le cadre de ce didacticiel.

Pour créer une règle avec une action DynamoDB

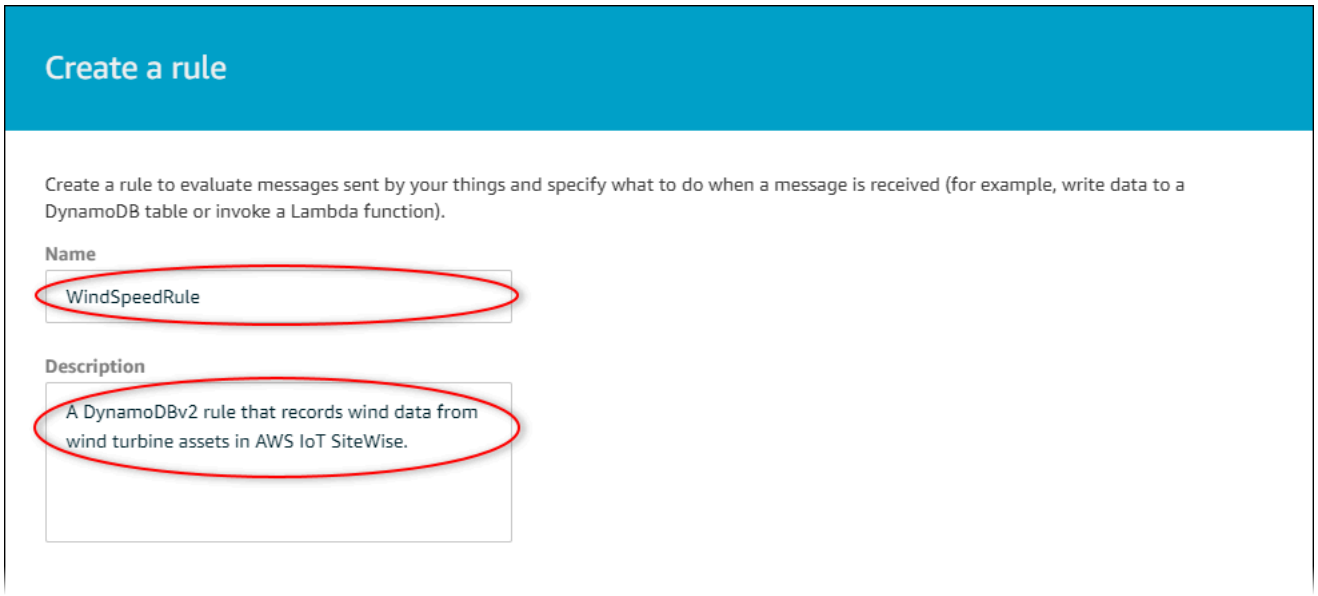
1. Accédez à la console AWS IoT. Si un bouton Get started (Démarrer) apparaît, sélectionnez-le.

2. Dans le panneau de navigation de gauche, choisissez Act (Agir) puis Rules (Règles).



3. Si une boîte de dialogue Vous ne possédez pas encore de règle s'affiche, choisissez Créer une règle. Sinon, cliquez sur Create.

4. Saisissez un nom et une description pour la règle.



5. Recherchez la rubrique de notification que vous avez enregistrée précédemment dans ce didacticiel.

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

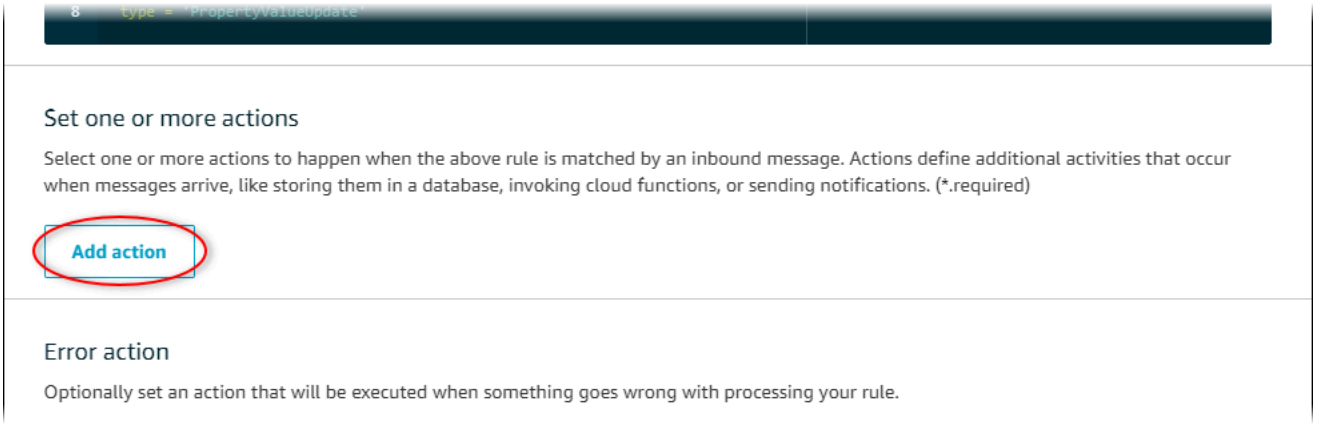
Remplacez l'ID de ressource (l'ID après`assets/`) dans la rubrique par un+. Cela permet de sélectionner la propriété de vitesse du vent pour tous les actifs d'éoliennes de démonstration. Le filtre de rubrique + accepte tous les nœuds d'un seul niveau dans une rubrique. Votre sujet doit ressembler à l'exemple suivant.

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

6. Entrez l'instruction de requête de règle suivante. Remplacez la rubrique de la section `FROM` par votre rubrique de notification.

```
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. Sous Définissez une ou plusieurs actions, choisissez Ajouter une action.



8. Sur la page Sélectionner une action, choisissez Diviser le message en plusieurs colonnes d'une table DynamoDB (DynamoDBv2).

9. En bas de la page, choisissez Configure action (Configurer l'action).
10. Sur la page Configure action, choisissez Create a new resource.

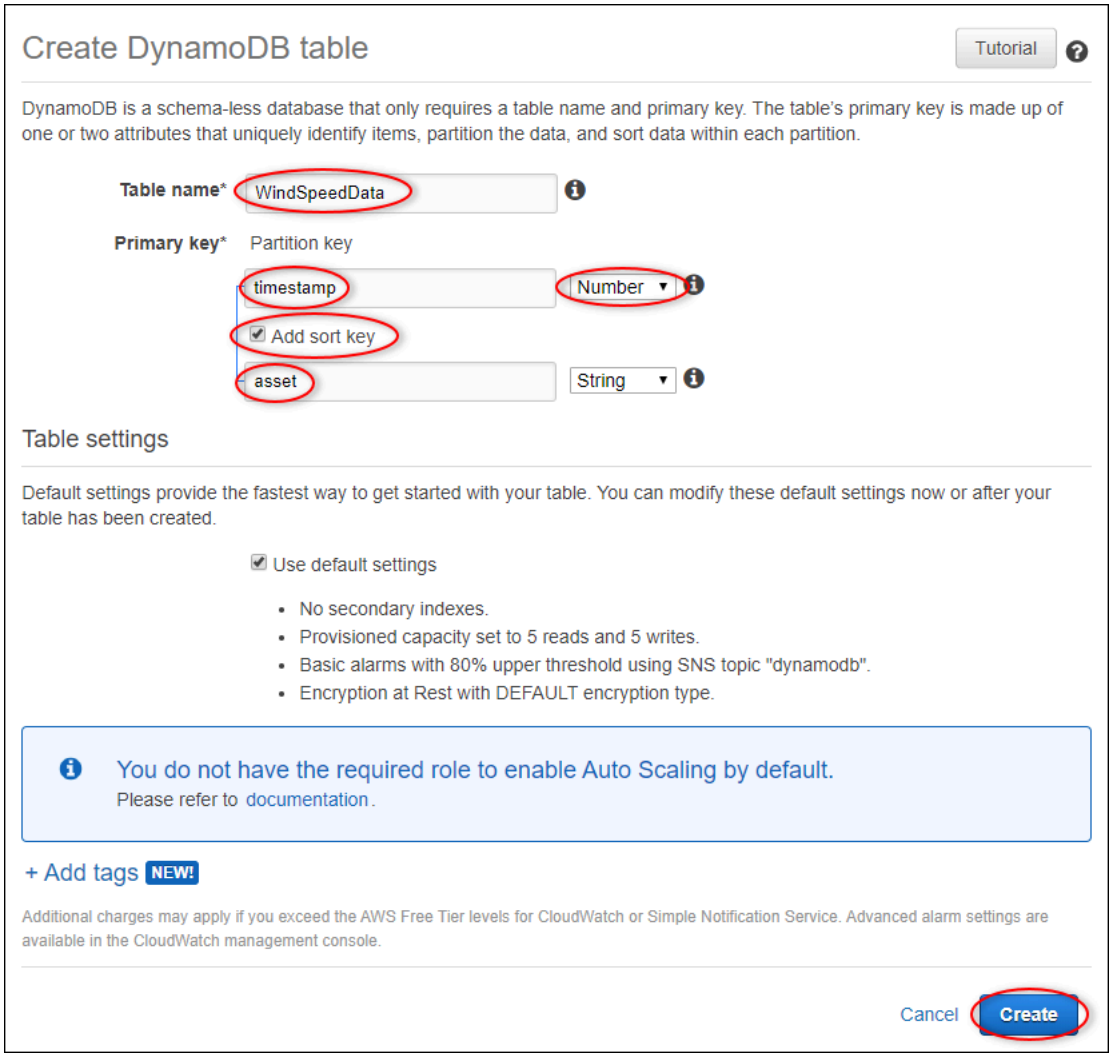
    La console DynamoDB s'ouvre dans un nouvel onglet. Laissez l'onglet de l'action de la règle ouvert pendant que vous effectuez les procédures suivantes.

Étape 3 : Création d'une table DynamoDB

Dans cette procédure, vous créez une table Amazon DynamoDB pour recevoir les données de vitesse du vent issues de l'action de la règle.

Pour créer une table DynamoDB

1. Dans le tableau de bord de la console DynamoDB, choisissez Create table.
2. Saisissez un nom pour votre table.



3. Pour Clé primaire, procédez comme suit :

   a. Pour la clé de partition, saisissez **`timestamp`**.

   b. Choisissez le type Numéro .

   c. Cochez la case Ajouter une clé de tri.

   d. Pour la clé de tri, saisissez **`asset`** et laissez le type de clé de tri par défaut Chaîne.

4. Choisissez Créer.

   Lorsque le message La table est en cours de création. disparaît, votre table est prête.

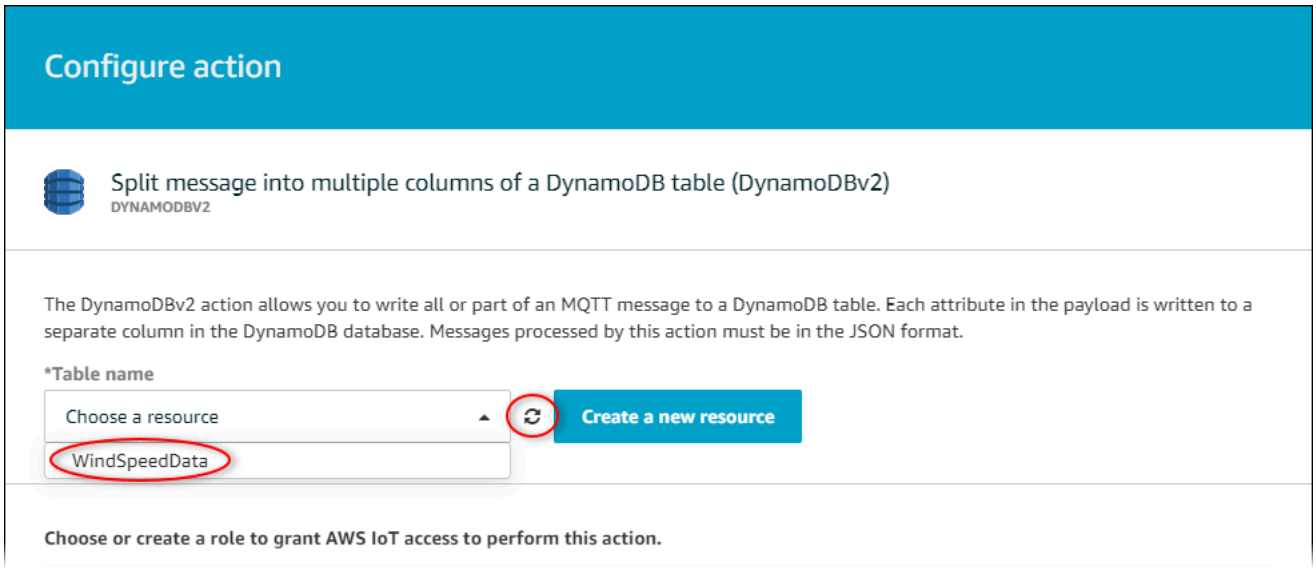
5. Retournez à l'onglet avec la page Configure action (Configurer l'action). Gardez l'onglet DynamoDB ouvert pendant que vous effectuez les procédures suivantes.

Étape 4 : Configuration de l'action de la règle DynamoDB

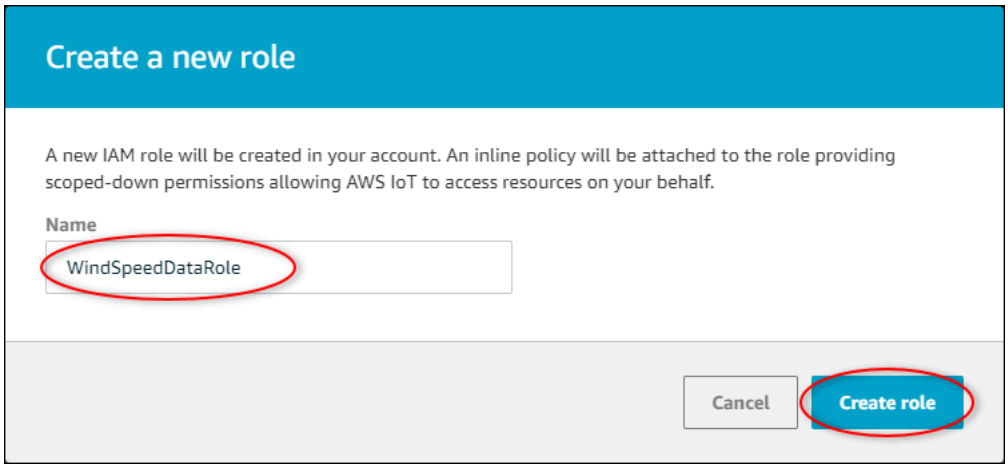
Dans cette procédure, vous configurez l'action de règle Amazon DynamoDB pour insérer les données issues des mises à jour des valeurs de propriété dans votre nouvelle table DynamoDB.

Pour configurer l'action de règle DynamoDB

1. Sur la page Configurer l'action, actualisez la liste des noms de table et choisissez votre nouvelle table DynamoDB.



2. Choisissez Create role pour créer un rôle IAM qui accorde un accès AWS IoT Core pour exécuter l'action de règle.
3. Saisissez un nom de rôle, puis choisissez Create role (Créer un rôle).



4. Choisissez Add action.
5. Choisissez Create rule (Créer une règle) au bas de la page pour terminer la création de la règle.

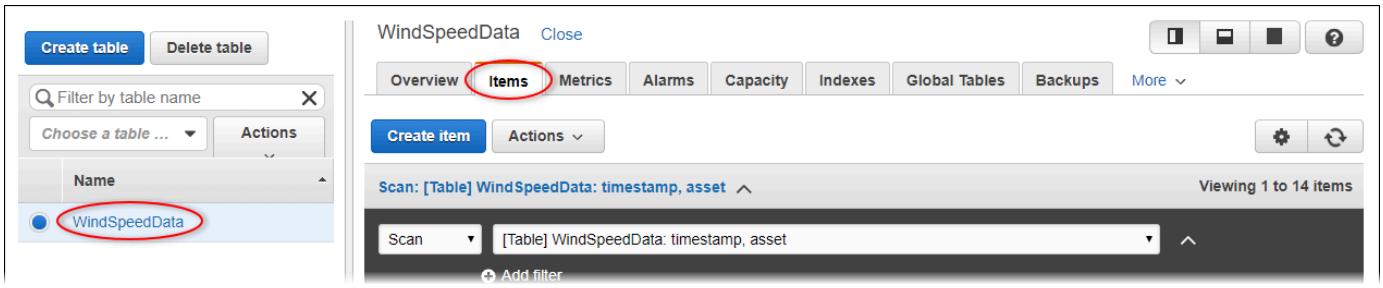
Les données de vos actifs de démonstration devraient commencer à apparaître dans votre table DynamoDB.

Étape 5 : explorer les données dans DynamoDB

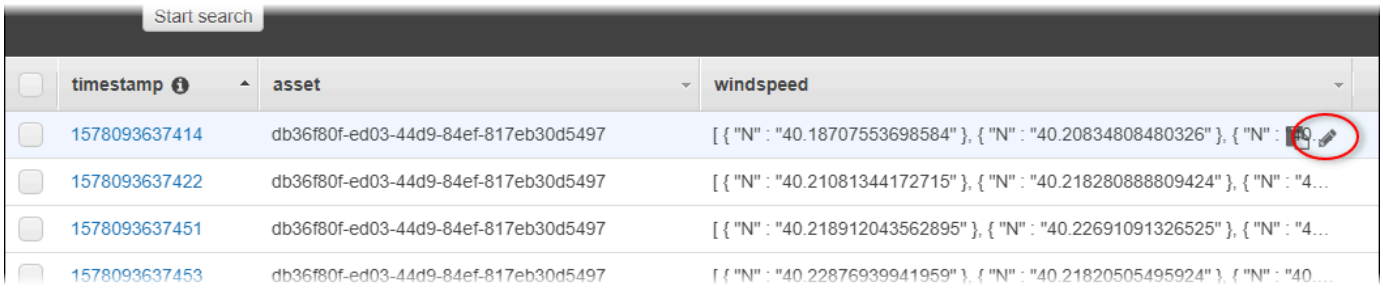
Dans cette procédure, vous allez explorer les données de vitesse du vent des actifs de démonstration dans votre nouvelle table Amazon DynamoDB.

Pour explorer les données relatives aux actifs dans DynamoDB

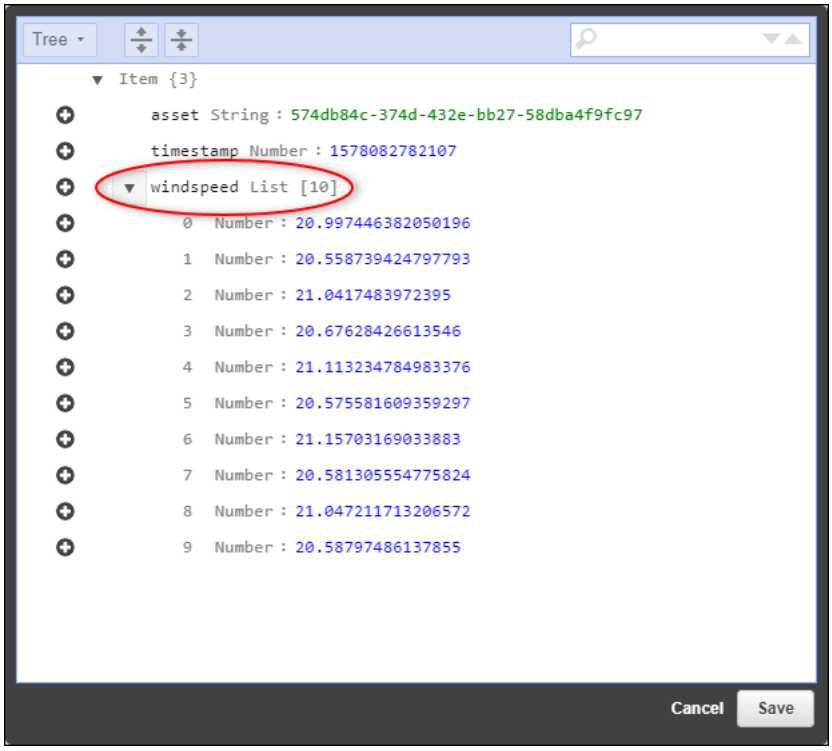
1. Retournez à l'onglet avec la table DynamoDB ouverte.
2. Dans la table que vous avez créée précédemment, choisissez l'onglet Éléments pour afficher les données de la table. Actualisez la page si la table ne comporte aucune ligne. Si aucune ligne n'apparaît après quelques minutes, consultez Résolution des problèmes d'une règle.



3. Dans une ligne du tableau, choisissez l'icône de modification pour développer les données.



4. Choisissez la flèche en regard de la structure windspeed pour développer la liste des points de données de vitesse du vent. Chaque liste reflète un lot de points de données sur la vitesse du vent envoyés AWS IoT SiteWise par la démo du parc éolien. Vous pouvez avoir besoin d'un format de données différent si vous configurez une action de règle adaptée à votre utilisation. Pour plus d'informations, consultez Interrogation des messages de notification de propriété de ressource.



Maintenant que vous avez terminé le didacticiel, désactivez ou supprimez la règle et supprimez votre table DynamoDB pour éviter des frais supplémentaires. Pour nettoyer vos ressources, voirÉtape 6 : Nettoyer les ressources après le didacticiel.

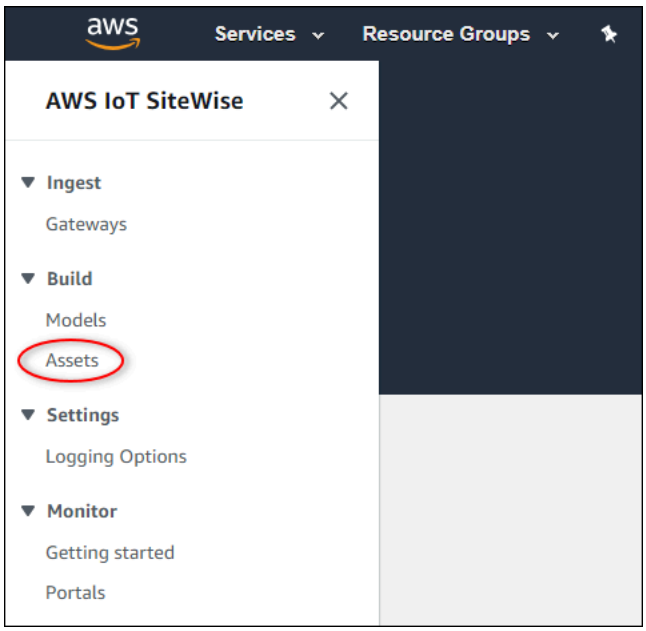
Étape 6 : Nettoyer les ressources après le didacticiel

Une fois que vous avez terminé le didacticiel, nettoyez les ressources pour éviter d'encourir des frais supplémentaires. Les actifs de votre parc éolien de démonstration sont supprimés à la fin de la durée que vous avez choisie lors de la création de la démo. Vous pouvez également supprimer la démo manuellement. Pour plus d'informations, consultez Supprimer la AWS IoT SiteWise démo.

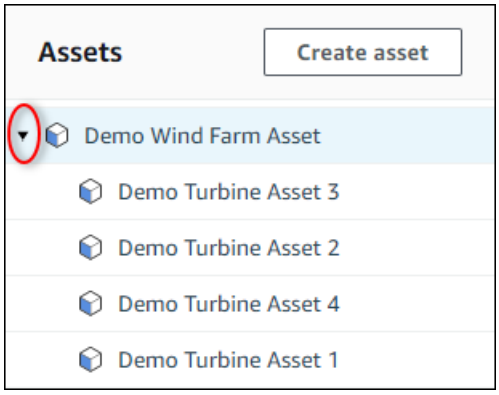
Utilisez les procédures suivantes pour désactiver les notifications de mise à jour de la valeur des propriétés (si vous n'avez pas supprimé la démo), désactiver ou supprimer votre AWS IoT règle et supprimer votre table DynamoDB.

Pour désactiver les notifications de mise à jour de valeur des propriétés de ressources

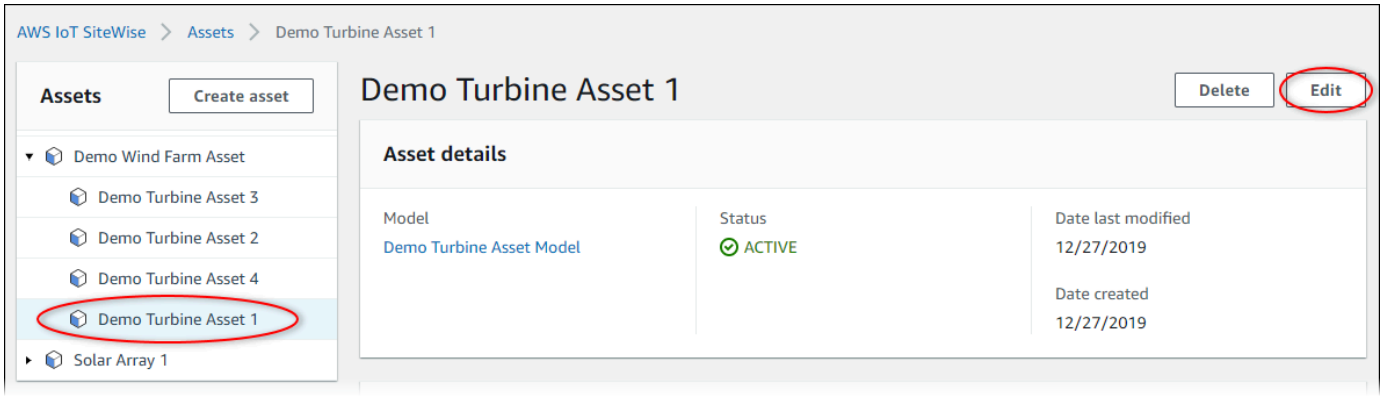
1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation de gauche, choisissez Assets (Ressources).



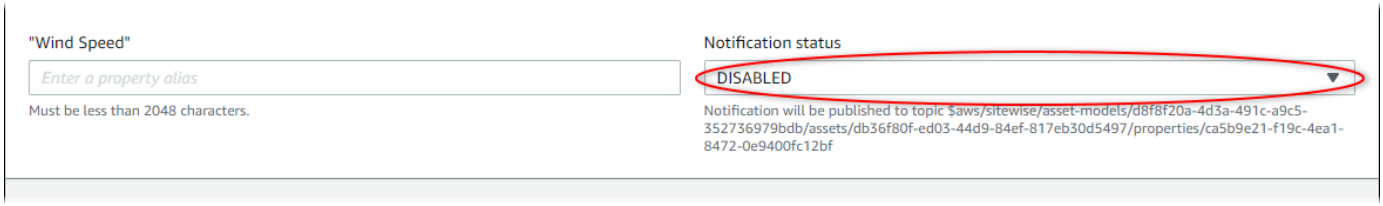
3. Sélectionnez la flèche en regard de Demo Wind Farm Asset pour développer la hiérarchie de la ressource du parc éolien.



4. Choisissez une éolienne de démonstration et choisissez Edit (Modifier).



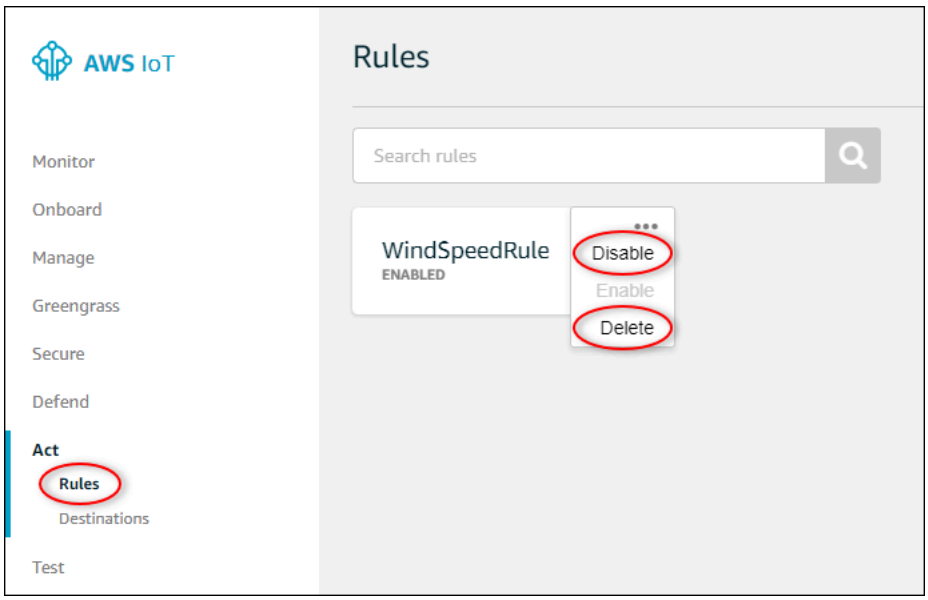
5. Mettez à jour le statut de notification de la Wind Speedpropriété sur DÉSACTIVÉ.



6. En bas de la page, choisissez Save asset (Enregistrer la ressource).
7. Répétez les étapes 4 à 6 pour chaque ressource d'éolienne de démonstration.

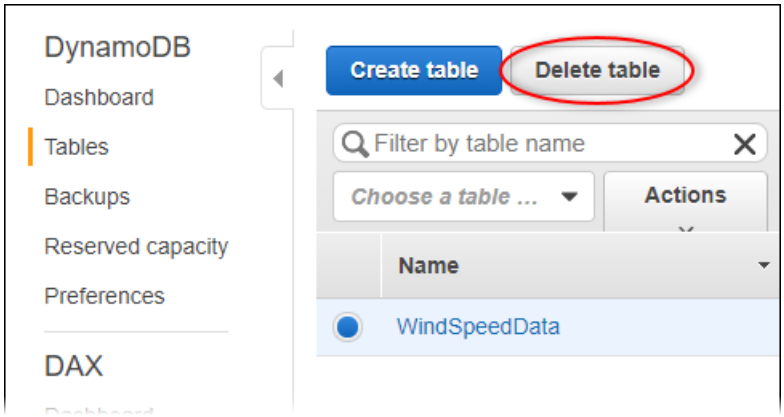
Pour désactiver ou supprimer une règle dans AWS IoT Core

1. Accédez à la console AWS IoT.
2. Dans le panneau de navigation de gauche, choisissez Act (Agir) puis Rules (Règles).
3. Choisissez le menu de votre règle et choisissez Désactiver ou Supprimer.

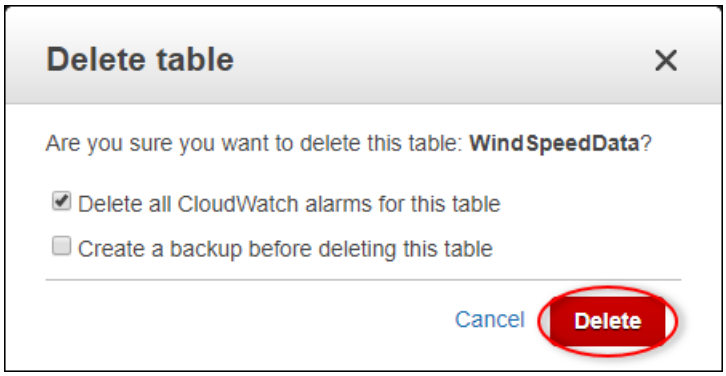


Pour supprimer une table DynamoDB

1. Accédez à la console DynamoDB.
2. Dans le volet de navigation de gauche, choisissez Tables.
3. Choisissez la table que vous avez créée précédemment WindSpeedData.
4. Choisissez Supprimer la table.



5. Dans la boîte de dialogue Delete table (Supprimer la table), choisissez Delete (Supprimer).



Ingestion de données pour AWS IoT SiteWise

AWS IoT SiteWise est conçu pour collecter et corréler efficacement les données industrielles avec les actifs correspondants, représentant divers aspects des opérations industrielles. Cette documentation se concentre sur les aspects pratiques de l'ingestion de données AWS IoT SiteWise, en proposant de multiples méthodes adaptées à divers cas d'utilisation industrielle. Pour obtenir des instructions sur la création de votre opération industrielle virtuelle, veuillez consulter Modélisation des ressources industrielles.

Vous pouvez envoyer des données industrielles à AWS IoT SiteWise l'aide de l'une des options suivantes :

- AWS IoT SiteWise Edge —Utilisez la passerelle SiteWise Edge comme intermédiaire entre AWS IoT SiteWise et vos serveurs de données. AWS IoT SiteWise fournit des AWS IoT Greengrass composants que vous pouvez déployer sur n'importe quelle plate-forme pouvant être exécutée AWS IoT Greengrass pour configurer une passerelle SiteWise Edge. Cette option prend en charge la liaison avec le protocole de serveur OPC-UA.
- AWS IoT SiteWise API —Utilisez l'AWS IoT SiteWise API pour télécharger des données depuis n'importe quelle autre source. Utilisez notre BatchPutAssetPropertyValueAPI de streaming pour une ingestion en quelques secondes, ou l'CreateBulkImportJobAPI orientée par lots pour faciliter une ingestion rentable en lots plus importants.
- AWS IoT Règles de base : utilisez les règles de AWS IoT base pour télécharger des données à partir de messages MQTT publiés par un AWS IoT objet ou un autre AWS service.
- AWS IoT Events actions —Utilisez des AWS IoT Events actions déclenchées par des événements spécifiques dans AWS IoT Events. Cette méthode convient aux scénarios dans lesquels le téléchargement de données est lié à des événements.
- AWS IoT Greengrass gestionnaire de flux : utilisez le gestionnaire de AWS IoT Greengrass flux pour télécharger des données à partir de sources de données locales à l'aide d'un périphérique périphérique. Cette option convient aux situations dans lesquelles les données proviennent de sites locaux ou périphériques.

Ces méthodes offrent une gamme de solutions pour gérer les données provenant de différentes sources. Examinez les détails de chaque option pour acquérir une compréhension complète des fonctionnalités d'ingestion de données AWS IoT SiteWise .

Gestion des flux de données

Avant de vous lancer dans la création de modèles d'actifs et d'actifs AWS IoT SiteWise, commencez par configurer vos sources de données pour envoyer des informations directement depuis votre équipement industriel vers la plateforme. AWS IoT SiteWise est conçu pour générer automatiquement des flux de données qui collectent vos données brutes. Chacun des flux de données est identifié par un alias unique, ce qui permet de suivre plus facilement l'origine de chaque donnée.

Imaginons, par exemple, qu'un parc éolien utilise une passerelle AWS IoT SiteWise Edge pour envoyer des données sur la température de l'air, la vitesse de rotation de l'hélice et les séries chronologiques de puissance de sortie d'un serveur OPC-UA à destination. AWS IoT SiteWise L'alias du flux de `server1-windfarm/3/turbine/7/temperature` données identifie les valeurs de température provenant de la turbine #7 du parc éolien #3. `server1`est le nom de la source de données OPC-UA. Le `server1` préfixe est utilisé pour tous les flux de données provenant de ce serveur, ce qui permet d'organiser les données par source.

Après avoir créé les modèles d'actifs et les actifs, organisez l'afflux de données en associant chaque flux de données à des propriétés d'actifs spécifiques. Cette association AWS IoT SiteWise permet non seulement de collecter, mais également de traiter les données en fonction de la structure de vos actifs. Si nécessaire, vous pouvez également supprimer le lien entre les flux de données et les propriétés des actifs.

Actuellement, vous pouvez uniquement associer des flux de données à des mesures. Les mesures sont un type de propriété d'actif qui représente les flux de données brutes des capteurs des appareils, tels que les valeurs de température horodatées ou les valeurs de rotations par minute (RPM) horodatées.

Lorsque ces mesures définissent des métriques ou des transformations, les données entrantes déclenchent des calculs spécifiques. Il est important de noter qu'une propriété d'actif ne peut être liée qu'à un seul flux de données à la fois.

> **Note**
>
> Une propriété d'actif ne peut pas être associée à plusieurs flux de données en même temps.

AWS IoT SiteWise utilise `TimeSeries` la ressource Amazon Resource Name (ARN) pour déterminer vos frais de stockage. Pour plus d'informations, consultez Tarification d'AWS IoT SiteWise.

Les sections suivantes expliquent comment utiliser la AWS IoT SiteWise console ou l'API pour gérer les flux de données.

Rubriques

- Gestion des flux de données

Gestion des flux de données

Pour commencer à gérer les flux de données, procédez comme suit.

> **Note**
>
> Si vous êtes nouveau AWS IoT SiteWise après le 24 novembre 2021, vous pouvez ignorer cette section. Les clients qui ont commencé à l'utiliser AWS IoT SiteWise avant cette date doivent configurer les paramètres du service pour AWS IoT SiteWise permettre l'ingestion de données sans modèles d'actifs ni actifs.

- Assurez-vous que votre rôle IAM dispose des autorisations indiquées dans l'exemple suivant.

  Example Politique utilisateur IAM

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

> **Important**
>
> Avant d'ingérer des données dans un flux de données, procédez comme suit.
>
> - La `time-series` ressource doit être autorisée si vous utilisez un alias de propriété pour identifier le flux de données.
> - La `asset` ressource doit être autorisée si vous utilisez un ID d'actif pour identifier l'actif qui contient la propriété d'actif associée.

Pour plus d'informations sur la configuration des politiques IAM, consultez la section Gestion des politiques IAM dans le Guide de l'utilisateur IAM.

- Configurez les paramètres d'ingestion de données AWS IoT SiteWise pour autoriser l'acceptation de flux de données qui ne sont pas associés aux propriétés des actifs.

Rubriques

- Configuration des paramètres d'ingestion de données
- Gestion des flux de données

Configuration des paramètres d'ingestion de données

Console

Configurez AWS IoT SiteWise pour accepter les flux de données non associés aux propriétés des actifs à l'aide de la AWS IoT SiteWise console.

Pour configurer les paramètres d'ingestion de données (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans le volet de navigation, sous Paramètres, sélectionnez Ingestion de données.
3. Sur la page Ingestion des données, choisissez Modifier.
4. Dans la section Ingestion des données dissociées, sélectionnez Activer l'ingestion de données pour les flux de données non associés aux propriétés des actifs.

> **Important**
>
> Une fois que vous avez configuré AWS IoT SiteWise pour accepter les flux de données non associés aux propriétés des actifs, vous ne pouvez pas désactiver ce paramètre.

5. Choisissez Enregistrer.
6. Dans Activer l'ingestion de données dissociées, sélectionnez Mettre à jour. L'état de l'ingestion de données dissociées devient actif. Ce processus peut prendre quelques minutes.

AWS CLI

Configurez AWS IoT SiteWise pour accepter les flux de données non associés aux propriétés des actifs à l'aide de l'opération PutStorageConfigurationAPI. La section suivante utilise le AWS CLI.

Pour configurer les paramètres d'ingestion de données (AWS CLI)

1. AWS IoT SiteWise Pour configurer la réception de flux de données non associés aux propriétés des actifs, exécutez la commande suivante.

> **Important**
>
> Une fois que vous avez configuré AWS IoT SiteWise pour accepter les flux de données non associés aux propriétés des actifs, vous ne pouvez pas désactiver ce paramètre.

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

Vous pouvez configurer le `storageType` pour`MULTI_LAYER_STORAGE`. Pour plus d'informations, consultez Gestion du stockage des données.

Example réponse

```
{
```

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

Ce processus peut prendre quelques minutes.

2. Pour récupérer les informations de configuration du stockage, exécutez la commande suivante.

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

Example réponse

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

Gestion des flux de données

Gérez vos flux de données à l'aide du Console AWS IoT SiteWise ou AWS CLI.

Console

Utilisez la AWS IoT SiteWise console pour gérer vos flux de données.

Pour gérer les flux de données (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans le volet de navigation, sélectionnez Data streams.
3. (Facultatif) Pour ajouter ou mettre à jour des balises, sélectionnez le flux de données à modifier, puis choisissez Gérer les balises.

Sur la page Modifier les balises, choisissez Ajouter une étiquette. Dans le champ Clé, saisissez le nom de la balise à utiliser.

Choisissez Enregistrer.

4. (Facultatif) Dans le tableau des flux de données, vous pouvez filtrer les flux de données de la manière suivante.

   - Dans le premier menu déroulant, sélectionnez Préfixe d'alias ou ID d'actif.
     - Préfixe d'alias : préfixe d'alias du flux de données. Vous pouvez choisir cette option si vos flux de données cibles ont un préfixe d'alias.
     - ID d'actif : ID de l'actif dans lequel la propriété de l'actif a été créée. Vous pouvez choisir cette option si vos flux de données cibles sont associés à une propriété d'actif.
   - Dans le deuxième menu déroulant, sélectionnez Tous les flux de données, Flux de données associés ou Flux de données dissociés.
     - Tous les flux de données : flux de données associés ou non à une propriété d'actif.
     - Flux de données associés : flux de données associés à une propriété d'actif.
     - Flux de données dissociés : flux de données qui ne sont pas associés à une propriété d'actif.
5. Sélectionnez les flux de données que vous gérez. AWS IoT SiteWise affiche les flux de données que vous avez sélectionnés dans un graphique en bas de page. Si vous en sélectionnez plus de 10, le graphique n'affichera que les 10 premiers.
6. (Facultatif) Configurez le graphique de la manière suivante.

   a. Pour la fonction d'agrégation, sélectionnez l'une des options suivantes.

      - Nombre de points de données : nombre total de points de données pour les variables données sur l'intervalle de temps actuel.
      - Moyenne — La moyenne des valeurs des variables données sur l'intervalle de temps actuel.
      - Somme — Somme des valeurs des variables données sur l'intervalle de temps actuel.
      - Minimum — Le minimum des valeurs des variables données sur l'intervalle de temps actuel.
      - Maximum — Le maximum des valeurs des variables données sur l'intervalle de temps actuel.

Pour plus d'informations, consultez Utilisation de fonctions d'agrégation dans des expressions de formule.

b. Pour Plages temporelles, sélectionnez l'une des options suivantes.

- Dernière heure : le graphique affiche les données agrégées de la dernière heure.
- 2 dernières heures : le graphique affiche les données agrégées des deux dernières heures.
- 3 dernières heures : le graphique affiche les données agrégées des trois dernières heures.
- 4 dernières heures — Le graphique affiche les données agrégées des quatre dernières heures.

c. Pour Intervalle de temps, sélectionnez l'une des options suivantes.

- 1 minute : agrège les données toutes les minutes sur la plage de temps spécifiée.
- 1 heure : agrège les données toutes les heures sur la plage de temps spécifiée.

7. Choisissez Gérer les flux de données.
8. Dans la section Mettre à jour les associations de flux de données, dans la colonne Nom de la mesure, effectuez l'une des opérations suivantes.
   - Si le flux de données est associé à une mesure, supprimez l'association en cliquant sur l'icône de fermeture.
   - Si le flux de données n'est associé à aucune mesure, choisissez Choisir une mesure.
9. Dans le tableau Choisissez une mesure, naviguez jusqu'à l'actif cible, puis choisissez la mesure que vous associez.
10. (Facultatif) Dans la section Mettre à jour les alias des propriétés des actifs, entrez un alias unique pour chaque mesure.
11. Choisissez Mettre à jour.

La colonne Status peut afficher l'une des valeurs suivantes.

- En attente : vous mettez à jour l'association du flux de données ou l'alias de propriété de l'actif.
- Soumettre — La modification apportée à l'association ou à l'alias de propriété de l'actif est enregistrée.

- Erreur : AWS IoT SiteWise impossible de traiter votre demande de mise à jour de l'association du flux de données ou de l'alias de la mesure.
- Succès : vous avez correctement mis à jour l'association du flux de données ou l'alias de la mesure.

AWS CLI

Utilisez les opérations d'API suivantes pour gérer vos flux de données. Les exemples de code utilisent le AWS CLI.

- AssociateTimeSeriesToAssetProperty— Associe un flux de données (série chronologique) à une propriété d'actif.
- DisassociateTimeSeriesFromAssetProperty— Dissocie un flux de données d'une propriété d'actif.
- DeleteTimeSeries— Supprime un flux de données.
- DescribeTimeSeries— Récupère les informations relatives à un flux de données.
- ListTimeSeries— Récupère une liste paginée de flux de données.

AssociateTimeSeriesToAssetProperty

Pour associer un flux de données à une propriété d'actif, exécutez la commande suivante.

> **Important**
>
> La propriété d'actif spécifiée ne doit être actuellement associée à aucun flux de données.

- *data-stream-alias*Remplacez-le par l'alias du flux de données que vous associez.
- Remplacez *Asset-ID* par l'ID de l'actif dans lequel la propriété de l'actif a été créée.
- Remplacez *Property-ID* par l'ID de la propriété de l'actif.

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

DisassociateTimeSeriesFromAssetProperty

Pour dissocier un flux de données d'une propriété de ressource, exécutez la commande suivante.

- *data-stream-alias*Remplacez-le par l'alias du flux de données que vous dissociez.
- Remplacez *Asset-ID* par l'ID de l'actif dans lequel la propriété de l'actif a été créée.
- Remplacez *Property-ID* par l'ID de la propriété de l'actif.

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

DeleteTimeSeries

Pour supprimer un flux de données, exécutez la commande suivante.

*data-stream-alias*Remplacez-le par l'alias du flux de données que vous supprimez.

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

Pour identifier un flux de données, effectuez l'une des opérations suivantes :

- Si le flux de données n'est associé à aucune propriété d'actif, spécifiez le flux `alias` de données.
- Si le flux de données est associé à une propriété d'actif, spécifiez l'une des options suivantes :
  - Le `alias` du flux de données.
  - Le `assetId` et `propertyId` qui identifie la propriété de l'actif.

DescribeTimeSeries

Utilisez l'opération `DescribeTimeSeries` API pour vérifier si vous avez correctement associé ou dissocié un flux de données.

Pour récupérer des informations sur un flux de données, exécutez la commande suivante.

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

Pour identifier un flux de données, effectuez l'une des opérations suivantes :

- Si le flux de données n'est associé à aucune propriété d'actif, spécifiez le flux `alias` de données.
- Si le flux de données est associé à une propriété d'actif, spécifiez l'une des options suivantes :
  - Le `alias` du flux de données.
  - Le `assetId` et `propertyId` qui identifie la propriété de l'actif.

ListTimeSeries

Utilisez l'opération `ListTimeSeries` API pour vérifier si vous avez correctement supprimé un flux de données.

Pour récupérer une liste paginée de flux de données, exécutez la commande suivante.

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

Ingestion de données à l'aide de l'API AWS IoT SiteWise

Utilisez l' AWS IoT SiteWise API pour envoyer des données industrielles horodatées aux attributs et aux propriétés de mesure de vos actifs. L'API accepte une charge utile contenant des structures timestamp-quality-value (TQV).

Utilisez cette BatchPutAssetPropertyValueopération pour télécharger vos données. Grâce à cette opération, vous pouvez télécharger plusieurs entrées de données à la fois pour collecter des données provenant de plusieurs appareils et les envoyer en une seule demande.

> **Important**
>
> L'BatchPutAssetPropertyValueopération est soumise aux quotas suivants :
>
> - Jusqu'à 10 entrées par demande.
> - Jusqu'à 10 valeurs de propriété (points de données TQV) par entrée.
> - AWS IoT SiteWise rejette toutes les données dont l'horodatage date de plus de 7 jours dans le passé ou de plus de 10 minutes dans le futur.

Pour plus d'informations sur ces quotas, consultez BatchPutAssetPropertyValuela référence de l'AWS IoT SiteWise API.

Pour identifier une propriété d'actif, spécifiez l'une des options suivantes :

- La `assetId` fin `propertyId` de la propriété de l'actif à laquelle les données sont envoyées.
- Le`propertyAlias`, qui est un alias de flux de données (par exemple,`/company/windfarm/3/turbine/7/temperature`). Pour utiliser cette option, vous devez d'abord définir l'alias de votre propriété de ressource. Pour définir des alias de propriété, consultezMappage des flux de données industrielles avec des propriétés de ressources.

L'exemple suivant montre comment envoyer des lectures de température et de rotations par minute (RPM) d'une éolienne à partir d'une charge utile stockée dans un fichier JSON.

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

L'exemple de charge utile dans `batch-put-payload.json` comporte le contenu suivant.

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

Chaque entrée de la charge utile contient un `entryId` que vous pouvez définir sous la forme d'une chaîne unique. Si des entrées de demande échouent, chaque erreur contiendra l'`entryId` de la demande correspondante afin que vous sachiez quelles demandes réessayer.

Chaque structure de la liste des `propertyValues` est une structure timestamp-quality-value (TQV) qui contient a `valuetimestamp`, a et éventuellement a. `quality`

- `value`— Structure contenant l'un des champs suivants, selon le type de propriété définie :
  - `booleanValue`
  - `doubleValue`
  - `integerValue`
  - `stringValue`
- `timestamp`— Une structure qui contient l'heure actuelle d'Unix en secondes,. `timeInSeconds` Vous pouvez également définir la `offsetInNanos` clé dans la `timestamp` structure si vous disposez de données temporellement précises. AWS IoT SiteWise rejette tous les points de données dont l'horodatage date de plus de 7 jours dans le passé ou de moins de 10 minutes dans le futur.
- `quality`— (Facultatif) L'une des chaînes de qualité suivantes :
  - `GOOD`— (Par défaut) Les données ne sont affectées par aucun problème.
  - `BAD`— Les données sont affectées par un problème tel qu'une défaillance du capteur.
  - `UNCERTAIN`— Les données sont affectées par un problème tel que l'imprécision du capteur.

Pour plus d'informations sur la gestion de AWS IoT SiteWise la qualité des données dans les calculs, consultez la section Qualité des données dans les expressions de formule.

Ingestion de données à l'aide de règles AWS IoT Core

Envoyez des données AWS IoT SiteWise depuis des AWS IoT objets et d'autres AWS services en utilisant des règles dans AWS IoT Core. Les règles transforment les messages MQTT et exécutent des actions pour interagir avec les AWS services. L'action de AWS IoT SiteWise règle transmet les données des messages à l'BatchPutAssetPropertyValueopération depuis l' AWS IoT SiteWise API. Pour plus d'informations, consultez la section Règles et AWS IoT SiteWise actions du Guide du AWS IoT développeur.

Pour suivre un didacticiel décrivant les étapes nécessaires à la configuration d'une règle qui ingère des données par le biais des ombres des appareils, voirIngestion de données provenant d'objets AWS IoT.

Vous pouvez également envoyer des données depuis AWS IoT SiteWise d'autres AWS services. Pour plus d'informations, consultez Interaction avec d'autres AWS services.

Rubriques

- Octroi AWS IoT de l'accès requis
- Configuration de l'action de la AWS IoT SiteWise règle
- Réduction des coûts grâce à l'ingestion de base

Octroi AWS IoT de l'accès requis

Vous utilisez les rôles IAM pour contrôler les AWS ressources auxquelles chaque règle a accès. Avant de créer une règle, vous devez créer un rôle IAM avec une politique qui permet à la règle d'effectuer des actions sur la AWS ressource requise. AWS IoT assume ce rôle lors de l'exécution d'une règle.

Si vous créez l'action de règle dans la AWS IoT console, vous pouvez choisir une ressource racine pour créer un rôle ayant accès à une hiérarchie de ressources sélectionnée. Pour plus d'informations sur la façon de définir manuellement un rôle pour une règle, consultez les sections Accorder AWS IoT les autorisations d'accès et de transfert de rôle requises dans le Guide du AWS IoT développeur.

Pour l'action de la AWS IoT SiteWise règle, vous devez définir un rôle qui autorise l'`iotsitewise:BatchPutAssetPropertyValue`accès aux propriétés des actifs auxquels la règle envoie des données. Pour améliorer la sécurité, vous pouvez spécifier un chemin hiérarchique des AWS IoT SiteWise actifs dans la `Condition` propriété.

L'exemple de stratégie d'approbation suivant permet d'accéder à une ressource spécifique et à ses enfants.

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

`Condition`Supprimez-le de la politique pour autoriser l'accès à tous vos actifs. L'exemple de stratégie d'approbation suivant permet d'accéder à toutes vos ressources dans la région active.

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

Configuration de l'action de la AWS IoT SiteWise règle

L'action de AWS IoT SiteWise règle envoie les données du message MQTT à l'origine de la règle aux propriétés des actifs dans AWS IoT SiteWise. Vous pouvez télécharger plusieurs entrées de données sur différentes propriétés d'actifs en même temps, afin d'envoyer des mises à jour pour tous les capteurs d'un appareil en un seul message. Vous pouvez également charger plusieurs points de données à la fois pour chaque entrée de données.

> **Note**
>
> Lorsque vous envoyez des données à AWS IoT SiteWise avec l'action de règle, vos données doivent répondre à toutes les exigences de l'`BatchPutAssetPropertyValue`opération. Par exemple, vos données ne peuvent pas être horodatées de moins de 7 jours par rapport à l'époque Unix actuelle. Pour plus d'informations, consultez Ingestion de données avec l'API AWS IoT SiteWise.

Pour chaque entrée de données de l'action de règle, vous identifiez une propriété de ressource et spécifiez l'horodatage, la qualité et la valeur de chaque point de données pour cette propriété. L'action de règle accepte des chaînes pour tous les paramètres.

Pour identifier une propriété de ressource, vous pouvez spécifier l'une des options suivantes :

- ID de ressource (`assetId`) et ID de propriété (`propertyId`) pour la propriété de ressource à laquelle vous envoyez des données. Vous pouvez trouver l'ID d'actif et l'ID de propriété à l'aide du Console AWS IoT SiteWise. Si vous connaissez l'identifiant de l'actif, vous pouvez utiliser le AWS CLI DescribeAssetto call pour trouver l'identifiant de la propriété.
- Alias de propriété (`propertyAlias`), qui est un alias de flux de données (par exemple, `/company/windfarm/3/turbine/7/temperature`). Pour utiliser cette option, vous devez d'abord définir l'alias de votre propriété de ressource. Pour découvrir comment définir des alias de propriété de ressource, consultez Mappage des flux de données industrielles avec des propriétés de ressources.

Pour l'horodatage de chaque entrée, utilisez l'horodatage indiqué par votre équipement ou l'horodatage fourni par. AWS IoT Core L'horodatage comporte deux paramètres :

- Durée en secondes (`timeInSeconds`) — Durée de l'époque Unix, en secondes, à laquelle le capteur ou l'équipement a rapporté les données.

- Décalage en nanos (`offsetInNanos`) — (Facultatif) Le décalage de nanosecondes par rapport au temps en secondes.

> **Important**
>
> Si votre horodatage est une chaîne, comporte une partie décimale ou n'est pas exprimé en secondes, AWS IoT SiteWise rejette la demande. Vous devez convertir l'horodatage en secondes et en décalage de nanosecondes. Utilisez les fonctionnalités du moteur de AWS IoT règles pour convertir l'horodatage. Pour plus d'informations, consultez les ressources suivantes :
>
> - Obtenir des horodatages pour les appareils qui n'indiquent pas l'heure exacte
> - Conversion des horodatages au format chaîne

Vous pouvez utiliser des modèles de substitution pour plusieurs paramètres de l'action afin d'effectuer des calculs, d'invoquer des fonctions et d'extraire des valeurs de la charge utile du message. Pour plus d'informations, consultez la section Modèles de substitution dans le Guide du AWS IoT développeur.

> **Note**
>
> Comme une expression dans un modèle de substitution est évaluée séparément de l'instruction `SELECT`, vous ne pouvez pas utiliser un modèle de substitution pour référencer un alias créé à l'aide d'une clause `AS`. Vous pouvez référencer uniquement les informations présentes dans la charge utile d'origine, en plus des fonctions et opérateurs pris en charge.

Rubriques

- Obtenir des horodatages pour les appareils qui n'indiquent pas l'heure exacte
- Conversion des horodatages au format chaîne
- Conversion de chaînes d'horodatage d'une précision de la nanoseconde
- Exemples de configurations de règles
- Dépannage de l'action de règle

Obtenir des horodatages pour les appareils qui n'indiquent pas l'heure exacte

Si votre capteur ou équipement ne fournit pas de données temporelles précises, obtenez l'heure actuelle de l'époque Unix à partir du moteur de AWS IoT règles avec timestamp (). Cette fonction affiche le temps en millisecondes. Vous devez donc convertir la valeur en temps en secondes et en décalage en nanosecondes. Pour ce faire, utilisez les conversions suivantes :

- Pour Time in seconds (Délai en secondes) (`timeInSeconds`), utilisez **`${floor(timestamp() / 1E3)}`** pour convertir le temps de millisecondes en secondes.
- Pour Offset in nanos (Décalage en nanosecondes) (`offsetInNanos`), utilisez **`${(timestamp() % 1E3) * 1E6}`** pour calculer le décalage en nanosecondes de l'horodatage.

Conversion des horodatages au format chaîne

Si votre capteur ou équipement indique les données temporelles sous forme de chaîne (par exemple,`2020-03-03T14:57:14.699Z`), utilisez time_to_epoch (String, String). Cette fonction saisit l'horodatage et le modèle de format sous forme de paramètres et affiche le temps en millisecondes. Ensuite, vous devez convertir le temps en temps en secondes et en décalage en nanosecondes. Pour ce faire, utilisez les conversions suivantes :

- Pour Time in seconds (`timeInSeconds`), utilisez cette option **`${floor(time_to_epoch("2020-03-03T14:57:14.699Z", "yyyy-MM-dd'T'HH:mm:ss'Z'") / 1E3)}`** pour convertir la chaîne d'horodatage en millisecondes, puis en secondes.
- Pour Offset in nanos (`offsetInNanos`), utilisez **`${(time_to_epoch("2020-03-03T14:57:14.699Z", "yyyy-MM-dd'T'HH:mm:ss'Z'") % 1E3) * 1E6}`** pour calculer le décalage en nanosecondes de la chaîne d'horodatage.

> **Note**
>
> La `time_to_epoch` fonction prend en charge les chaînes d'horodatage d'une précision maximale de quelques millisecondes. Pour convertir des chaînes avec une précision de la microseconde ou de la nanoseconde, configurez une AWS Lambda fonction appelée par votre règle pour convertir l'horodatage en valeurs numériques. Pour plus d'informations, consultez Conversion de chaînes d'horodatage d'une précision de la nanoseconde.

Conversion de chaînes d'horodatage d'une précision de la nanoseconde

Si votre appareil envoie des informations d'horodatage sous forme de chaîne avec une précision de la nanoseconde (par exemple,`2020-03-03T14:57:14.699728491Z`), suivez la procédure suivante pour configurer l'action de votre règle. Vous pouvez créer une AWS Lambda fonction qui convertit l'horodatage d'une chaîne en heure en secondes (`timeInSeconds`) et en décalage en nanos (). `offsetInNanos` Utilisez ensuite aws_lambda (FunctionArn, InputJson) dans les paramètres d'action de votre règle pour appeler cette fonction Lambda et utiliser la sortie de votre règle.

> **Note**
>
> Cette section contient des instructions avancées qui supposent que vous êtes familier avec la création des ressources suivantes :
>
> - Fonctions Lambda. Pour plus d'informations, voir Création d'une fonction Lambda avec la console ou Utilisation de Lambda avec la AWS CLI dans le manuel du développeur.AWS Lambda
> - AWS IoT règles avec l'action de la AWS IoT SiteWise règle. Pour plus d'informations, consultez Ingestion de données à l'aide de règles AWS IoT Core.

Pour créer une action de AWS IoT SiteWise règle qui analyse les chaînes d'horodatage

1. Créez une fonction Lambda avec les propriétés suivantes :
   - Nom de la fonction : utilisez un nom de fonction descriptif (par exemple,**`ConvertNanosecondTimestampFromString`**).
   - Runtime — Utilisez un environnement d'exécution Python 3, tel que Python 3.11 (`python3.11`).
   - Autorisations — Créez un rôle avec des autorisations Lambda de base () AWS LambdaBasicExecutionRole.
   - Couches — Ajoutez la couche AWS SDKPandas-Python311 à utiliser par la fonction Lambda. `numpy`
   - Code de fonction — Utilisez le code de fonction suivant, qui utilise un argument de chaîne nommé `timestamp` `timeInSeconds` et génère des `offsetInNanos` valeurs pour cet horodatage.

```
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
    }
```

Cette fonction Lambda saisit des chaînes d'horodatage au format ISO 8601 à l'aide de datetime64 à partir de. NumPy

> **Note**
>
> Si vos chaînes d'horodatage ne sont pas au format ISO 8601, vous pouvez implémenter une solution pandas qui définit le format d'horodatage. Pour plus d'informations, consultez pandas.to_datetime.

2. Lorsque vous configurez l' AWS IoT SiteWise action pour votre règle, utilisez les modèles de substitution suivants pour le temps en secondes (`timeInSeconds`) et le décalage en nanos (`offsetInNanos`). Ces modèles de substitution supposent que votre charge utile de message contient la chaîne d'horodatage dans `timestamp`. La fonction `aws_lambda` utilise une structure JSON pour son second paramètre, de sorte que vous pouvez modifier les modèles de substitution ci-dessous si nécessaire.

   - Pour Time in seconds (Temps en secondes) (`timeInSeconds`), utilisez le modèle de substitution suivant.

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

- Pour Offset in nanos (Décalage en nanos) (`offsetInNanos`), utilisez le modèle de substitution suivant.

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

Pour chaque paramètre, remplacez *`region`* et *`account-id`* par votre région et votre identifiant de AWS compte. Si vous avez utilisé un autre nom pour votre fonction Lambda, modifiez-le également.

3. Accordez AWS IoT les autorisations nécessaires pour appeler votre fonction avec `lambda:InvokeFunction` cette autorisation. Pour de plus amples informations, veuillez consulter aws_lambda(functionArn, inputJson).
4. Testez votre règle (par exemple, utilisez le client de test AWS IoT MQTT) et vérifiez qu'il AWS IoT SiteWise reçoit les données que vous envoyez.

   Si votre règle ne fonctionne pas comme prévu, veuillez consulter Résolution des problèmes liés à une action de AWS IoT SiteWise règle.

> **Note**
>
> Cette solution appelle la fonction Lambda deux fois pour chaque chaîne d'horodatage. Vous pouvez créer une autre règle pour réduire le nombre d'appels de fonctions Lambda si votre règle gère plusieurs points de données ayant le même horodatage dans chaque charge utile. Pour ce faire, créez une règle avec une action de republication qui invoque le Lambda et publie la charge utile d'origine avec la chaîne d'horodatage convertie en et. `timeInSeconds` `offsetInNanos` Créez ensuite une règle avec une action de AWS IoT SiteWise règle pour consommer la charge utile convertie. Avec cette approche, vous réduisez le nombre de fois que la règle invoque le Lambda, mais vous augmentez le nombre AWS IoT d'actions de règle exécutées. Pensez à la tarification de chaque service si vous appliquez cette solution à votre cas d'utilisation.

Exemples de configurations de règles

Cette section contient des exemples de configurations de règles permettant de créer une règle avec une AWS IoT SiteWise action.

Example Exemple d'action de règle qui utilise des alias de propriété comme rubriques de message

L'exemple suivant crée une règle avec une AWS IoT SiteWise action qui utilise le topic (via topic ()) comme alias de propriété pour identifier les propriétés des actifs. Utilisez cet exemple pour définir une règle pour l'ingestion de données de type double pour toutes les éoliennes de tous les parcs éoliens. Cet exemple nécessite que vous définissiez des alias de propriété sur les propriétés de tous les actifs de turbine. Vous devez définir une deuxième règle similaire pour ingérer des données de type entier.

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

L'exemple de charge utile dans `sitewise-rule-payload.json` comporte le contenu suivant.

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

Avec cette action de règle, envoyez le message suivant à un alias de propriété d'éolienne (par exemple,`/company/windfarm/3/turbine/7/temperature`) en tant que sujet pour ingérer des données.

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

Example Exemple d'action de règle qui utilise timestamp() pour déterminer l'heure

L'exemple suivant crée une règle avec une AWS IoT SiteWise action qui identifie une propriété d'actif par des identifiants et utilise timestamp () pour déterminer l'heure actuelle.

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

L'exemple de charge utile dans `sitewise-rule-payload.json` comporte le contenu suivant.

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

Avec cette action de règle, envoyez le message suivant au pour `my/asset/property/topic` ingérer des données.

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

Dépannage de l'action de règle

Pour résoudre les problèmes liés à votre action de AWS IoT SiteWise règle dans AWS IoT Core, configurez CloudWatch les journaux ou configurez une action d'erreur de republication pour votre règle. Pour plus d'informations, consultez Résolution des problèmes liés à une action de AWS IoT SiteWise règle.

Réduction des coûts grâce à l'ingestion de base

AWS IoT Core fournit une fonctionnalité appelée Basic Ingest que vous pouvez utiliser pour envoyer des données AWS IoT Core sans encourir AWS IoT de frais de messagerie. Cette fonctionnalité optimise le flux de données pour les charges de travail relatives à l'ingestion de grands volumes de données en supprimant l'agent de messages de publication et d'abonnement dans le circuit d'ingestion. Vous pouvez utiliser l'ingestion de base si vous connaissez les règles vers lesquelles vos messages doivent être acheminés.

Pour utiliser l'ingestion de base, vous envoyez des messages directement à une règle spécifique à l'aide d'une rubrique spéciale, `$aws/rules/rule-name`. Par exemple, pour envoyer un message à une règle nommée `SiteWiseWindFarmRule`, vous envoyez un message à la rubrique `$aws/rules/SiteWiseWindFarmRule`.

Si votre action de règle utilise des modèles de substitution contenant topic(Decimal), vous pouvez transmettre la rubrique d'origine à la fin de la rubrique spéciale d'ingestion de base, par exemple `$aws/rules/rule-name/original-topic`. Par exemple, pour utiliser l'ingestion de base avec l'exemple d'alias de propriété de parc éolien de la section précédente, vous pouvez envoyer des messages à la rubrique suivante.

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

> **Note**
>
> L'exemple ci-dessus inclut une deuxième barre oblique (`//`) car AWS IoT le préfixe Basic Ingest (`$aws/rules/rule-name/`) est supprimé de la rubrique visible par l'action de la règle. Dans cet exemple, la règle reçoit la rubrique `/company/windfarm/3/turbine/7/temperature`.

Pour plus d'informations, consultez la section Réduction des coûts de messagerie grâce à l'ingestion de base dans le Guide du AWS IoT développeur.

Ingestion de données provenant de AWS IoT Events

Avec AWS IoT Events, vous pouvez créer des applications complexes de surveillance des événements pour votre flotte IoT dans le AWS cloud. Utilisez l' SiteWise action IoT AWS IoT Events pour envoyer des données aux propriétés des actifs AWS IoT SiteWise lorsqu'un événement se produit.

AWS IoT Events est conçu pour rationaliser le développement d'applications de surveillance des événements pour les appareils et systèmes IoT dans le AWS cloud. En utilisant AWS IoT Events, vous pouvez :

- Détectez les changements, les anomalies ou les conditions spécifiques au sein de votre flotte IoT et répondez-y.

- Améliorez votre efficacité opérationnelle et permettez une gestion proactive de votre écosystème IoT.

En l'intégrant AWS IoT SiteWise via l' AWS IoT SiteWise action, il AWS IoT Events étend ses fonctionnalités, vous permettant de mettre à jour automatiquement les propriétés des actifs AWS IoT SiteWise en réponse à des événements spécifiques. Cette interaction peut simplifier l'ingestion et la gestion des données. Il peut également vous fournir des informations exploitables.

Pour plus d'informations, consultez les rubriques suivantes du guide du AWS IoT Events développeur :

- Qu'est-ce que c'est AWS IoT Events ?
- Actions AWS IoT Events
- SiteWise Action dans le domaine de l'IoT

Utilisation du gestionnaire de AWS IoT Greengrass flux

AWS IoT Greengrass le gestionnaire de flux est une fonctionnalité d'intégration qui facilite le transfert de flux de données depuis des sources locales vers le AWS Cloud. Il agit comme une couche intermédiaire qui gère les flux de données, permettant aux appareils fonctionnant en périphérie de collecter et de stocker les données avant qu'elles ne soient envoyées AWS IoT SiteWise, pour une analyse et un traitement plus approfondis.

Ajoutez une destination de données en configurant une source locale sur la AWS IoT SiteWise console. Vous pouvez également utiliser le gestionnaire de flux dans votre AWS IoT Greengrass solution personnalisée pour ingérer AWS IoT SiteWise des données.

> **Note**
>
> Pour ingérer des données provenant de sources OPC-UA, configurez une passerelle AWS IoT SiteWise Edge qui s'exécute sur. AWS IoT Greengrass Pour plus d'informations, consultez Utilisation des passerelles SiteWise Edge.

Pour plus d'informations sur la configuration d'une destination pour les données source locales, consultezConfiguration des sources de données.

Pour plus d'informations sur la façon d'ingérer des données à l'aide du gestionnaire de flux dans une AWS IoT Greengrass solution personnalisée, consultez les rubriques suivantes du guide du AWS IoT Greengrass Version 2 développeur :

- Qu'est-ce que c'est AWS IoT Greengrass ?
- Gérez les flux de données sur le AWS IoT Greengrass cœur
- Exportation de données vers les propriétés des AWS IoT SiteWise actifs

Ingestion de données à l'aide de l'API CreateBulkImportJob

Utilisez l'`CreateBulkImportJob`API pour importer de grandes quantités de données depuis Amazon S3. Vos données doivent être enregistrées au format CSV dans Amazon S3. Les fichiers de données peuvent comporter les colonnes suivantes.

> **Note**
>
> Pour identifier une propriété d'actif, spécifiez l'une des options suivantes.
>
> - La `ASSET_ID` fin `PROPERTY_ID` de la propriété de l'actif à laquelle vous envoyez des données.
> - Le`ALIAS`, qui est un alias de flux de données (par exemple,`/company/windfarm/3/turbine/7/temperature`). Pour utiliser cette option, vous devez d'abord définir l'alias de votre propriété de ressource. Pour découvrir comment définir des alias de propriété de ressource, consultez the section called “Mappage des flux de données industrielles avec des propriétés de ressources”.

- `ALIAS`— L'alias qui identifie la propriété, tel qu'un chemin de flux de données du serveur OPC-UA (par exemple,`/company/windfarm/3/turbine/7/temperature`). Pour plus d'informations, consultez Mappage des flux de données industrielles avec des propriétés de ressources.
- `ASSET_ID`— L'ID de l'actif.
- `PROPERTY_ID`— L'ID de la propriété de l'actif.
- `DATA_TYPE`— Le type de données de la propriété peut être l'un des suivants.
  - `STRING`— Chaîne de 1024 octets maximum.
  - `INTEGER`— Un entier signé de 32 bits dont la plage est comprise entre [-2 147 483 648, 2 147 483 647].

  - `DOUBLE`— Un nombre à virgule flottante avec une plage [-10^100, 10^100] et une double précision IEEE 754.
  - `BOOLEAN`— `true` ou`false`.
- `TIMESTAMP_SECONDS`— L'horodatage du point de données, à l'époque Unix.
- `TIMESTAMP_NANO_OFFSET`— Le décalage en nanosecondes converti à partir de. `TIMESTAMP_SECONDS`
- `QUALITY`— (Facultatif) La qualité de la valeur de la propriété de l'actif. La valeur peut être l'une des suivantes.
  - `GOOD`— (Par défaut) Les données ne sont affectées par aucun problème.
  - `BAD`— Les données sont affectées par un problème tel qu'une défaillance du capteur.
  - `UNCERTAIN`— Les données sont affectées par un problème tel que l'imprécision du capteur.

  Pour plus d'informations sur la gestion de AWS IoT SiteWise la qualité des données dans les calculs, consultez la section Qualité des données dans les expressions de formule.
- `VALUE`— La valeur de la propriété de l'actif.

Example fichier (s) de données au format .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 fournit les opérations d'API suivantes pour créer une tâche d'importation en bloc et obtenir des informations sur une tâche existante.

- CreateBulkImportJob— Crée une nouvelle tâche d'importation en bloc.

- DescribeBulkImportJob— Récupère les informations relatives à une tâche d'importation groupée.
- ListBulkImportJob— Récupère une liste paginée de résumés de toutes les tâches d'importation en bloc.

Création d'une tâche d'importation en bloc (AWS CLI)

Utilisez l'opération CreateBulkImportJobd'API pour transférer des données d'Amazon S3 vers AWS IoT SiteWise. Utilisez l'CreateBulkImportJobAPI pour ingérer des données par petits lots de manière rentable. L'exemple suivant utilise AWS CLI.

> **Important**
>
> Avant de créer une tâche d'importation en bloc, vous devez activer le niveau AWS IoT SiteWise chaud ou le niveau AWS IoT SiteWise froid. Pour plus d'informations, consultez Configuration des paramètres de stockage.
> L'importation en bloc est conçue pour stocker les données historiques dans AWS IoT SiteWise. Il ne lance pas de calculs ni de notifications en mode AWS IoT SiteWise chaud ou en mode AWS IoT SiteWise froid.

Exécutez la commande suivante. Remplacez *file-name* par le nom du fichier contenant la configuration de la tâche d'importation en bloc.

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

Example Configuration des tâches d'importation en bloc

Voici des exemples de paramètres de configuration :

- Remplacez *adaptive-ingestion-flag* par `true` ou `false`.
  - Si cette valeur est définie sur`false`, la tâche d'importation en bloc ingère les données historiques dans AWS IoT SiteWise.
  - Si cette valeur est définie sur`true`, la tâche d'importation en bloc effectue les opérations suivantes :
    - Ingère de nouvelles données dans. AWS IoT SiteWise
    - Calcule les métriques et les transforme, et prend en charge les notifications pour les données dont l'horodatage est établi dans les sept jours.

- Remplacez *delete-files-after-import-flag* par `true` pour supprimer les données du compartiment de données S3 après les avoir ingérées dans un stockage à AWS IoT SiteWise chaud.
- Remplacez *error-bucket* par le nom du compartiment Amazon S3 auquel les erreurs associées à cette tâche d'importation en masse sont envoyées.
- *error-bucket-prefix*Remplacez-le par le préfixe du compartiment Amazon S3 auquel les erreurs associées à cette tâche d'importation en masse sont envoyées.

  Amazon S3 utilise le préfixe comme nom de dossier pour organiser les données dans le compartiment. Chaque objet Amazon S3 possède une clé qui constitue son identifiant unique dans le compartiment. Chaque objet d'un compartiment possède une clé et une seule. Le préfixe doit se terminer par une barre oblique (/). Pour plus d'informations, consultez la section Organisation des objets à l'aide de préfixes dans le guide de l'utilisateur d'Amazon Simple Storage Service.
- Remplacez *data-bucket* par le nom du bucket Amazon S3 à partir duquel les données sont importées.
- *data-bucket-key*Remplacez-la par la clé de l'objet Amazon S3 qui contient vos données. Chaque objet a une clé qui est un identifiant unique. Chaque objet a exactement une clé.
- *data-bucket-version-id*Remplacez-le par l'ID de version pour identifier une version spécifique de l'objet Amazon S3 contenant vos données. Ce paramètre est facultatif.
- Remplacez le *nom de colonne* par le nom de colonne spécifié dans le fichier .csv.
- Remplacez *le nom* de la tâche par un nom unique identifiant la tâche d'importation en bloc.
- Remplacez *job-role-arn*par le rôle IAM qui permet AWS IoT SiteWise de lire les données Amazon S3.

> **Note**
>
> Assurez-vous que votre rôle dispose des autorisations indiquées dans l'exemple suivant. Remplacez *data-bucket* par le nom du bucket Amazon S3 qui contient vos données. Remplacez également *error-bucket* par le nom du compartiment Amazon S3 auquel les erreurs associées à cette tâche d'importation en masse sont envoyées.
>
> ```
> {
>     "Version": "2012-10-17",
>     "Statement": [
>         {
>             "Action": [
> ```

```
                "s3:GetObject",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::data-bucket",
                "arn:aws:s3:::data-bucket/*",
            ],
            "Effect": "Allow"
        },
       {
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::error-bucket",
                "arn:aws:s3:::error-bucket/*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

```
{
   "adaptiveIngestion": adaptive-ingestion-flag,
   "deleteFilesAfterImport": delete-files-after-import-flag,
   "errorReportLocation": {
      "bucket": "error-bucket",
      "prefix": "error-bucket-prefix"
   },
   "files": [
      {
         "bucket": "data-bucket",
         "key": "data-bucket-key",
         "versionId": "data-bucket-version-id"
      }
   ],
   "jobConfiguration": {
      "fileFormat": {
         "csv": {
```

```
            "columnNames": [ "column-name" ]
         }
      }
   },
   "jobName": "job-name",
   "jobRoleArn": "job-role-arn"
}
```

Example réponse

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

Décrire une tâche d'importation en masse (AWS CLI)

Utilisez l'opération DescribeBulkImportJobAPI pour récupérer les informations relatives à une tâche d'importation en bloc. L'exemple suivant utilise AWS CLI.

Remplacez *Job-ID* par l'ID de la tâche d'importation en bloc que vous souhaitez récupérer.

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

Example réponse

```
{
   "files":[
      {
         "bucket":"test-bucket",
         "key":"100Tags12Hours.csv"
      },
      {
         "bucket":"test-bucket",
         "key":"BulkImportData1MB.csv"
      },
      {
         "bucket":"test-bucket",
         "key":"UnmodeledBulkImportData1MB.csv"
      }
```

```
   ],
   "errorReportLocation":{
      "prefix":"errors/",
      "bucket":"test-error-bucket"
   },
   "jobConfiguration":{
      "fileFormat":{
         "csv":{
            "columnNames":[
               "ALIAS",
               "DATA_TYPE",
               "TIMESTAMP_SECONDS",
               "TIMESTAMP_NANO_OFFSET",
               "QUALITY",
               "VALUE"
            ]
         }
      }
   },
   "jobCreationDate":1645745176.498,
   "jobStatus":"COMPLETED",
   "jobName":"myBulkImportJob",
   "jobLastUpdateDate":1645745279.968,
   "jobRoleArn":"arn:aws:iam::123456789012:role/DemoRole",
   "jobId":"f8c031d0-01d1-4b94-90b1-afe8bb93b7e5"
}
```

Répertorier les tâches d'importation en bloc (AWS CLI)

Utilisez l'opération ListBulkImportJobsAPI pour récupérer une liste paginée de résumés de toutes les tâches d'importation en bloc. L'exemple suivant utilise AWS CLI.

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

Example réponse

```
{
   "jobSummaries":[
      {
         "id":"bdbbfa52-d775-4952-b816-13ba1c7cb9da",
         "name":"myBulkImportJob",
         "status":"COMPLETED"
```

```
      },
      {
         "id":"15ffc641-dbd8-40c6-9983-5cb3b0bc3e6b",
         "name":"myBulkImportJob2",
         "status":"RUNNING"
      }
   ]
}
```

Utilisation des passerelles SiteWise Edge

Une passerelle AWS IoT SiteWise Edge sert d'intermédiaire entre votre équipement industriel et AWS IoT SiteWise. La passerelle SiteWise Edge s'exécute et prend AWS IoT Greengrass V2 en charge la collecte et le traitement des données sur site. Vous pouvez utiliser AWS OpsHub for AWS IoT SiteWise pour gérer vos passerelles SiteWise Edge et surveiller les opérations sur site.

Vous pouvez surveiller les données localement dans votre établissement à l'aide des portails de SiteWise surveillance installés sur vos appareils locaux. Pour plus d'informations, voir Activation de votre portail à la périphérie.

Rubriques

- SiteWise Exigences relatives à la passerelle Edge
- Création d'une passerelle SiteWise Edge
- Installation du logiciel de passerelle SiteWise Edge sur votre appareil local
- Permettre le traitement des données de pointe
- Traitement des données à la périphérie
- Configuration du composant AWS IoT SiteWise Publisher
- Configuration des sources de données
- Ajouter des sources de données partenaires aux passerelles SiteWise Edge
- Utiliser des packs
- Gestion des passerelles SiteWise Edge
- Running SiteWise Edge sur Siemens Industrial Edge
- Filtrer les actifs sur une passerelle SiteWise Edge
- Utilisation d'AWS IoT SiteWiseAPI à la périphérie
- Backup et restauration des passerelles SiteWise Edge
- Configuration des passerelles SiteWise Edge ()AWS IoT Greengrass Version 1

SiteWise Exigences relatives à la passerelle Edge

AWS IoT SiteWise Les passerelles Edge fonctionnent AWS IoT Greengrass V2 sous la forme d'un ensemble de AWS IoT Greengrass composants qui prennent en charge la collecte, le traitement et la publication de données sur site. Pour configurer une passerelle SiteWise Edge qui s'exécute sur

AWS IoT Greengrass V2, vous devez créer une passerelle dans le logiciel de passerelle SiteWise Edge AWS Cloud et exécuter le logiciel de passerelle Edge pour configurer votre appareil local.

Prérequis

Les appareils locaux doivent répondre aux exigences suivantes pour installer et exécuter le logiciel de passerelle SiteWise Edge.

- Supporte la version v2.3.0 ou ultérieure du logiciel AWS IoT Greengrass V2 Core. Pour plus d'informations, consultez la section Exigences du guide du AWS IoT Greengrass Version 2 développeur.
- L'une des plateformes prises en charge suivantes :
  - Système d'exploitation : Ubuntu 20.04 ou version ultérieure

    Architecture : x86_64 (AMD64) ou ARMv8 (Aarch64)
  - Système d'exploitation : Red Hat Enterprise Linux (RHEL) 8

    Architecture : x86_64 (AMD64) ou ARMv8 (Aarch64)
  - Système d'exploitation : Amazon Linux 2

    Architecture : x86_64 (AMD64) ou ARMv8 (Aarch64)
  - Système d'exploitation : Debian 11

    Architecture : x86_64 (AMD64) ou ARMv8 (Aarch64)
  - Système d'exploitation : Windows Server 2019 et versions ultérieures

    Architecture : x86_64 (AMD64)

  > **Note**
  >
  > Les plateformes ARM prennent en charge les passerelles SiteWise Edge uniquement avec le pack de collecte de données. Le pack de traitement des données n'est pas pris en charge.

- Minimum de 4 Go de RAM.
- Au moins 10 Go d'espace disque disponible pour le logiciel de passerelle SiteWise Edge.
- Si vous envisagez de traiter des données en périphérie AWS IoT SiteWise, votre appareil local doit également répondre aux exigences suivantes :

  - Dispose d'un processeur quadricœur x86 64 bits.
  - Dispose d'au moins 16 Go de RAM.
  - Dispose d'au moins 32 Go de RAM si vous utilisez Windows.
  - Disposait d'au moins 256 Go d'espace disque libre.
- Les exigences minimales en matière d'espace disque et de capacité de calcul dépendent de divers facteurs propres à votre implémentation et à votre cas d'utilisation.
  - L'espace disque requis pour la mise en cache des données pour une connectivité Internet intermittente dépend des facteurs suivants :
    - Nombre de flux de données chargés
    - Points de données par flux de données par seconde
    - Taille de chaque point de données
    - Vitesses de communication
    - Temps d'arrêt du réseau attendu
  - La capacité de calcul requise pour interroger et charger les données dépend des facteurs suivants :
    - Nombre de flux de données chargés
    - Points de données par flux de données par seconde
- Configurez votre appareil local pour accéder au compartiment S3 suivant :`iot-sitewise-gateway-<region>-748875242063`.
- Configurez votre appareil local pour vous assurer que les ports suivants sont accessibles :
  - Le périphérique local doit autoriser le trafic réseau entrant sur le port 443.
  - Le périphérique local doit autoriser le trafic sortant sur les ports 443 et 8883.

    Pour obtenir la liste complète des points de terminaison de service sortants requis, voir Points de terminaison de service requis pour les AWS IoT SiteWise passerelles Edge.
  - Les ports suivants sont réservés pour être utilisés par AWS IoT SiteWise : 80, 443, 3001, 4569, 4572, 8000, 8081, 8082, 8084, 8085, 8445, 8086, 9000, 9500, 11080 et 50010. L'utilisation d'un port réservé pour le trafic peut entraîner l'interruption de la connexion.

> **Note**
>
> Le composant AWS IoT Greengrass V2 Stream manager a ses propres exigences. Pour plus d'informations, consultez la section Configuration dans le guide du AWS IoT Greengrass Version 2 développeur.

- Java Runtime Environment (JRE) version 11 ou supérieure. Java doit être disponible sur la variable d'`PATH`environnement de l'appareil. Pour utiliser Java pour développer des composants personnalisés, vous devez installer un kit de développement Java (JDK). Nous vous recommandons d'utiliser Amazon Corretto ou OpenJDK.

Vous devez disposer des autorisations suivantes pour utiliser les passerelles SiteWise Edge :

> **Note**
>
> Si vous utilisez la AWS IoT SiteWise console pour créer votre passerelle SiteWise Edge, ces autorisations sont ajoutées pour vous.

- Le rôle IAM de votre passerelle SiteWise Edge doit vous permettre d'utiliser une passerelle SiteWise Edge sur un AWS IoT Greengrass V2 appareil pour traiter les données des modèles d'actifs et les données des actifs.

  Le rôle permet au service suivant d'assumer le rôle :`credentials.iot.amazonaws.com`.

  Détails de l'autorisation

  Le rôle doit disposer des autorisations suivantes :

  - `iotsitewise`— Permet aux principaux de récupérer les données des modèles d'actifs et les données des actifs à la périphérie.
  - `iot`— Permet à vos AWS IoT Greengrass V2 appareils d'interagir avec AWS IoT.
  - `logs`— Permet à vos AWS IoT Greengrass V2 appareils d'envoyer des journaux à Amazon CloudWatch Logs.
  - `s3`— Permet à vos AWS IoT Greengrass V2 appareils de télécharger des artefacts de composants personnalisés depuis 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": "*"
        }
    ]
}
```

Création d'une passerelle SiteWise Edge

Vous pouvez utiliser la AWS IoT SiteWise console pour créer une passerelle SiteWise Edge. Cette procédure explique comment créer une passerelle SiteWise Edge auto-hébergée que vous installerez sur votre propre matériel. Pour plus d'informations sur la création d'une passerelle SiteWise Edge qui s'exécute sur Siemens Industrial Edge, consultezRunning SiteWise Edge sur Siemens Industrial Edge.

Création d'une passerelle SiteWise Edge

1. Accédez à la console AWS IoT SiteWise.
2. Dans le volet de navigation, choisissez Edge gateways.
3. Cliquez sur Create gateway (Créer une passerelle).
4. Pour Type de déploiement, choisissez Passerelle auto-hébergée.
5. Entrez un nom pour votre passerelle SiteWise Edge ou utilisez le nom généré par AWS IoT SiteWise.
6. Sous le système d'exploitation de l'appareil Greengrass, sélectionnez le système d'exploitation de l'appareil sur lequel vous allez installer cette passerelle SiteWise Edge.

   > **Note**
   >
   > Le pack de traitement des données n'est disponible que sur les plateformes x86.

7. (Facultatif) Pour traiter et organiser les données à la périphérie, sous Fonctionnalités de la périphérie, sélectionnez Data Processing Pack.

   > **Note**
   >
   > Pour autoriser les groupes d'utilisateurs de votre annuaire d'entreprise à accéder à cette passerelle SiteWise Edge, voir Configuration de la fonctionnalité Edge

8. (Facultatif) Dans la section Configuration avancée, procédez comme suit :

   - Pour l'appareil Greengrass Core, choisissez l'une des options suivantes :

     - Configuration par défaut : utilise AWS automatiquement les paramètres par défaut pour créer un appareil Greengrass Core dans. AWS IoT Greengrass V2

       1. Entrez un nom pour le périphérique principal de Greengrass ou utilisez le nom généré par. AWS IoT SiteWise

     - Configuration avancée — Choisissez cette option si vous souhaitez utiliser un appareil principal Greengrass existant ou en créer un manuellement.

       1. Choisissez un appareil Greengrass core ou choisissez Create Greengrass core device pour en créer un dans la console. AWS IoT Greengrass V2 Pour plus d'informations,

consultez la section Configuration des appareils AWS IoT Greengrass V2 principaux dans le Guide du AWS IoT Greengrass Version 2 développeur.

9. Cliquez sur Create gateway (Créer une passerelle).
10. Dans la boîte de dialogue Générer le programme d'installation de la passerelle SiteWise Edge, sélectionnez Générer et télécharger. AWS IoT SiteWise génère automatiquement un programme d'installation que vous pouvez utiliser pour configurer votre appareil local.

> **Important**
>
> Assurez-vous d'enregistrer le fichier d'installation dans un emplacement sécurisé. Vous utiliserez le fichier ultérieurement.

Maintenant que vous avez créé la passerelle SiteWise Edge, ajoutez des sources de données, configurez le composant éditeur et faites en sorte que votre passerelle SiteWise Edge reçoive des données et les envoie au AWS cloud.

Installation du logiciel de passerelle SiteWise Edge sur votre appareil local

Une fois que vous avez créé une passerelle SiteWise Edge, vous devez installer le logiciel de passerelle SiteWise Edge sur votre appareil local. SiteWise Le logiciel de passerelle Edge peut être installé sur des appareils locaux sur lesquels des systèmes d'exploitation serveur Linux ou Windows sont installés.

> **Important**
>
> Assurez-vous que votre appareil local est connecté à Internet.

Linux

La procédure suivante utilise SSH pour se connecter à votre appareil local. Vous pouvez également utiliser une clé USB ou d'autres outils pour transférer le fichier d'installation sur votre appareil local. Si vous ne souhaitez pas utiliser SSH, passez à l'étape 2 : Installation du logiciel de passerelle SiteWise Edge ci-dessous.

Prérequis SSH

Avant de vous connecter à votre appareil via SSH, remplissez les conditions préalables suivantes.

- Obtenez l'adresse IP de votre appareil.
- Obtenez le nom d'utilisateur pour vous connecter à votre appareil.
- Installez un client SSH sur votre ordinateur local selon vos besoins.

  Un client SSH peut être installé par défaut sur votre ordinateur local. Vous pouvez le vérifier en tapant ssh dans la ligne de commande. Si votre ordinateur ne reconnaît pas la commande, vous pouvez installer un client SSH pour vous connecter au nœud maître.

  - Linux et macOS : téléchargez et installez OpenSSH. Pour plus d'informations, consultez https://www.openssh.com.

Étape 1 : Copiez le programme d'installation sur votre périphérique de passerelle SiteWise Edge

Les instructions suivantes expliquent comment vous connecter à votre appareil local à l'aide d'un client SSH.

1. Pour vous connecter à votre appareil, exécutez la commande suivante dans une fenêtre de terminal de votre ordinateur, en remplaçant le *nom d'utilisateur* et l'*adresse IP* par un nom d'utilisateur doté de privilèges et d'une adresse IP élevés.

   ```
   ssh username@IP
   ```

2. Pour transférer le fichier d'installation AWS IoT SiteWise généré sur votre périphérique de passerelle SiteWise Edge, exécutez la commande suivante.

   > **Note**
   >
   > - Remplacez-le *path-to-saved-installer*par le chemin sur votre ordinateur que vous avez utilisé pour enregistrer le fichier d'installation et le nom du fichier d'installation.
   > - Remplacez *l'adresse IP* par l'adresse IP de votre appareil local.
   > - *directory-to-receive-installer*Remplacez-le par le chemin sur le périphérique local que vous utilisez pour recevoir le fichier d'installation.

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

Étape 2 : Installation du logiciel de passerelle SiteWise Edge

Dans les procédures suivantes, exécutez les commandes dans une fenêtre de terminal sur votre périphérique de passerelle SiteWise Edge.

1. Donnez au fichier d'installation l'autorisation d'exécution.

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

2. Exécutez le programme d'installation.

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

Windows server

Prérequis

Vous devez remplir les conditions préalables suivantes pour installer le logiciel de passerelle SiteWise Edge :

- Windows Server 2019 ou version ultérieure installé
- Privilèges d'administrateur
- PowerShell version 5.1 ou ultérieure installée
- SiteWise Le programme d'installation de la passerelle Edge a été téléchargé sur le serveur Windows où il sera provisionné

Étape 1 : Exécuter en PowerShell tant qu'administrateur

1. Sur le serveur Windows sur lequel vous souhaitez installer la passerelle SiteWise Edge, connectez-vous en tant qu'administrateur.
2. Entrez PowerShelldans la barre de recherche Windows.

3. Dans les résultats de recherche, ouvrez le menu contextuel (clic droit) de l' PowerShell application Windows. Choisissez Exécuter en tant qu'administrateur.

Étape 2 : Installation du logiciel de passerelle SiteWise Edge

Exécutez les commandes suivantes dans une fenêtre de terminal sur votre périphérique SiteWise Edge Gateway.

1. Débloquez le programme d'installation de la passerelle SiteWise Edge.

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

2. Lancez le programme d'installation.

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

> **Note**
>
> Si l'exécution du script est désactivée sur le système, remplacez la politique d'exécution du script par`RemoteSigned`.
>
> ```
> Set-ExecutionPolicy RemoteSigned
> ```

Permettre le traitement des données de pointe

Vous pouvez utiliser AWS IoT SiteWise Edge pour collecter, stocker, organiser et surveiller les données des équipements localement. Vous pouvez utiliser SiteWise Edge pour modéliser vos données industrielles et SiteWise Monitor pour créer des tableaux de bord permettant à votre personnel opérationnel de visualiser les données localement. Vous pouvez traiter vos données localement et les envoyer au AWS Cloud, ou les traiter sur site à l'aide de l' AWS IoT SiteWise API.

Avec AWS IoT SiteWise Edge, vous pouvez traiter les données brutes localement et choisir de n'envoyer que des données agrégées au AWS Cloud afin d'optimiser votre utilisation de la bande passante et les coûts de stockage dans le cloud.

> **Note**
>
> - AWS IoT SiteWise conserve vos données Edge sur vos passerelles SiteWise Edge jusqu'à 30 jours. La durée de conservation de vos données dépend de l'espace disque disponible sur votre appareil.
> - Si votre passerelle SiteWise Edge est déconnectée du AWS Cloud depuis 30 jours, le pack de traitement des données est automatiquement désactivé.

Configuration de la fonctionnalité Edge

AWS IoT SiteWise fournit les packs suivants que votre passerelle SiteWise Edge peut utiliser pour déterminer comment collecter et traiter vos données. Sélectionnez des packs pour activer les fonctionnalités Edge de votre passerelle SiteWise Edge.

- Le pack de collecte de données permet à votre passerelle SiteWise Edge de collecter des données à partir de plusieurs serveurs OPC-UA, puis d'exporter les données de la périphérie vers le. AWS Cloud Il devient actif une fois que vous avez ajouté des sources de données à votre passerelle SiteWise Edge.
- Le pack de traitement des données permet à votre passerelle SiteWise Edge de traiter les données de votre équipement à la périphérie. Par exemple, vous pouvez utiliser des modèles d'actifs pour calculer des métriques et des transformations. Pour plus d'informations sur les modèles d'actifs et les actifs, consultezModélisation des ressources industrielles.

> **Note**
>
> - Le pack de traitement des données n'est disponible que sur les plateformes x86.
> - Le pack de traitement des données ne prend pas en charge les proxys réseau.

Pour configurer les fonctionnalités Edge

1. Accédez à la console AWS IoT SiteWise.
2. Dans le volet de navigation, choisissez Edge gateways.
3. Sélectionnez la passerelle SiteWise Edge pour laquelle vous souhaitez activer les fonctionnalités Edge.

4. Dans la section Fonctionnalités Edge, choisissez Modifier
5. Dans la section Fonctionnalités Edge, sélectionnez Activer le pack de traitement des données (entraîne des frais supplémentaires).
6. (Facultatif) Dans la section Connexion LDAP Edge, vous pouvez autoriser les groupes d'utilisateurs de votre annuaire d'entreprise à accéder à cette passerelle SiteWise Edge. Les groupes d'utilisateurs peuvent utiliser les informations d'identification LDAP (Lightweight Directory Access Protocol) pour accéder à la passerelle SiteWise Edge. Ils peuvent ensuite utiliser l' AWS IoT SiteWise application AWS OpsHub for, les opérations d' AWS IoT SiteWise API ou d'autres outils pour gérer la passerelle SiteWise Edge. Pour plus d'informations, consultez Gestion des passerelles SiteWise Edge.

   > **Note**
   >
   > Vous pouvez également utiliser les informations d'identification Linux ou Windows pour accéder à la passerelle SiteWise Edge. Pour plus d'informations, consultez Accès à votre passerelle SiteWise Edge à l'aide des informations d'identification du système d'exploitation Linux.

   a. Sélectionnez Activé.
   b. Dans Nom du fournisseur, entrez le nom de votre fournisseur LDAP.
   c. Dans Nom d'hôte ou adresse IP, entrez le nom d'hôte ou l'adresse IP de votre serveur LDAP.
   d. Pour Port, entrez un numéro de port.
   e. Pour Nom distinctif de base (DN), entrez un nom distinctif (DN) pour la base.

      Les types d'attributs suivants sont pris en charge : CommonName (CN), LocalityName (L), Name (ST) stateOrProvince, OrganizationName (O), (OU), CountryName (C) organizationalUnitName , StreetAddress (STREET), DomainComponent (DC) et userid (UID).
   f. Pour le DN du groupe d'administrateurs, entrez un DN.
   g. Pour le DN du groupe d'utilisateurs, entrez un DN.
7. Choisissez Enregistrer.

Maintenant que vous avez activé les fonctionnalités Edge sur votre passerelle SiteWise Edge, vous devez configurer votre modèle d'actif pour la périphérie. La configuration périphérique de votre modèle d'actifs indique où les propriétés de vos actifs sont calculées. Vous pouvez calculer toutes les propriétés à la périphérie ou configurer les propriétés de votre modèle d'actifs séparément. Les propriétés du modèle d'actifs incluent les métriques, les transformations et les mesures.

Pour plus d'informations sur les propriétés des actifs, consultezthe section called "Définition des propriétés des données".

Après avoir créé votre modèle d'actif, vous pouvez le configurer pour la périphérie. Pour plus d'informations sur la configuration de votre modèle d'actif pour la périphérie, consultezthe section called "Création d'un modèle de ressource (console)".

> **Note**
>
> Les modèles d'actifs et les tableaux de bord sont automatiquement synchronisés entre la passerelle AWS Cloud et votre passerelle SiteWise Edge toutes les 10 minutes. Vous pouvez également effectuer une synchronisation manuelle à partir de l'application de passerelle SiteWise Edge locale.

Traitement des données à la périphérie

Vous devez configurer votre modèle d'actif pour la périphérie avant de pouvoir traiter les données de votre passerelle SiteWise Edge à la périphérie. La configuration périphérique de votre modèle d'actifs indique où les propriétés de vos actifs sont calculées. Vous pouvez choisir de calculer toutes les propriétés à la périphérie et d'envoyer les résultats au AWS Cloud, ou de personnaliser l'endroit où calculer chaque propriété d'actif séparément. Pour de plus amples informations, veuillez consulter Permettre le traitement des données de pointe.

Les propriétés des actifs incluent les métriques, les transformations et les mesures :

- Les métriques sont les données agrégées de l'actif sur une période donnée. Vous pouvez calculer de nouvelles mesures en utilisant les données métriques existantes. AWS IoT SiteWise envoie toujours vos indicateurs vers le AWS Cloud pour un stockage à long terme. AWS IoT SiteWise calcule les métriques sur le AWS Cloud par défaut. Vous pouvez configurer votre modèle d'actifs pour calculer vos indicateurs à la périphérie. AWS IoT SiteWise envoie les résultats traités vers le AWS Cloud.

- Les transformations sont des expressions mathématiques qui mappent les points de données d'une propriété de ressource à partir d'un formulaire vers un autre. Les transformations peuvent utiliser des métriques comme données d'entrée et doivent être calculées et stockées au même endroit que leurs entrées. Si vous configurez une entrée métrique pour qu'elle soit calculée à la périphérie, calcule AWS IoT SiteWise également la transformation associée à la périphérie.
- Les mesures sont formatées sous forme de données brutes que votre appareil collecte et envoie au AWS Cloud par défaut. Vous pouvez configurer votre modèle d'actif pour stocker ces données sur votre appareil local.

Pour plus d'informations sur les propriétés des actifs, consultezthe section called "Définition des propriétés des données".

Après avoir créé votre modèle d'actif, vous pouvez le configurer pour la périphérie. Pour plus d'informations sur la configuration de votre modèle d'actif pour la périphérie, consultezthe section called "Création d'un modèle de ressource (console)".

> **Note**
>
> Les modèles d'actifs et les tableaux de bord sont automatiquement synchronisés entre le AWS Cloud et votre passerelle SiteWise Edge toutes les 10 minutes. Vous pouvez également effectuer une synchronisation manuelle à partir duGestion des passerelles SiteWise Edge.

Vous pouvez utiliser les AWS IoT SiteWise API REST et le AWS Command Line Interface (AWS CLI) pour interroger votre passerelle SiteWise Edge pour obtenir des données en périphérie. Avant d'interroger votre passerelle SiteWise Edge pour obtenir des données en périphérie, vous devez remplir les conditions préalables suivantes :

- Vos informations d'identification doivent être définies pour les API REST. Pour plus d'informations sur la définition des informations d'identification, consultezthe section called "Gestion des passerelles SiteWise Edge".
- Le point de terminaison du SDK doit pointer vers l'adresse IP de votre passerelle SiteWise Edge. Vous trouverez de plus amples informations dans la documentation de votre SDK. Par exemple, consultez la section Spécification de points de terminaison personnalisés dans le guide du AWS SDK for Java 2.x développeur.
- Votre certificat de passerelle SiteWise Edge doit être enregistré. Vous trouverez plus d'informations sur l'enregistrement de votre certificat de passerelle SiteWise Edge dans la documentation de votre

SDK. Par exemple, consultez l'enregistrement des ensembles de certificats dans le fichier Node.js du guide du AWS SDK for Java 2.x développeur.

Pour plus d'informations sur l'interrogation de données avec AWS IoT SiteWise, consultezInterrogez les données de AWS IoT SiteWise.

Configuration du composant AWS IoT SiteWise Publisher

Après avoir créé une passerelle AWS IoT SiteWise Edge et installé le logiciel, configurez le composant Publisher afin que votre passerelle SiteWise Edge puisse exporter des données vers le AWS cloud. Pour plus d'informations, consultez AWS IoT SiteWise Publisher dans le guide du AWS IoT Greengrass Version 2 développeur.

Console

1. Accédez à la console AWS IoT SiteWise.
2. Dans le volet de navigation, choisissez Edge gateways.
3. Sélectionnez la passerelle SiteWise Edge pour laquelle vous souhaitez configurer l'éditeur.
4. Dans la section Configuration de l'éditeur, choisissez Modifier
5. Pour Ordre de publication, sélectionnez l'une des options suivantes :
   - Publier les données les plus anciennes en premier — La passerelle SiteWise Edge publie d'abord les données les plus anciennes dans le cloud par défaut.
   - Publiez d'abord les données les plus récentes : la passerelle SiteWise Edge publie d'abord les données les plus récentes dans le cloud.
6. (Facultatif) Si vous ne souhaitez pas que la passerelle SiteWise Edge compresse vos données, désélectionnez Activer la compression lors du téléchargement des données.
7. (Facultatif) Si vous ne souhaitez pas publier d'anciennes données, choisissez Exclure les données expirées et procédez comme suit :
   - Pour Période limite, entrez une valeur et choisissez une unité. La période limite doit être comprise entre cinq minutes et sept jours. Par exemple, si la période limite est de trois jours, les données datant de plus de trois jours ne sont pas publiées dans le cloud.
8. (Facultatif) Pour définir des paramètres personnalisés concernant le traitement des données sur votre appareil local, choisissez Paramètres de stockage local et procédez comme suit :

a. Pour Période de rétention, entrez un nombre et choisissez une unité. La période de conservation doit être comprise entre une minute et 30 jours, et être supérieure ou égale à la période de rotation. Par exemple, si la période de conservation est de 14 jours, la passerelle SiteWise Edge supprime toutes les données de la périphérie qui sont antérieures à la période limite spécifiée après les avoir stockées pendant 14 jours.

b. Pour Période de rotation, entrez un nombre et choisissez une unité. La période de rotation doit être supérieure à une minute et égale ou inférieure à la période de conservation. Par exemple, supposons que la période de rotation soit de deux jours, la passerelle SiteWise Edge regroupe et enregistre les données antérieures à la période limite dans un seul fichier. La passerelle SiteWise Edge transfère un lot de données vers le répertoire local suivant une fois tous les deux jours :`/greengrass/v2/work/aws.iot.SiteWiseEdgePublisher/exports`.

c. Pour Capacité de stockage, entrez une valeur supérieure ou égale à 1. Si la capacité de stockage est de 2 Go, la passerelle SiteWise Edge commence à supprimer les données lorsque plus de 2 Go de données sont stockées localement.

9. Choisissez Enregistrer.

AWS CLI

Vous pouvez utiliser l'UpdateGatewayCapabilityConfigurationAPI pour configurer l'éditeur. Définissez le paramètre `capabilityNamespace` sur `iotsitewise:publisher:2`.

L'éditeur fournit les paramètres de configuration suivants que vous pouvez personnaliser :

`SiteWisePublisherConfiguration`

`publishingOrder`

Ordre dans lequel les données sont publiées dans le cloud. La valeur de ce paramètre peut être l'une des suivantes :

- `TIME_ORDER`(Publiez d'abord les données les plus anciennes) — Les données les plus anciennes sont publiées dans le cloud en premier, par défaut.
- `RECENT_DATA`(Publiez d'abord les données les plus récentes) — Les données les plus récentes sont d'abord publiées dans le cloud.

`dropPolicy`

(Facultatif) Une politique qui contrôle les données publiées dans le cloud.

`cutoffAge`

Les données antérieures à la période limite ne sont pas publiées dans le cloud. L'âge limite doit être compris entre cinq minutes et sept jours.

Vous pouvez utiliser `m`, `h`, et `d` lorsque vous spécifiez un âge limite. Notez que cela `m` représente les minutes, `h` les heures et les `d` jours.

`exportPolicy`

(Facultatif) Une politique qui gère le stockage des données à la périphérie. Cette politique s'applique aux données antérieures à l'âge limite.

`retentionPeriod`

Votre passerelle SiteWise Edge supprime toutes les données de la périphérie antérieures à la période limite du stockage local une fois qu'elles ont été stockées pendant la période de conservation spécifiée. La période de conservation doit être comprise entre une minute et 30 jours, et être supérieure ou égale à la période de rotation.

Vous pouvez utiliser `m`, `h`, et `d` lorsque vous spécifiez une période de conservation. Notez que cela `m` représente les minutes, `h` les heures et les `d` jours.

`rotationPeriod`

Intervalle de temps pendant lequel les données antérieures à la période limite peuvent être regroupées et enregistrées dans un seul fichier. La passerelle SiteWise Edge transfère un lot de données vers le répertoire local suivant à la fin de chaque période de rotation :`/greengrass/v2/work/aws.iot.SiteWiseEdgePublisher/exports`. La période de rotation doit être supérieure à une minute et égale ou inférieure à la période de conservation.

Vous pouvez utiliser `m`, `h`, et `d` lorsque vous spécifiez une période de rotation. Notez que cela `m` représente les minutes, `h` les heures et les `d` jours.

`exportSizeLimitGB`

Taille maximale autorisée des données stockées localement, en Go. Si ce quota est dépassé, la passerelle SiteWise Edge commence à supprimer les données les plus anciennes jusqu'à ce que la taille des données stockées localement soit égale ou inférieure au quota. La valeur de ce paramètre doit être supérieure ou égale à 1.

Example configuration de l'éditeur :

L'espace de noms de l'éditeur : `iotsitewise:publisher:2`

```
{
"SiteWisePublisherConfiguration": {
    "publishingOrder": "TIME_ORDER",
    "dropPolicy": {
        "cutoffAge": "7d",
        "exportPolicy": {
            "retentionPeriod": "7d",
            "rotationPeriod": "6h",
            "exportLocation": "/greengrass/v2/work/aws.iot.SiteWiseEdgePublisher/
exports",
            "exportSizeLimitGB": 10
        }
    }
}
}
```

Configuration des sources de données

Après avoir configuré une passerelle AWS IoT SiteWise Edge, vous pouvez configurer des sources de données afin que votre passerelle SiteWise Edge puisse ingérer des données provenant d'équipements industriels locaux vers AWS IoT SiteWise. Chaque source représente un serveur local, tel qu'un serveur OPC-UA, auquel votre passerelle SiteWise Edge connecte et récupère les flux de données industriels. Pour plus d'informations sur la configuration d'une passerelle SiteWise Edge, consultezConfiguration d'une passerelle AWS IoT Greengrass V1 SiteWise Edge.

> **Note**
>
> AWS IoT SiteWise redémarre votre passerelle SiteWise Edge chaque fois que vous ajoutez ou modifiez une source. Votre passerelle SiteWise Edge n'ingère pas de données lors du redémarrage. Le délai de redémarrage de votre passerelle SiteWise Edge dépend du nombre de balises figurant sur les sources de votre passerelle SiteWise Edge. Le temps de redémarrage peut aller de quelques secondes (pour une passerelle SiteWise Edge avec peu de balises) à plusieurs minutes (pour une passerelle SiteWise Edge avec de nombreuses balises).

Après avoir créé les sources, vous pouvez associer vos flux de données aux propriétés des actifs. Pour plus d'informations sur la création et l'utilisation de ressources, reportez-vous aux sections Modélisation des ressources industrielles etMappage des flux de données industrielles avec des propriétés de ressources.

Vous pouvez consulter CloudWatch les métriques pour vérifier qu'une source de données est connectée à AWS IoT SiteWise. Pour plus d'informations, consultez AWS IoT Greengrass Version 2 métriques de passerelle.

Actuellement, AWS IoT SiteWise prend en charge les protocoles de source de données suivants :

- OPC-UA — Protocole de communication machine-to-machine (M2M) pour l'automatisation industrielle.

> **Note**
>
> SiteWise Les passerelles Edge exécutées AWS IoT Greengrass V2 actuellement ne prennent pas en charge les sources IP Modbus TCP et Ethernet.

Rubriques

- Configuration d'une source OPC-UA
- Configuration de l'authentification des sources de données
- Choix d'une destination pour les données de votre serveur source

Configuration d'une source OPC-UA

Vous pouvez utiliser la AWS IoT SiteWise console ou une fonctionnalité de passerelle SiteWise Edge pour définir et ajouter une source OPC-UA à votre passerelle SiteWise Edge afin de représenter un serveur OPC-UA local.

Rubriques

- Configuration d'une source OPC-UA (console)
- Configuration d'une source OPC-UA (CLI)
- Permettre à vos serveurs sources OPC-UA de faire confiance à la passerelle Edge SiteWise
- Filtrez les plages d'ingestion de données avec OPC-UA

- Utilisation des filtres de nœuds OPC-UA

Configuration d'une source OPC-UA (console)

Pour configurer une source OPC-UA à l'aide de la console AWS IoT SiteWise

1. Accédez à la console AWS IoT SiteWise.
2. Dans le volet de navigation, choisissez Passerelles.
3. Sélectionnez la passerelle SiteWise Edge pour ajouter une source OPC-UA.
4. Choisissez Add data source.
5. Entrez le nom de la source.
6. Entrez le point de terminaison local du serveur de source de données. Le point de terminaison peut être l'adresse IP ou le nom d'hôte. Vous pouvez également ajouter un numéro de port au point de terminaison local. Par exemple, votre point de terminaison local peut ressembler à ceci : **`opc.tcp://203.0.113.0:49320`**

   > **Note**
   >
   > Si votre passerelle SiteWise Edge est équipée `Deployment type` d'un appareil Siemens Industrial Edge neuf et que vous souhaitez ingérer des données provenant de l'application Edge OPC UA Server exécutée sur le même périphérique Siemens Industrial Edge que l'application AWS IoT SiteWise Edge, entrez. **`opc.tcp://ie-opcua:48010`**

7. (Facultatif) Pour l'ID de nœud à sélectionner, ajoutez des filtres de nœuds pour limiter les flux de données ingérés dans le AWS Cloud. Par défaut, les passerelles SiteWise Edge utilisent le nœud racine d'un serveur pour ingérer tous les flux de données. Vous pouvez utiliser des filtres de nœuds pour réduire le temps de démarrage et l'utilisation du processeur de votre passerelle SiteWise Edge en incluant uniquement les chemins d'accès aux données que vous modélisez AWS IoT SiteWise. Par défaut, les passerelles SiteWise Edge téléchargent tous les chemins OPC-UA à l'exception de ceux qui commencent par. `/Server/` Pour définir des filtres de nœud OPC-UA, vous pouvez utiliser les chemins de nœud ou les caractères génériques `*` et `**`. Pour plus d'informations, consultez Utilisation des filtres de nœuds OPC-UA.
8. Pour Destinations, choisissez la destination des données sources :

- AWS IoT SiteWise en temps réel — Choisissez cette option pour envoyer les données directement au AWS IoT SiteWise stockage. Ingérez et surveillez les données en temps réel, et traitez-les à la périphérie.
- AWS IoT SiteWise Mise en mémoire tampon à l'aide d'Amazon S3 : envoyez les données au format parquet vers Amazon S3, puis importez-les dans le AWS IoT SiteWise stockage. Choisissez cette option pour ingérer les données par lots et stocker les données historiques de manière rentable. Vous pouvez configurer l'emplacement de votre compartiment Amazon S3 préféré et la fréquence à laquelle vous souhaitez que les données soient chargées sur Amazon S3. Vous pouvez également choisir ce que vous souhaitez faire avec les données après leur ingestion dans AWS IoT SiteWise. Vous pouvez choisir que les données soient disponibles à la fois dans Amazon S3 SiteWise et dans Amazon S3 ou vous pouvez choisir de les supprimer automatiquement d'Amazon S3.
  - Le bucket Amazon S3 est un mécanisme de préparation et de mise en mémoire tampon qui prend en charge les fichiers au format parquet.
  - Si vous cochez la case Importer les données dans le AWS IoT SiteWise stockage, les données sont d'abord chargées dans Amazon S3, puis dans le AWS IoT SiteWise stockage.
    - Si vous cochez la case Supprimer les données d'Amazon S3, les données sont supprimées d'Amazon S3 après leur importation dans le SiteWise stockage.
    - Si vous décochez la case Supprimer les données d'Amazon S3, les données sont stockées à la fois dans Amazon S3 et dans le SiteWise stockage.
  - Si vous décochez la case Importer les données dans le AWS IoT SiteWise stockage, les données sont stockées uniquement dans Amazon S3. Il n'est pas importé dans le SiteWise stockage.

  Visitez Gestion du stockage des données pour plus de détails sur les différentes options de stockage AWS IoT SiteWise proposées. Pour en savoir plus sur les options de tarification, consultez la section AWS IoT SiteWise Tarification.
- AWS IoT Greengrass gestionnaire de flux — Utilisez le gestionnaire de AWS IoT Greengrass flux pour envoyer des données vers les AWS Cloud destinations suivantes : canaux AWS IoT Analytics entrants, flux dans Amazon Kinesis Data Streams, propriétés des actifs ou objets AWS IoT SiteWise dans Amazon Simple Storage Service (Amazon S3). Pour plus d'informations, consultez la section Gérer les flux de données sur le AWS IoT Greengrass Core dans le Guide AWS IoT Greengrass Version 2 du développeur.

  Entrez un nom pour le AWS IoT Greengrass flux.

Lors de la configuration d'une source de données, l'ID de nœud pour la sélection est utilisé pour déterminer la destination du flux de données.

- Si les mêmes données sont publiées à la fois AWS IoT SiteWise en temps réel et en AWS IoT SiteWise mémoire tampon à l'aide d'Amazon S3, vous devez ajouter deux sources de données qui publient sur les deux destinations.
- Pour diviser les données afin qu'une partie soit publiée AWS IoT SiteWise en temps réel et l'autre partie sur AWS IoT SiteWise Buffered à l'aide d'Amazon S3, vous devez filtrer les alias de données suivants :

```
/Alias01/Data1
/Alias02/Data1
/Alias03/Data1
/Alias03/Data2
```

Par exemple, vous pouvez ajouter une source de données pointant vers un filtre de `/**/Data1` nœuds, vers un filtre AWS IoT SiteWise en temps réel, et une autre source de données pointant vers une `/**/Data2` AWS IoT SiteWise mémoire tampon à l'aide d'Amazon S3

9. Dans le volet Configuration avancée, vous pouvez effectuer les opérations suivantes :

   a. Choisissez un mode de sécurité des messages pour les connexions et les données en transit entre votre serveur source et votre passerelle SiteWise Edge. Ce champ est la combinaison de la politique de sécurité OPC-UA et du mode de sécurité des messages. Choisissez la même politique de sécurité et le même mode de sécurité des messages que ceux que vous avez spécifiés pour votre serveur OPC-UA.

   b. Si votre source nécessite une authentification, choisissez un AWS Secrets Manager secret dans la liste de configuration de l'authentification. La passerelle SiteWise Edge utilise les informations d'authentification contenues dans ce secret lorsqu'elle se connecte à cette source de données. Vous devez associer des secrets au AWS IoT Greengrass composant de votre passerelle SiteWise Edge pour les utiliser pour l'authentification des sources de données. Pour plus d'informations, consultez the section called "Configuration de l'authentification des sources de données".

> **Tip**
>
> Votre serveur de données peut avoir une option nommée Autoriser la connexion anonyme. Si cette option est Oui, votre source n'a pas besoin d'authentification.

c. (Facultatif) Entrez un préfixe de flux de données. La passerelle SiteWise Edge ajoute ce préfixe à tous les flux de données provenant de cette source. Utilisez un préfixe de flux de données pour distinguer les flux de données portant le même nom mais provenant de sources différentes. Chaque flux de données doit avoir un nom unique dans votre compte.

d. (Facultatif) Pour les groupes de propriétés, choisissez Ajouter un nouveau groupe.

   i. Entrez un nom pour le groupe de propriétés.

   ii. Pour les propriétés :

      1. Pour les chemins de nœud, ajoutez des filtres de nœuds OPC-UA pour limiter les chemins OPC-UA vers lesquels le téléchargement est effectué. AWS IoT SiteWise Le format est similaire à celui de l'ID de nœud pour la sélection.

   iii. Pour les paramètres de groupe, procédez comme suit :

      1. Pour le paramètre de qualité des données, choisissez le type de qualité de données que AWS IoT SiteWise Collector doit ingérer.
      2. Pour le réglage du mode Scan, configurez les propriétés d'abonnement standard suivantes :
         - Pour le mode de numérisation, choisissez l'une des options suivantes : Pour plus d'informations sur le mode de numérisation, consultezthe section called “Filtrer les plages d'ingestion de données avec OPC-UA”.
            - Pour envoyer chaque point de données, choisissez Subscribe et définissez les paramètres suivants :
               - Déclencheur de modification des données : condition qui déclenche une alerte de modification des données.
               - Taille de la file d'attente d'abonnement : profondeur de la file d'attente sur un serveur OPC-UA pour une métrique particulière dans laquelle les notifications relatives aux éléments surveillés sont mises en file d'attente.
               - Intervalle de publication par abonnement : intervalle (en millisecondes) du cycle de publication spécifié lors de la création de l'abonnement.

- Intervalle entre les instantanés : paramètre de délai d'expiration de la fréquence des instantanés pour garantir qu' AWS IoT SiteWise Edge ingère un flux constant de données.
- Fréquence de numérisation : fréquence à laquelle vous souhaitez que la passerelle SiteWise Edge lise vos registres. AWS IoT SiteWise calcule automatiquement le taux de numérisation minimum autorisé pour votre passerelle SiteWise Edge.

- Pour envoyer des points de données à un intervalle spécifique, choisissez Poll et entrez une fréquence de numérisation.

3. Si vous choisissez le mode Scan de Subscribe, configurez un type Deadband et les paramètres associés pour votre source. Cela permet de contrôler les données que votre AWS IoT SiteWise source vous envoie et celles qu'elle supprime. Pour plus d'informations sur le paramètre Deadband, consultezthe section called “Filtrer les plages d'ingestion de données avec OPC-UA”.

10. Choisissez Enregistrer.

Configuration d'une source OPC-UA (CLI)

Vous pouvez définir des sources de données OPC-UA pour une passerelle SiteWise Edge à l'aide du. AWS CLI Pour ce faire, créez un fichier JSON de configuration des fonctionnalités OPC-UA et utilisez la update-gateway-capability-configurationcommande pour mettre à jour la configuration de la passerelle SiteWise Edge. Vous devez définir toutes vos sources OPC-UA dans une configuration de capacité unique.

Cette fonctionnalité possède l'espace de noms suivant.

- `iotsitewise:opcuacollector:2`

Syntaxe de demande

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

```
          "certificateBody": "string",
          "certificateChain": "string",
        },
        "endpointUri": "string",
        "securityPolicy": "NONE" | "BASIC128_RSA15" | "BASIC256" | "BASIC256_SHA256" |
 "AES128_SHA256_RSAOAEP" | "AES256_SHA256_RSAPSS",
        "messageSecurityMode": "NONE" | "SIGN" | "SIGN_AND_ENCRYPT",
        "identityProvider": {
          "type": "Anonymous" | "Username",
          "usernameSecretArn": "string"
        },
        "nodeFilterRules": [
          {
            "action": "INCLUDE",
            "definition": {
              "type": "OpcUaRootPath",
              "rootPath": "string"
            }
          }
        ]
      },
      "measurementDataStreamPrefix": "string"
    "destination": {
        "type": "StreamManager",
        "streamName": "string",
        "streamBufferSize": integer
      },
      "propertyGroups": [
        {
          "name": "string",
          "nodeFilterRuleDefinitions": [
            {
              "type": "OpcUaRootPath",
              "rootPath": "string"
            }
          ],
          "deadband": {
            "type": "PERCENT" | "ABSOLUTE",
            "value": double,
            "eguMin": double,
            "eguMax": double,
            "timeoutMilliseconds": integer
          },
          "scanMode": {
```

```
            "type": "EXCEPTION" | "POLL",
            "rate": integer
          },
          "dataQuality": {
            "allowGoodQuality": true | false,
            "allowBadQuality": true | false,
            "allowUncertainQuality": true | false
          },
          "subscription": {
            "dataChangeTrigger": "STATUS" | "STATUS_VALUE" | "STATUS_VALUE_TIMESTAMP",
            "queueSize": integer,
            "publishingIntervalMilliseconds": integer,
            "snapshotFrequencyMilliseconds": integer
          }
        }
      ]
    }
  ]
}
```

Corps de la demande

sources

Liste des structures de définition de source OPC-UA contenant chacune les informations suivantes :

nom

Nom unique et convivial pour la source.

point de terminaison

Structure de point de terminaison contenant les informations suivantes :

Certificat Trust

Structure de stratégie d'approbation de certificat contenant les informations suivantes :

type

Mode d'approbation de certificat pour la source. Sélectionnez l'une des méthodes suivantes :

- **`TrustAny`**— La passerelle SiteWise Edge fait confiance à n'importe quel certificat lorsqu'elle se connecte à la source OPC-UA.

- `X509`— La passerelle SiteWise Edge fait confiance à un certificat X.509 lorsqu'elle se connecte à la source OPC-UA. Si vous choisissez cette option, vous devez définir `certificateBody` dans `certificateTrust`. Vous pouvez également définir `certificateChain` dans `certificateTrust`.

Organisme de certification

(Facultatif) Corps d'un certificat X.509.

Ce champ est obligatoire si vous choisissez `X509` pour `type` dans `certificateTrust`.

CertificateChain

(Facultatif) Chaîne de confiance pour un certificat X.509.

Ce champ n'est utilisé que si vous choisissez `X509` pour `type` dans `certificateTrust`.

URI du point de terminaison

Point de terminaison local de la source OPC-UA. Par exemple, votre point de terminaison local peut ressembler à `opc.tcp://203.0.113.0:49320`.

Politique de sécurité

Politique de sécurité à utiliser pour sécuriser les messages lus depuis la source OPC-UA. Sélectionnez l'une des méthodes suivantes :

- `NONE`— La passerelle SiteWise Edge ne sécurise pas les messages provenant de la source OPC-UA. Nous vous recommandons de choisir une autre politique de sécurité. Si vous choisissez cette option, vous devez également choisir `NONE` pour `messageSecurityMode`.
- `BASIC256_SHA256`— La politique `Basic256Sha256` de sécurité.
- `AES128_SHA256_RSAOAEP`— La politique `Aes128_Sha256_RsaOaep` de sécurité.
- `AES256_SHA256_RSAPSS`— La politique `Aes256_Sha256_RsaPss` de sécurité.
- `BASIC128_RSA15`— (Obsolète) La politique de `Basic128Rsa15` sécurité est déconseillée dans la spécification OPC-UA car elle n'est plus considérée comme sécurisée. Nous vous recommandons de choisir une autre politique de sécurité. Pour plus d'informations, consultez Basic128Rsa15.
- `BASIC256`— (Obsolète) La politique de `Basic256` sécurité est déconseillée dans la spécification OPC-UA car elle n'est plus considérée comme sécurisée. Nous vous

recommandons de choisir une autre politique de sécurité. Pour plus d'informations, consultez Basic256.

> **Important**
>
> Si vous choisissez une politique de sécurité autre que`NONE`, vous devez choisir `SIGN` ou `SIGN_AND_ENCRYPT` pour`messageSecurityMode`. Vous devez également configurer votre serveur source pour qu'il fasse confiance à la passerelle SiteWise Edge. Pour plus d'informations, consultez Permettre à vos serveurs sources OPC-UA de faire confiance à la passerelle Edge SiteWise .

message SecurityMode

Mode de sécurité des messages à utiliser pour sécuriser les connexions à la source OPC-UA. Sélectionnez l'une des méthodes suivantes :

- `NONE`— La passerelle SiteWise Edge ne sécurise pas les connexions à la source OPC-UA. Nous vous recommandons de choisir un autre mode de sécurité des messages. Si vous choisissez cette option, vous devez également choisir `NONE` pour `securityPolicy`.
- `SIGN`— Les données en transit entre la passerelle SiteWise Edge et la source OPC-UA sont signées mais pas chiffrées.
- `SIGN_AND_ENCRYPT`— Les données en transit entre la passerelle et la source OPC-UA sont signées et cryptées.

> **Important**
>
> Si vous choisissez un mode de sécurité des messages autre que`NONE`, vous devez en choisir un `securityPolicy` autre que`NONE`. Vous devez également configurer votre serveur source pour qu'il fasse confiance à la passerelle SiteWise Edge. Pour plus d'informations, consultez Permettre à vos serveurs sources OPC-UA de faire confiance à la passerelle Edge SiteWise .

Fournisseur d'identité

Structure de fournisseur d'identité contenant les informations suivantes :

type

Type d'informations d'identification d'authentification requises par la source. Sélectionnez l'une des méthodes suivantes :

- `Anonymous`— La source n'a pas besoin d'authentification pour se connecter.
- `Username`— La source a besoin d'un nom d'utilisateur et d'un mot de passe pour se connecter. Si vous choisissez cette option, vous devez définir `usernameSecretArn` dans `identityProvider`.

nom d'utilisateur SecretArn

(Facultatif) L'ARN d'un AWS Secrets Manager secret. La passerelle SiteWise Edge utilise les informations d'authentification contenues dans ce secret lorsqu'elle se connecte à cette source. Vous devez associer des secrets au SiteWise connecteur IoT de votre passerelle SiteWise Edge pour les utiliser à des fins d'authentification à la source. Pour plus d'informations, consultez Configuration de l'authentification des sources de données.

Ce champ est obligatoire si vous choisissez `Username` pour `type` dans `identityProvider`.

nœud FilterRules

Liste des structures de règles de filtrage des nœuds qui définissent les chemins de flux de données OPC-UA à envoyer vers le AWS cloud. Vous pouvez utiliser des filtres de nœuds pour réduire le temps de démarrage et l'utilisation du processeur de votre passerelle SiteWise Edge en incluant uniquement les chemins d'accès aux données que vous modélisez AWS IoT SiteWise. Par défaut, les passerelles SiteWise Edge téléchargent tous les chemins OPC-UA à l'exception de ceux qui commencent par. `/Server/` Pour définir des filtres de nœud OPC-UA, vous pouvez utiliser les chemins de nœud ou les caractères génériques `*` et `**`. Pour plus d'informations, consultez Utilisation des filtres de nœuds OPC-UA.

Chaque structure de la liste doit contenir les informations suivantes :

action

Action pour cette règle de filtrage de nœud. Vous pouvez choisir les options suivantes :

- `INCLUDE`— La passerelle SiteWise Edge inclut uniquement les flux de données qui répondent à cette règle.

définition

Structure de règles de filtrage de nœud contenant les informations suivantes :

type

Type de chemin de filtre de nœud pour cette règle. Vous pouvez choisir les options suivantes :

- `OpcUaRootPath`— La passerelle SiteWise Edge évalue ce chemin de filtre de nœuds par rapport à la racine de la hiérarchie des chemins OPC-UA.

Trajectoire racine

Chemin du filtre de nœud à évaluer par rapport à la racine de la hiérarchie des chemins OPC-UA. Ce chemin doit commencer par`/`.

DataStreamPréfixe de mesure

Chaîne à ajouter à tous les flux de données provenant de la source. La passerelle SiteWise Edge ajoute ce préfixe à tous les flux de données provenant de cette source. Utilisez un préfixe de flux de données pour distinguer les flux de données portant le même nom mais provenant de sources différentes. Chaque flux de données doit avoir un nom unique dans votre compte.

Groupes de propriétés

(Facultatif) La liste des groupes de propriétés qui définissent `deadband` et `scanMode` demandés par le protocole.

nom

Nom du groupe de propriétés. Il doit s'agir d'un identifiant unique.

bandeau

`deadband`Structure qui contient les informations suivantes :

type

Les types de deadband pris en charge. Les valeurs acceptées sont `ABSOLUTE` et`PERCENT`.

valeur

La valeur du deadband. Dans ce cas `type`ABSOLUTE, cette valeur est un double sans unité. Dans ce cas `type`PERCENT, cette valeur est un double compris entre `1` et`100`.

Gumin

(Facultatif) L'unité d'ingénierie minimale lors de l'utilisation d'une `PERCENT` zone morte. Vous définissez ce paramètre si aucune unité d'ingénierie n'est configurée sur le serveur OPC-UA.

EGUmax

(Facultatif) L'unité d'ingénierie maximale lors de l'utilisation d'une `PERCENT` zone morte. Vous définissez ce paramètre si aucune unité d'ingénierie n'est configurée sur le serveur OPC-UA.

Délai d'expiration en millisecondes

Durée en millisecondes avant le délai d'expiration. Le minimum est`100`.

Mode de numérisation

`scanMode`Structure qui contient les informations suivantes :

type

Les types pris en charge de`scanMode`. Les valeurs acceptées sont `POLL` et`EXCEPTION`.

taux

Intervalle d'échantillonnage pour le mode de numérisation.

FilterRuleDéfinitions des nœuds

(Facultatif) Liste des chemins de nœuds à inclure dans le groupe de propriétés. Les groupes de propriétés ne peuvent pas se chevaucher. Si vous ne spécifiez aucune valeur pour ce champ, le groupe contient tous les chemins situés sous la racine et vous ne pouvez pas créer de groupes de propriétés supplémentaires. La structure `nodeFilterRuleDefinitions` contient les informations suivantes :

type

`OpcUaRootPath`est le seul type pris en charge. Cela indique que la valeur de `rootPath` est un chemin relatif à la racine de l'espace de navigation OPC-UA.

Trajectoire racine

Liste séparée par des virgules qui indique les chemins (relatifs à la racine) à inclure dans le groupe de propriétés.

Exemples de configuration des capacités

L'exemple suivant définit une configuration de fonctionnalité de passerelle OPC-UA SiteWise Edge à partir d'une charge utile stockée dans un fichier JSON.

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

Example : configuration de la source OPC-UA

Le `opc-ua-configuration.json` fichier suivant définit une configuration de source OPC-UA de base non sécurisée.

```
{
    "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 : configuration de source OPC-UA avec groupes de propriétés définis

Le `opc-ua-configuration.json` fichier suivant définit une configuration de source OPC-UA de base non sécurisée avec des groupes de propriétés définis.

```
{
    "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 : configuration de la source OPC-UA avec propriétés

L'exemple JSON suivant pour `opc-ua-configuration.json` définit une configuration source OPC-UA avec les propriétés suivantes :

- Faire confiance à n'importe quel certificat.
- Utilise la politique de `BASIC256` sécurité pour sécuriser les messages.
- Utilise le mode `SIGN_AND_ENCRYPT` pour sécuriser les connexions.
- Utilise les informations d'authentification stockées dans un secret de Secrets Manager.

- Filtre les flux de données sauf ceux dont le chemin commence par `/WindFarm/2/WindTurbine/`.
- Ajoute `/Washington` au début de chaque chemin de flux de données pour distinguer ce « parc éolien #2 » et un « parc éolien #2 » dans une autre zone.

```
{
    "sources": [
        {
            "name": "Wind Farm #2",
            "endpoint": {
                "certificateTrust": {
                    "type": "TrustAny"
                },
                "endpointUri": "opc.tcp://203.0.113.1:49320",
                "securityPolicy": "BASIC256",
                "messageSecurityMode": "SIGN_AND_ENCRYPT",
                "identityProvider": {
                    "type": "Username",
                    "usernameSecretArn":
 "arn:aws:secretsmanager:region:123456789012:secret:greengrass-windfarm2-auth-1ABCDE"
                },
                "nodeFilterRules": [
                  {
                      "action": "INCLUDE",
                      "definition": {
                          "type": "OpcUaRootPath",
                          "rootPath": "/WindFarm/2/WindTurbine/"
                    }
                  }
                ]
            },
            "measurementDataStreamPrefix": "/Washington"
        }
    ]
}
```

Example : configuration de source OPC-UA avec certificat de confiance

L'exemple JSON suivant pour `opc-ua-configuration.json` définit une configuration source OPC-UA avec les propriétés suivantes :

- Approuve un certificat X.509 donné.
- Utilise la politique de `BASIC256` sécurité pour sécuriser les messages.
- Utilise le mode `SIGN_AND_ENCRYPT` pour sécuriser les connexions.

```
{
    "sources": [
        {
            "name": "Wind Farm #3",
            "endpoint": {
                "certificateTrust": {
                    "type": "X509",
                    "certificateBody": "-----BEGIN CERTIFICATE-----
          MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w
 0BAQUFADCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZ
 WF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIw
 EAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5
 jb20wHhcNMTEwNDI1MjA0NTIxWhcNMTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBh
 MCVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBb
 WF6b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMx
 HzAdBgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wgZ8wDQYJKoZIhvcNAQE
 BBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ21uUSfwfEvySWtC2XADZ4nB+BLYgVI
 k60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9TrDHudUZg3qX4waLG5M43q7Wgc/MbQ
 ITxOUSQv7c7ugFFDzQGBzZswY6786m86gpEIbb3OhjZnzcvQAaRHhdlQWIMm2nr
 AgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4nUhVVxYUntneD9+h8Mg9q6q+auN
 KyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0FkbFFBjvSfpJIlJ00zbhNYS5f6Guo
 EDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTbNYiytVbZPQUQ5Yaxu2jXnimvw
 3rrszlaEXAMPLE=
          -----END CERTIFICATE-----",
                    "certificateChain": "-----BEGIN CERTIFICATE-----
          MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w
 0BAQUFADCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZ
 WF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIw
 EAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5
 jb20wHhcNMTEwNDI1MjA0NTIxWhcNMTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBh
 MCVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBb
 WF6b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMx
 HzAdBgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wgZ8wDQYJKoZIhvcNAQE
 BBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ21uUSfwfEvySWtC2XADZ4nB+BLYgVI
 k60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9TrDHudUZg3qX4waLG5M43q7Wgc/MbQ
 ITxOUSQv7c7ugFFDzQGBzZswY6786m86gpEIbb3OhjZnzcvQAaRHhdlQWIMm2nr
 AgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4nUhVVxYUntneD9+h8Mg9q6q+auN
 KyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0FkbFFBjvSfpJIlJ00zbhNYS5f6Guo
```

```
 EDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTbNYiytVbZPQUQ5Yaxu2jXnimvw
 3rrszlaEXAMPLE=
          -----END CERTIFICATE-----"
                },
                "endpointUri": "opc.tcp://203.0.113.2:49320",
                "securityPolicy": "BASIC256",
                "messageSecurityMode": "SIGN_AND_ENCRYPT",
                "identityProvider": {
                    "type": "Anonymous"
                },
                "nodeFilterRules": []
              },
            "measurementDataStreamPrefix": ""

        }
    ]
}
```

Permettre à vos serveurs sources OPC-UA de faire confiance à la passerelle Edge SiteWise

Si vous choisissez une valeur `messageSecurityMode` autre que None lors de la configuration de votre source OPC-UA, vous devez permettre à vos serveurs source de faire confiance à la passerelle AWS IoT SiteWise Edge. La passerelle SiteWise Edge génère un certificat dont votre serveur source peut avoir besoin. Le processus varie en fonction de vos serveurs sources. Pour plus d'informations, consultez la documentation de vos serveurs.

La procédure suivante décrit les étapes de base.

Pour permettre à un serveur OPC-UA de faire confiance à la passerelle Edge SiteWise

1. Ouvrez l'interface de configuration de votre serveur OPC-UA.
2. Entrez le nom d'utilisateur et le mot de passe de l'administrateur du serveur OPC-UA.
3. Localisez Clients de confiance dans l'interface, puis choisissez Client de passerelle AWS IoT SiteWise .
4. Choisissez Trust (Approuver).

Exportation du certificat client OPC-UA

Certains serveurs OPC-UA ont besoin d'accéder au fichier de certificat client OPC-UA pour faire confiance à la passerelle Edge. SiteWise Si cela s'applique à vos serveurs OPC-UA, vous pouvez utiliser la procédure suivante pour exporter le certificat client OPC-UA depuis la passerelle Edge. SiteWise Ensuite, vous pouvez importer le certificat sur votre serveur OPC-UA.

Pour exporter le fichier de certificat client OPC-UA pour une source

1. Exécutez la commande suivante pour passer au répertoire contenant le fichier de certificat. *Remplacez sitewise-work par le chemin de stockage local pour le fichier aws.iot. SiteWiseEdgeCollectorOpcua* le dossier de travail Greengrass et remplacez *source-name par le nom* de la source de données.

   Par défaut, le dossier de travail Greengrass est /greengrass/v2/work/aws.iot. SiteWiseEdgeCollectorOpcua sous Linux et *C : /greengrass/v2/work/aws.iot. SiteWiseEdgeCollectorOpcua sous Windows*.

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

2. Le certificat client OPC-UA de la passerelle SiteWise Edge pour cette source se trouve dans le `aws-iot-opcua-client.pfx` fichier.

   Exécutez la commande suivante pour exporter le certificat vers un fichier `.pem` appelé `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. Transférez le fichier de `aws-iot-opcua-client-certificate.pem` certificat de la passerelle SiteWise Edge vers le serveur OPC-UA.

   Pour ce faire, vous pouvez utiliser un logiciel commun tel que le programme `scp` pour transférer le fichier en utilisant le protocole SSH. Pour de plus amples informations, veuillez consulter Copie sécurisée sur Wikipédia.

> **Note**
>
> Si votre passerelle SiteWise Edge s'exécute sur Amazon Elastic Compute Cloud (Amazon EC2) et que vous vous y connectez pour la première fois, vous devez configurer les conditions requises pour vous connecter. Pour plus d'informations, consultez Connect to your Linux instance dans le guide de l'utilisateur Amazon EC2.

4. Importez le fichier de certificat sur `aws-iot-opcua-client-certificate.pem` le serveur OPC-UA pour faire confiance à la passerelle SiteWise Edge. Les étapes varient en fonction du serveur source que vous utilisez. Consultez la documentation de votre serveur.

Filtrez les plages d'ingestion de données avec OPC-UA

Vous pouvez contrôler la façon dont vous ingérez les données avec une source OPC-UA en utilisant le mode scan et les plages de zones mortes. Ces fonctionnalités vous permettent de contrôler le type de données à ingérer, ainsi que la manière et le moment où votre serveur et la passerelle SiteWise Edge échangent ces informations.

Collectez ou filtrez les données en fonction de leur qualité

Vous pouvez configurer vos paramètres de qualité des données pour contrôler les données collectées à partir de la source OPC-UA. La source de données inclut l'évaluation de qualité sous forme de métadonnées lorsqu'elle l'envoie. Vous pouvez sélectionner l'une ou l'ensemble des options suivantes :

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

Contrôlez la fréquence de collecte des données avec le mode Scan

Vous pouvez configurer votre mode de numérisation OPC-UA pour contrôler la manière dont vous collectez les données à partir de votre source OPC-UA. Vous pouvez choisir le mode abonnement ou le mode sondage.

- Mode d'abonnement — La source OPC-UA collecte des données à envoyer à votre passerelle SiteWise Edge à la fréquence définie par votre taux de numérisation. Le serveur envoie des

données uniquement lorsque la valeur a changé. Il s'agit donc de la fréquence maximale à laquelle votre passerelle SiteWise Edge reçoit des données.

- Mode d'interrogation : votre passerelle SiteWise Edge interroge la source OPC-UA à une fréquence définie en fonction de votre fréquence de numérisation. Le serveur envoie des données, que la valeur ait changé ou non, de sorte que votre passerelle SiteWise Edge reçoit toujours les données à cet intervalle.

> **Note**
>
> L'option du mode de sondage remplace vos paramètres de zone morte pour cette source.

Filtrez l'ingestion de données OPC-UA avec des plages mortes

Vous pouvez appliquer une zone morte à vos groupes de propriétés sources OPC-UA afin de filtrer et de supprimer certaines données au lieu de les envoyer vers le Cloud. AWS Une zone morte indique une fenêtre de fluctuations attendues des valeurs de données entrantes provenant de votre source OPC-UA. Si les valeurs se trouvent dans cette fenêtre, votre serveur OPC-UA ne les enverra pas au AWS Cloud. Vous pouvez utiliser le filtrage en zone morte pour réduire la quantité de données que vous traitez et envoyez vers le AWS cloud. Pour savoir comment configurer des sources OPC-UA pour votre passerelle SiteWise Edge, consultez. the section called “Configuration des sources de données”

> **Note**
>
> Votre serveur supprime toutes les données qui se trouvent dans la fenêtre spécifiée par votre deadband. Vous ne pouvez pas récupérer ces données supprimées.

Types de deadbands

Vous pouvez spécifier deux types de zones mortes pour le groupe de propriétés de votre serveur OPC-UA. Ils vous permettent de choisir la quantité de données à envoyer AWS vers le cloud et celle à supprimer.

- Pourcentage : vous spécifiez une fenêtre en utilisant un pourcentage de fluctuation attendue de la valeur de mesure. Le serveur calcule la fenêtre exacte à partir de ce pourcentage et envoie au AWS Cloud les données qui dépassent les limites de la fenêtre. Par exemple, la spécification

d'une valeur de zone morte de 2 % sur un capteur dans une plage comprise entre -100 degrés Fahrenheit et +100 degrés Fahrenheit indique au serveur d'envoyer des données vers le AWS cloud lorsque la valeur change de 4 degrés Fahrenheit ou plus.

> **Note**
>
> Vous pouvez éventuellement spécifier une valeur de bande morte minimale et maximale pour cette fenêtre si votre serveur source ne définit pas d'unités d'ingénierie. Si aucune plage d'unités d'ingénierie n'est fournie, le serveur OPC-UA utilise par défaut la plage complète du type de données de mesure.

- Absolu — Vous spécifiez une fenêtre en utilisant des unités exactes. Par exemple, la spécification d'une valeur de zone morte de 2 sur un capteur indique au serveur d'envoyer des données au AWS Cloud lorsque sa valeur change d'au moins 2 unités. Vous pouvez utiliser le deadbanding absolu pour les environnements dynamiques dans lesquels des fluctuations sont régulièrement attendues pendant les opérations normales.

Délais d'expiration de la bande morte

Vous pouvez éventuellement configurer un paramètre de délai d'expiration en zone morte. Après ce délai, le serveur OPC-UA envoie la valeur de mesure actuelle même si elle se situe dans les limites de la fluctuation de bande morte attendue. Vous pouvez utiliser le paramètre de temporisation pour garantir AWS IoT SiteWise l'ingestion d'un flux constant de données à tout moment, même lorsque les valeurs ne dépassent pas la fenêtre de zone morte définie.

Utilisation des filtres de nœuds OPC-UA

Lorsque vous définissez des sources de données OPC-UA pour une passerelle SiteWise Edge, vous pouvez définir des filtres de nœuds. Les filtres de nœuds vous permettent de limiter les chemins de flux de données que la passerelle SiteWise Edge envoie vers le cloud. Vous pouvez utiliser des filtres de nœuds pour réduire le temps de démarrage et l'utilisation du processeur de votre passerelle SiteWise Edge en incluant uniquement les chemins d'accès aux données que vous modélisez AWS IoT SiteWise. Par défaut, les passerelles SiteWise Edge téléchargent tous les chemins OPC-UA à l'exception de ceux qui commencent par. `/Server/` Vous pouvez utiliser les caractères génériques * et ** dans vos filtres de nœuds pour inclure plusieurs chemins de flux de données avec un seul filtre. Pour savoir comment configurer des sources OPC-UA pour votre passerelle SiteWise Edge, consultez. Configuration des sources de données

> **Note**
>
> AWS IoT SiteWise redémarre votre passerelle SiteWise Edge chaque fois que vous ajoutez ou modifiez une source. Votre passerelle SiteWise Edge n'ingère pas de données lors du redémarrage. Le délai de redémarrage de votre passerelle SiteWise Edge dépend du nombre de balises figurant sur les sources de votre passerelle SiteWise Edge. Le temps de redémarrage peut aller de quelques secondes (pour une passerelle SiteWise Edge avec peu de balises) à plusieurs minutes (pour une passerelle SiteWise Edge avec de nombreuses balises).

Le tableau suivant répertorie les caractères génériques que vous pouvez utiliser pour filtrer les sources de données OPC-UA.

Caractères génériques des filtres de nœuds OPC-UA

Caractère générique	Description
*	Correspond à un niveau unique dans un chemin de flux de données.
**	Correspond à plusieurs niveaux dans un chemin de flux de données.

> **Note**
>
> Si vous configurez une source avec un filtre large, puis que vous modifiez ultérieurement la source pour utiliser un filtre plus restrictif, AWS IoT SiteWise arrête de stocker les données qui ne correspondent pas au nouveau filtre.

Example Exemple de scénario utilisant des filtres de nœuds

Considérons les flux de données hypothétiques suivants :

- `/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`

À l'aide des flux de données précédents, vous pouvez définir des filtres de nœuds pour limiter les données à inclure à partir de votre source OPC-UA.

- Pour sélectionner tous les nœuds dans cet exemple, utilisez `/` ou`/**/`. Vous pouvez inclure plusieurs répertoires ou dossiers avec les caractères génériques « `**` ».
- Pour sélectionner tous les flux de données `PLC`, utilisez `/*/*/*/PLC*` ou `/**/PLC*`.
- Pour sélectionner tous les compteurs dans cet exemple, utilisez `/**/Counter*` ou`/*/*/*/Counter*`.
- Pour sélectionner tous les compteurs à partir de `Line 2`, utilisez `/**/Line 2/Counter*`.

Configuration de l'authentification des sources de données

Si votre serveur OPC-UA nécessite des informations d'authentification pour se connecter, vous pouvez les utiliser AWS Secrets Manager pour créer et déployer un secret sur votre passerelle SiteWise Edge. AWS Secrets Manager chiffre les secrets sur l'appareil pour protéger votre nom d'utilisateur et votre mot de passe jusqu'à ce que vous ayez besoin de les utiliser. Pour plus d'informations sur le composant du gestionnaire de AWS IoT Greengrass secrets, consultez la section Gestionnaire de secrets dans le guide du AWS IoT Greengrass Version 2 développeur.

Pour plus d'informations sur la gestion de l'accès aux secrets de Secrets Manager, rendez-vous sur :

- Qui est autorisé à accéder à vos AWS Secrets Manager secrets.
- Déterminer si une demande est autorisée ou refusée dans un compte.

Étape 1 : créer des secrets d'authentification à la source

Vous pouvez l'utiliser AWS Secrets Manager pour créer un secret d'authentification pour votre source de données. Dans le secret, définissez **`username`** des paires **`password`** clé-valeur contenant les détails d'authentification de votre source de données.

Pour créer des secrets (console)

1. Accédez à la console AWS Secrets Manager.
2. Choisissez Store a new secret (Stocker un nouveau secret).
3. Sous Type de secret, sélectionnez Autre type de secret.
4. Sous Paires clé/valeur, procédez comme suit :
    1. Dans la première zone de saisie, entrez **`username`** le nom d'utilisateur dans la deuxième zone de saisie.
    2. Choisissez Add row (Ajouter une ligne).
    3. Dans la première zone de saisie, entrez **`password`** le mot de passe dans la deuxième zone de saisie.
5. Pour Clé de chiffrement, sélectionnez aws/secretsmanager, puis Next.
6. Sur la page Enregistrer un nouveau secret, entrez un nom secret.
7. (Facultatif) Entrez une description qui vous aidera à identifier ce secret, puis choisissez Next.
8. (Facultatif) Sur la page Enregistrer une nouvelle page secrète, activez la rotation automatique. Pour plus d'informations, voir Rotation des secrets dans le guide de AWS Secrets Manager l'utilisateur.
9. Spécifiez un calendrier de rotation.
10. Choisissez une fonction Lambda capable de faire pivoter ce secret, puis choisissez Next.
11. Passez en revue vos configurations secrètes, puis choisissez Store.

Pour autoriser l'interaction avec votre passerelle SiteWise Edge AWS Secrets Manager, le rôle IAM de votre passerelle SiteWise Edge doit autoriser l'`secretsmanager:GetSecretValue`action. Vous pouvez utiliser le périphérique principal de Greengrass pour rechercher la politique IAM. Pour plus d'informations sur la mise à jour d'une stratégie IAM, consultez la section Modification des politiques IAM dans le Guide de l'AWS Identity and Access Management utilisateur.

Example politique

Remplacez *`secret-arn`* par le Amazon Resource Name (ARN) du secret que vous avez créé à l'étape précédente. Pour plus d'informations sur la façon d'obtenir l'ARN d'un secret, consultez la section Extraire votre secret AWS Secrets Manager dans le guide de AWS Secrets Manager l'utilisateur.

```
{
"Version":"2012-10-17",
"Statement":[
  {
     "Action":[
        "secretsmanager:GetSecretValue"
     ],
     "Effect":"Allow",
     "Resource":[
        "secret-arn"
     ]
  }
]
}
```

Étape 2 : Déployer des secrets sur votre périphérique de passerelle SiteWise Edge

Vous pouvez utiliser la AWS IoT SiteWise console pour déployer des secrets sur votre passerelle SiteWise Edge.

Pour déployer un secret (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans le volet de navigation, choisissez Passerelles.
3. Dans la liste des passerelles, choisissez la passerelle SiteWise Edge cible.
4. Dans la section Configuration de la passerelle, choisissez le lien du périphérique principal Greengrass pour ouvrir le AWS IoT Greengrass cœur associé à la passerelle SiteWise Edge.
5. Dans le volet de navigation, choisissez Deployments.
6. Choisissez le déploiement cible, puis sélectionnez Revise.
7. Sur la page Spécifier la cible, choisissez Next.
8. Sur la page Sélectionner les composants, dans la section Composants publics, désactivez Afficher uniquement les composants sélectionnés.
9. Recherchez et choisissez le fichier aws.greengrass. SecretManagercomposant, puis choisissez Next.
10. Dans la liste des composants sélectionnés, sélectionnez aws.greengrass. SecretManager, puis choisissez Configurer le composant.
11. Dans le champ Configuration à fusionner, ajoutez l'objet JSON suivant.

> **Note**
>
> Remplacez *secret-arn* par l'ARN du secret que vous avez créé à l'étape précédente. Pour plus d'informations sur la façon d'obtenir l'ARN d'un secret, consultez la section Extraire votre secret AWS Secrets Manager dans le guide de AWS Secrets Manager l'utilisateur.

```
{
"cloudSecrets":[
  {
     "arn":"secret-arn"
  }
]
}
```

12. Choisissez Confirmer.
13. Choisissez Suivant.
14. Sur la page Configurer les paramètres avancés, choisissez Next.
15. Passez en revue vos configurations de déploiement, puis choisissez Deploy.

Étape 3 : ajouter des configurations d'authentification

Vous pouvez utiliser la AWS IoT SiteWise console pour ajouter des configurations d'authentification à votre passerelle SiteWise Edge.

Pour ajouter des configurations d'authentification (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans la liste des passerelles, choisissez la passerelle SiteWise Edge cible.
3. Dans la liste des sources de données, choisissez la source de données cible, puis sélectionnez Modifier.
4. Sur la page Ajouter une source de données, choisissez Configuration avancée.
5. Pour la configuration de l'authentification, choisissez le secret que vous avez déployé à l'étape précédente.
6. Choisissez Enregistrer.

Choix d'une destination pour les données de votre serveur source

Les données sont exportées de la périphérie vers le AWS IoT SiteWise mode en temps réel, ou par lots à l'aide d'Amazon S3. Vous pouvez également envoyer le flux à un autre composant à l'aide d'un AWS IoT Greengrass flux.

- AWS IoT SiteWise en temps réel — Choisissez cette option pour envoyer les données directement au AWS IoT SiteWise stockage. Ingérez et surveillez les données en temps réel, et traitez-les à la périphérie.
- AWS IoT SiteWise Mise en mémoire tampon à l'aide d'Amazon S3 : envoyez les données au format parquet vers Amazon S3, puis importez-les dans le AWS IoT SiteWise stockage. Choisissez cette option pour ingérer les données par lots et stocker les données historiques de manière rentable. Vous pouvez configurer l'emplacement de votre compartiment Amazon S3 préféré et la fréquence à laquelle vous souhaitez que les données soient chargées sur Amazon S3. Vous pouvez également choisir ce que vous souhaitez faire avec les données après leur ingestion dans AWS IoT SiteWise. Vous pouvez choisir que les données soient disponibles à la fois dans Amazon S3 SiteWise et dans Amazon S3 ou vous pouvez choisir de les supprimer automatiquement d'Amazon S3.
  - Le bucket Amazon S3 est un mécanisme de préparation et de mise en mémoire tampon qui prend en charge les fichiers au format parquet.
  - Si vous cochez la case Importer les données dans le AWS IoT SiteWise stockage, les données sont d'abord chargées dans Amazon S3, puis dans le AWS IoT SiteWise stockage.
    - Si vous cochez la case Supprimer les données d'Amazon S3, les données sont supprimées d'Amazon S3 après leur importation dans le SiteWise stockage.
    - Si vous décochez la case Supprimer les données d'Amazon S3, les données sont stockées à la fois dans Amazon S3 et dans le SiteWise stockage.
  - Si vous décochez la case Importer les données dans le AWS IoT SiteWise stockage, les données sont stockées uniquement dans Amazon S3. Il n'est pas importé dans le SiteWise stockage.

  Visitez Gestion du stockage des données pour plus de détails sur les différentes options de stockage AWS IoT SiteWise proposées. Pour en savoir plus sur les options de tarification, consultez la section AWS IoT SiteWise Tarification.
- AWS IoT Greengrass gestionnaire de flux — Utilisez le gestionnaire de AWS IoT Greengrass flux pour envoyer des données vers les AWS Cloud destinations suivantes : canaux AWS IoT Analytics entrants, flux dans Amazon Kinesis Data Streams, propriétés des actifs ou objets AWS

IoT SiteWise dans Amazon Simple Storage Service (Amazon S3). Pour plus d'informations, consultez la section Gérer les flux de données sur le AWS IoT Greengrass Core dans le Guide AWS IoT Greengrass Version 2 du développeur.

L'exemple suivant montre la structure de message du flux de données requise. Tous les champs sont obligatoires.

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

> **Note**
>
> Le message du flux de données doit inclure (`assetIdetpropertyId`) ou `propertyAlias` dans sa structure.

`assetId`

(Facultatif) L'ID de la ressource à mettre à jour.

`propertyAlias`

(Facultatif) Alias identifiant la propriété, tel qu'un chemin de flux de données du serveur OPC-UA. Par exemple :

```
/company/windfarm/3/turbine/7/temperature
```

Pour plus d'informations, consultez la section Mappage des flux de données industriels aux propriétés des actifs dans le guide de AWS IoT SiteWise l'utilisateur.

`propertyId`

(Facultatif) ID de la propriété de l'actif pour cette entrée.

`propertyValues`

(Obligatoire) La liste des valeurs de propriétés à télécharger. Vous pouvez spécifier jusqu'à 10 éléments `propertyValues` de tableau.

`quality`

(Facultatif) La qualité de la valeur de la propriété de l'actif.

`timestamp`

(Obligatoire) Horodatage de la valeur de la propriété de l'actif.

`offsetInNanos`

(Facultatif) Le décalage de nanosecondes par rapport à`timeInSeconds`.

`timeInSeconds`

(Obligatoire) Date d'horodatage, en secondes, au format Unix Epoch. Les données de nanosecondes fractionnaires sont fournies par. `offsetInNanos`

`value`

(Obligatoire) La valeur de la propriété de l'actif.

> **Note**
>
> Seule l'une des valeurs suivantes peut exister dans le `value` champ.

`booleanValue`

(Facultatif) Données de propriété de l'actif de type booléen (`trueoufalse`).

`doubleValue`

(Facultatif) Données de propriété des actifs de type double (nombre à virgule flottante).

`integerValue`

(Facultatif) Données de propriété de l'actif de type entier (nombre entier).

`stringValue`

(Facultatif) Données de propriété de l'actif de type chaîne (séquence de caractères).

Ajouter des sources de données partenaires aux passerelles SiteWise Edge

Lorsque vous utilisez une passerelle AWS IoT SiteWise Edge, vous pouvez connecter une source de données partenaire à votre passerelle SiteWise Edge et recevoir des données du partenaire sur votre passerelle SiteWise Edge et dans le AWS cloud. Ces sources de données partenaires sont AWS IoT Greengrass des composants développés en partenariat entre AWS et le partenaire. Lorsque vous ajoutez une source de données partenaire, ce composant AWS IoT SiteWise sera créé et déployé sur votre passerelle SiteWise Edge.

Pour ajouter une source de données partenaire, procédez comme suit :

- Ajouter une source de données partenaire
- Accédez au portail Web du partenaire et configurez la source de données du partenaire afin qu'elle se connecte à la passerelle SiteWise Edge.

Rubriques

- Sécurité
- Ajouter une source de données partenaire
- Configurer docker sur votre passerelle Edge SiteWise
- SiteWise Sources de données des partenaires Edge Gateway

Sécurité

Dans le cadre du modèle de responsabilité partagée entre AWS nos clients et nos partenaires, les informations suivantes décrivent qui est responsable des différents aspects de la sécurité :

Responsabilité du client

- Sélection du partenaire.
- Configuration de l'accès réseau accordé au partenaire.

AWSresponsabilité

- Isoler le partenaire des ressources AWS cloud du client, à l'exception de celles dont le partenaire a besoin. Dans ce cas, AWS IoT SiteWise ingestion.
- Restreindre la solution partenaire à une utilisation raisonnable des ressources de la machine de passerelle SiteWise Edge (processeur, mémoire, système de fichiers).

Responsabilité du partenaire

- Utilisation de valeurs par défaut sécurisées.
- Garantir la sécurité de la solution au fil du temps grâce à des correctifs et à d'autres mises à jour appropriées.
- Préserver la confidentialité des données des clients.

Ajouter une source de données partenaire

Pour connecter une source de données partenaire à votre passerelle SiteWise Edge, ajoutez-la en tant que source de données. Lorsque vous l'ajoutez en tant que source de données, un AWS IoT Greengrass composant privé AWS IoT SiteWise sera déployé sur votre passerelle SiteWise Edge.

Prérequis

Pour ajouter une source de données partenaire, vous devez effectuer les opérations suivantes :

- Créez un compte auprès du partenaire.
- Liez les comptes.

Pour créer une passerelle SiteWise Edge avec une source de données partenaire

Si vous souhaitez créer une nouvelle passerelle SiteWise Edge, suivez les étapes décrites dansCréation d'une passerelle SiteWise Edge. Après avoir créé la passerelle SiteWise Edge, suivez

les étapes ci-dessous Pour ajouter une source de données partenaire à une passerelle SiteWise Edge existante pour ajouter une source de données partenaire.

Pour ajouter une source de données partenaire à une passerelle SiteWise Edge existante

1. Accédez à la console AWS IoT SiteWise.
2. Dans le volet de navigation, choisissez Passerelles.
3. Choisissez la passerelle SiteWise Edge à laquelle vous souhaitez connecter la source de données partenaire.
4. Sous Sources de données, choisissez Ajouter une source de données.
5. Pour Type de source, choisissez le partenaire auquel vous souhaitez connecter votre passerelle SiteWise Edge.

   > **Note**
   >
   > EasyEdge C'est actuellement la seule source de données partenaire disponible. La première fois que vous ajoutez une source de EasyEdge données, vous devez créer un EasyEdge compte.

6. Entrez le nom de la source.
7. Pour autoriser le partenaire à accéder à la source de données, sélectionnez Autoriser.
8. Pour autoriser la AWS IoT SiteWise mise à jour de votre composant AWS IoT SiteWise éditeur et, si le pack de traitement des données est activé, du composant AWS IoT SiteWise processeur, sélectionnez Mettre à jour les composants.
9. Choisissez Enregistrer.

Configurer docker sur votre passerelle Edge SiteWise

Pour ajouter une source de données partenaire, Docker Engine 1.9.1 ou version ultérieure doit être installé sur votre appareil local.

> **Note**
>
> La version 20.10 est la dernière version vérifiée pour fonctionner avec le logiciel de passerelle SiteWise Edge.

Pour vérifier que Docker est installé

Pour vérifier que Docker est installé, exécutez la commande suivante depuis un terminal connecté à votre passerelle SiteWise Edge :

```
docker info
```

Si la commande renvoie un `docker is not recognized` résultat ou si une ancienne version de Docker est installée, installez Docker Engine avant de continuer.

Pour configurer Docker

L'utilisateur du système qui exécute un composant de conteneur Docker doit disposer des autorisations root ou administrateur, ou vous devez configurer Docker pour l'exécuter en tant qu'utilisateur non root ou non administrateur.

Sur les appareils Linux, vous devez ajouter un `ggc_user` utilisateur au `docker` groupe sans `sudo` lequel vous pouvez appeler des commandes Docker.

Pour ajouter `ggc_user` au `docker` groupe l'utilisateur non root que vous utilisez pour exécuter les composants du conteneur Docker, exécutez la commande suivante :

```
sudo usermod -aG docker ggc_user
```

Pour plus d'informations, consultez les étapes de post-installation de Linux pour Docker Engine.

SiteWise Sources de données des partenaires Edge Gateway

Utilisez les informations ci-dessous pour configurer une source de données partenaire.

EasyEdge

Portail :

https://studio.easyedge.io/

EasyEdge documentation :

EasyEdge pour AWS

EasyEdge exigences — Informations sur les EasyEdge exigences, y compris les points de terminaison et les ports requis pour configurer le pare-feu. Remarque : vous aurez besoin d'un EasyEdge compte pour accéder à cette documentation.

Utiliser des packs

AWS IoT SiteWise Les passerelles Edge utilisent différents packs pour déterminer comment collecter et traiter vos données.

Les packs suivants sont actuellement disponibles :

- Pack de collecte de données : utilisez ce pack pour collecter vos données industrielles et les acheminer vers des destinations AWS cloud. Par défaut, ce pack est activé automatiquement pour votre passerelle SiteWise Edge.
- Pack de traitement des données : utilisez ce pack pour permettre la communication par passerelle SiteWise Edge avec des modèles d'actifs et des actifs configurés en périphérie. Vous pouvez utiliser la configuration périphérique pour contrôler les données d'actifs à calculer et à traiter sur site. Vous pouvez ensuite envoyer vos données à AWS IoT SiteWise d'autres AWS services. Pour plus d'informations sur le pack de traitement des données, consultezthe section called "Permettre le traitement des données de pointe".

Packs d'amélioration

> **Important**
>
> La mise à niveau des versions du pack de traitement des données antérieures (et incluses) à la version 2.1.x vers la version 2.1.x entraînera une perte de données des mesures stockées localement.

SiteWise Les passerelles Edge utilisent différents packs pour déterminer comment collecter et traiter vos données. Vous pouvez utiliser la AWS IoT SiteWise console pour mettre à niveau les packs.

Pour mettre à niveau des packs (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans le volet de navigation, choisissez Passerelles.

3. Dans la liste des passerelles, choisissez la passerelle SiteWise Edge contenant les packs que vous souhaitez mettre à niveau.
4. Dans la section Configuration de la passerelle, sélectionnez Mises à jour logicielles disponibles.
5. Sur la page de modification des versions du logiciel, dans la section Mises à jour des composants Gateway, procédez comme suit :

   - Pour mettre à jour le collecteur OPC-UA, choisissez une version, puis choisissez Deploy.
   - Pour mettre à jour l'éditeur, choisissez une version, puis choisissez Déployer.
   - Pour mettre à jour le pack de traitement des données, choisissez une version, puis choisissez Déployer.
6. Lorsque vous avez terminé de déployer les nouvelles versions, choisissez OK.

Si vous rencontrez des problèmes lors de la mise à niveau des packs, consultezImpossible de déployer des packs sur les passerelles SiteWise Edge.

Gestion des passerelles SiteWise Edge

Vous pouvez utiliser les opérations de AWS IoT SiteWise console et d'API pour gérer les passerelles AWS IoT SiteWise Edge. Vous pouvez également utiliser l'application AWS OpsHub for AWS IoT SiteWise for Windows pour gérer certains aspects de votre passerelle SiteWise Edge à partir de votre appareil local.

Nous vous recommandons vivement d'utiliser l' AWS IoT SiteWise application AWS OpsHub for pour surveiller l'utilisation du disque sur votre appareil local. Vous pouvez également surveiller les CloudWatch métriques `Gateway.AvailableDiskSpace` et `Gateway.UsedPercentageDiskSpace` celles d'Amazon et créer des alarmes pour être averti lorsque l'espace disque devient insuffisant. Pour plus d'informations sur les CloudWatch alarmes Amazon, consultez Créer une CloudWatch alarme basée sur un seuil statique.

Assurez-vous que votre appareil dispose de suffisamment d'espace pour les données à venir. Lorsque vous êtes sur le point de manquer d'espace sur votre appareil local, le service supprime automatiquement une petite quantité de données avec les horodatages les plus anciens pour faire de la place aux données à venir.

Pour vérifier si le service a supprimé vos données, procédez comme suit :

1. Connectez-vous à AWS OpsHub l' AWS IoT SiteWise application.

2. Sélectionnez Settings (Paramètres).
3. Pour les journaux, spécifiez une plage de temps, puis choisissez Télécharger.
4. Décompressez le fichier journal.
5. Si le fichier journal contient le message suivant, le service a supprimé vos données : un *certain nombre* d'octets de données ont été supprimés pour empêcher le stockage de la passerelle SiteWise Edge de manquer d'espace.

Gestion de votre passerelle SiteWise Edge avec la AWS IoT SiteWise console

Vous pouvez utiliser la AWS IoT SiteWise console pour configurer, mettre à jour et surveiller toutes les passerelles SiteWise Edge de votre AWS compte.

Vous pouvez consulter vos passerelles SiteWise Edge en accédant à la page Passerelles Edge de la console.AWS IoT SiteWise Pour accéder à la page de détails de la passerelle Edge d'une passerelle spécifique, choisissez le nom d'une passerelle Edge.

Dans l'onglet Vue d'ensemble de la page de détails de la passerelle Edge, vous pouvez effectuer les opérations suivantes :

- Dans la section Sources de données, mettez à jour la configuration des sources de données et configurez des sources de données supplémentaires
- Choisissez Open CloudWatch metrics pour afficher le nombre de points de données ingérés par source de données dans la console CloudWatch des métriques
- Dans la section Fonctionnalités Edge, ajoutez des packs de données à votre passerelle SiteWise Edge en cliquant sur Modifier
- Dans la section Configuration de la passerelle, consultez l'état de connectivité de vos passerelles SiteWise Edge
- Dans la section Configuration de l'éditeur, consultez l'état de synchronisation de la passerelle SiteWise Edge et la configuration du composant de l' AWS IoT SiteWise éditeur

Dans l'onglet Mises à jour de la page de détails de la passerelle Edge, vous pouvez voir les versions actuelles des composants et des packs déployées sur la passerelle Edge. C'est également là que vous déployez les nouvelles versions, lorsqu'elles sont disponibles.

Gestion des passerelles SiteWise Edge à l'aide de AWS OpsHubAWS IoT SiteWise

Vous utilisez l' AWS IoT SiteWise application AWS OpsHub for pour gérer et surveiller vos passerelles SiteWise Edge. Cette application propose les options de surveillance et de gestion suivantes :

- Sous Vue d'ensemble, vous pouvez effectuer les opérations suivantes :
  - Consultez les détails de la passerelle SiteWise Edge qui vous aident à obtenir des informations sur les données de votre appareil de passerelle SiteWise Edge, à identifier les problèmes et à améliorer les performances de la passerelle SiteWise Edge.
  - Portails View SiteWise Monitor qui surveillent les données provenant des serveurs locaux et des équipements situés en périphérie. Pour plus d'informations, voir Contenu AWS IoT SiteWise Monitor du guide de AWS IoT SiteWise Monitor candidature.
- Sous Health, un tableau de bord affiche les données de votre passerelle SiteWise Edge. Les experts du domaine, tels que les ingénieurs de processus, peuvent utiliser le tableau de bord pour avoir une vue d'ensemble du comportement de la passerelle SiteWise Edge.
- Sous Ressources, consultez les ressources déployées sur le périphérique local et la dernière valeur collectée ou calculée pour les propriétés des ressources.
- Dans Réglages, vous pouvez effectuer les opérations suivantes :
  - Si le pack de traitement des données est installé, consultez les informations de configuration de la passerelle SiteWise Edge et synchronisez les ressources avec le AWS cloud.
  - Téléchargez les fichiers d'authentification que vous pouvez utiliser pour accéder à la passerelle SiteWise Edge à l'aide d'autres outils.
  - Téléchargez des journaux que vous pouvez utiliser pour résoudre les problèmes liés à la passerelle SiteWise Edge.
  - Affichez les AWS IoT SiteWise composants déployés sur la passerelle SiteWise Edge.

Important

Les éléments suivants sont nécessaires AWS OpsHub pour AWS IoT SiteWise :

- Votre appareil local et l' AWS IoT SiteWise application AWS OpsHub for doivent être connectés au même réseau.

- Le pack de traitement des données doit être activé.

Pour gérer les passerelles SiteWise Edge à l'aide de AWS OpsHub

1. Téléchargez et installez l'application AWS OpsHubAWS IoT SiteWise pour Windows.
2. Ouvrez l'application .
3. Si vous n'avez pas configuré d'informations d'identification locales pour votre passerelle, suivez les étapes Accès à votre passerelle SiteWise Edge à l'aide des informations d'identification du système d'exploitation local ci-dessous pour les configurer.
4. Vous pouvez vous connecter à votre passerelle SiteWise Edge avec vos informations d'identification Linux ou LDAP (Lightweight Directory Access Protocol). Pour vous connecter à votre passerelle SiteWise Edge, effectuez l'une des opérations suivantes :

   Linux

   1. Dans Nom d'hôte ou adresse IP, entrez le nom d'hôte ou l'adresse IP de votre appareil local.
   2. Pour Authentification, choisissez Linux.
   3. Dans Nom d'utilisateur, entrez le nom d'utilisateur de votre système d'exploitation Linux.
   4. Dans Mot de passe, entrez le mot de passe de votre système d'exploitation Linux.
   5. Choisissez Sign in (Connexion).

   LDAP

   1. Dans Nom d'hôte ou adresse IP, entrez le nom d'hôte ou l'adresse IP de votre appareil local.
   2. Pour Authentification, choisissez LDAP.
   3. Dans Nom d'utilisateur, entrez le nom d'utilisateur de votre LDAP.
   4. Dans Mot de passe, entrez le mot de passe de votre LDAP.
   5. Choisissez Sign in (Connexion).

Accès à votre passerelle SiteWise Edge à l'aide des informations d'identification du système d'exploitation local

Outre le protocole LDAP (Lightweight Directory Access Protocol), vous pouvez utiliser les informations d'identification Linux ou Windows pour accéder à votre passerelle SiteWise Edge.

> **Important**
>
> Pour accéder à votre passerelle SiteWise Edge avec des informations d'identification Linux, vous devez activer le pack de traitement de données pour votre passerelle SiteWise Edge.

Accès à votre passerelle SiteWise Edge à l'aide des informations d'identification du système d'exploitation Linux

Les étapes suivantes supposent que vous utilisez un appareil avec Ubuntu. Si vous utilisez une autre distribution Linux, consultez la documentation correspondante à votre appareil.

Pour créer un groupe d'utilisateurs Linux

1. Pour créer un groupe d'administrateurs, exécutez la commande suivante.

   ```
   sudo groupadd --system SWE_ADMIN_GROUP
   ```

   Les utilisateurs du `SWE_ADMIN_GROUP` groupe peuvent autoriser l'accès administrateur à la passerelle SiteWise Edge.
2. Pour créer un groupe d'utilisateurs, exécutez la commande suivante.

   ```
   sudo groupadd --system SWE_USER_GROUP
   ```

   Les utilisateurs du `SWE_USER_GROUP` groupe peuvent autoriser l'accès en lecture seule à la passerelle SiteWise Edge.
3. Pour ajouter un utilisateur au groupe d'administrateurs, exécutez la commande suivante. Remplacez le *`nom d'utilisateur`* et le *`mot de passe`* par le nom d'utilisateur et le mot de passe que vous souhaitez ajouter.

   ```
   sudo useradd -p $(openssl passwd -1 password) user-name
   ```

4. Pour ajouter un utilisateur à l'une SWE_ADMIN_GROUP ou l'autreSWE_USER_GROUP, remplacez le *nom d'utilisateur par* le nom d'utilisateur que vous avez ajouté à l'étape précédente.

   ```
   sudo usermod -a -G SWE_ADMIN_GROUP user-name
   ```

Vous pouvez désormais utiliser le nom d'utilisateur et le mot de passe pour vous connecter à la passerelle SiteWise Edge sur l' AWS IoT SiteWise application AWS OpsHub for.

Accès à votre passerelle SiteWise Edge à l'aide des informations d'identification Windows

Les étapes suivantes supposent que vous utilisez un appareil Windows.

> **Important**
>
> La sécurité est une responsabilité partagée entre vous AWS et vous. Créez une politique de mot de passe robuste comportant au moins 12 caractères et une combinaison de majuscules, de minuscules, de chiffres et de symboles. Définissez également les règles du pare-feu Windows pour autoriser le trafic entrant sur le port 443 et pour bloquer le trafic entrant sur tous les autres ports.

Pour créer un groupe d'utilisateurs Windows Server

1. Exécutez PowerShell en tant qu'administrateur.

   a. Sur le serveur Windows sur lequel vous souhaitez installer SiteWise Edge Gateway, connectez-vous en tant qu'administrateur.

   b. Entrez PowerShelldans la barre de recherche Windows.

   c. Dans les résultats de recherche, cliquez avec le bouton droit sur l' PowerShellapplication Windows. Choisissez Exécuter en tant qu'administrateur.

2. Pour créer un groupe d'administrateurs, exécutez la commande suivante.

   ```
   net localgroup SWE_ADMIN_GROUP /add
   ```

   Vous devez être un utilisateur du SWE_ADMIN_GROUP groupe pour autoriser l'accès administrateur à la passerelle SiteWise Edge.

3. Pour créer un groupe d'utilisateurs, exécutez la commande suivante.

```
net localgroup SWE_USER_GROUP /add
```

Vous devez être un utilisateur du SWE_USER_GROUP groupe pour autoriser l'accès prêt à l'emploi à la passerelle SiteWise Edge.

4. Pour ajouter un utilisateur, exécutez la commande suivante. Remplacez le *nom d'utilisateur* et le *mot de passe* par le nom d'utilisateur et le mot de passe que vous souhaitez créer.

```
net user user-name password /add
```

5. Pour ajouter un utilisateur au groupe d'administrateurs, exécutez la commande suivante. Remplacez le *nom d'utilisateur par* le nom d'utilisateur que vous souhaitez ajouter.

```
net localgroup SWE_ADMIN_GROUP user-name /add
```

Vous pouvez désormais utiliser le nom d'utilisateur et le mot de passe pour vous connecter à la passerelle SiteWise Edge sur l' AWS IoT SiteWise application AWS OpsHub for.

Gestion du certificat de passerelle SiteWise Edge

Vous pouvez utiliser SiteWise Monitor et des applications tierces, telles que Grafana, sur vos appareils de passerelle SiteWise Edge. Ces applications nécessitent une connexion TLS au service. SiteWise Les passerelles Edge utilisent actuellement un certificat auto-signé. Si vous utilisez un navigateur pour ouvrir les applications, par exemple un portail SiteWise Monitor, vous pouvez recevoir un avertissement concernant un certificat non fiable.

Ce qui suit montre comment télécharger le certificat sécurisé depuis l' AWS IoT SiteWise application AWS OpsHub for.

1. Connectez-vous à l'application.
2. Sélectionnez Settings (Paramètres).
3. Pour Authentification, choisissez Télécharger le certificat.

Ce qui suit suppose que vous utilisez Google Chrome ou FireFox. Si vous utilisez un autre navigateur, consultez la documentation correspondante. Pour ajouter le certificat que vous avez téléchargé à l'étape précédente dans un navigateur, effectuez l'une des opérations suivantes :

- Si vous utilisez Google Chrome, suivez les instructions relatives à la configuration des certificats dans la documentation d'aide de Google Chrome Enterprise.
- Si vous utilisez Firefox, suivez les instructions pour charger le certificat dans le navigateur Mozilla ou Firefox de la documentation Oracle.

Modification de la version des packs de composants de la passerelle SiteWise Edge

Vous pouvez utiliser la AWS IoT SiteWise console pour modifier la version des packs de composants sur vos passerelles SiteWise Edge.

Pour modifier la version d'un pack de composants de passerelle SiteWise Edge

1. Accédez à la console AWS IoT SiteWise.
2. Dans le volet de navigation de gauche, sélectionnez Passerelles.
3. Sélectionnez la passerelle SiteWise Edge dont vous souhaitez modifier les versions du pack.
4. Sous Configuration de la passerelle, choisissez Afficher les versions du logiciel.
5. Sur la page Modifier les versions du logiciel, pour le pack dont vous souhaitez mettre à jour la version, sélectionnez la version que vous souhaitez déployer et choisissez Déployer.
6. Sélectionnez Exécuté.

Running SiteWise Edge sur Siemens Industrial Edge

Vous pouvez ingérer les données de votre appareil Siemens Industrial Edge vers le vôtre Compte AWS en exécutant une passerelle SiteWise Edge sur l'appareil. Pour ce faire, vous créez une ressource de passerelle SiteWise Edge avec une cible de déploiement de l'appareil Siemens Industrial Edge (nouveau), vous téléchargez le fichier de configuration et vous le chargez sur votre application Siemens via le portail Siemens Industrial Edge Management (IEM). Pour plus d'informations sur l'exécution d' AWS IoT SiteWise Edge sur Siemens Industrial Edge, notamment sur la configuration des ressources Siemens requises, voir Qu'est-ce qu'Industrial Edge ? dans la documentation de Siemens.

> **Note**
>
> Siemens n'est ni un vendeur ni un fournisseur d' AWS IoT SiteWise Edge. Le Siemens Industrial Edge Marketplace est un marché indépendant.

Rubriques

- Prérequis
- Sécurité
- Créez le fichier de configuration
- Résolution des problèmes
- Nous contacter

Prérequis

Pour exécuter AWS IoT SiteWise Edge sur Siemens Industrial Edge, vous avez besoin des éléments suivants :

- Un compte Siemens Digital Exchange Platform
- Un compte Siemens Industrial Edge Hub (iehub)
- Une instance de Siemens Industrial Edge Management (IEM)
- Un périphérique Siemens Industrial Edge (IED) ou un périphérique virtuel Siemens Industrial Edge (iEVD)
- Accès à la cible de déploiement des appareils Siemens Industrial Edge. Pour y accéder, accédez à la AWS IoT SiteWise console et choisissez Demander l'accès.

Sécurité

Dans le cadre du modèle de responsabilité partagée entre AWS nos clients et nos partenaires, les informations suivantes décrivent qui est responsable des différents aspects de la sécurité :

Responsabilité du client

- Sélection du partenaire.
- Configuration de l'accès réseau accordé au partenaire.

- Sécurisation physique de l'appareil exécutant AWS IoT SiteWise Edge.

AWS responsabilité

- Isoler le partenaire des ressources AWS cloud du client.

Responsabilité du partenaire

- Utilisation de valeurs par défaut sécurisées.
- Garantir la sécurité de la solution au fil du temps grâce à des correctifs et à d'autres mises à jour appropriées.
- Préserver la confidentialité des données des clients.
- Vérification des autres applications disponibles sur le marché des partenaires.

Au cours de la phase de prévisualisation de cette fonctionnalité, les données client mises en AWS IoT SiteWise cache sur l'appareil du partenaire sont accessibles par le partenaire et les autres applications installées via le marché partenaire.

Créez le fichier de configuration

Une fois que vous disposez des comptes Siemens et des instances IEM appropriés, vous pouvez créer une passerelle SiteWise Edge de type « appareil Siemens Industrial Edge » de type déploiement.

Pour créer le fichier de configuration

1. Accédez à la console AWS IoT SiteWise.
2. Dans le volet de navigation, choisissez Edge gateways.
3. Cliquez sur Create gateway (Créer une passerelle).
4. Pour le type de déploiement, choisissez Appareil Siemens Industrial Edge - nouveau.
5. Entrez un nom pour votre passerelle SiteWise Edge ou utilisez le nom généré par AWS IoT SiteWise.
6. (Facultatif) Dans la section Configuration avancée, procédez comme suit :
    - Entrez un nom pour votre AWS IoT Core objet ou utilisez le nom généré par AWS IoT SiteWise.
7. Cliquez sur Create gateway (Créer une passerelle).

8. Dans la boîte de dialogue Générer le fichier de configuration de la passerelle SiteWise Edge, sélectionnez Générer et télécharger. AWS IoT SiteWise génère automatiquement un fichier de configuration que vous utiliserez pour configurer l'application AWS IoT SiteWise Edge.

> **Important**
>
> Assurez-vous d'enregistrer le fichier de configuration dans un emplacement sécurisé. Vous utiliserez le fichier ultérieurement.

Maintenant que vous avez créé la passerelle SiteWise Edge, procédez comme suit pour terminer la configuration de votre passerelle SiteWise Edge :

1. Ajouter des sources de données
2. Configuration du composant Publisher

Une fois que vous avez le fichier de configuration et que la passerelle SiteWise Edge est configurée, téléchargez l'application AWS IoT SiteWise Edge depuis le Siemens Industrial Edge Marketplace et installez-la à l'aide du portail Siemens Industrial Edge Management (IEM). Accédez ensuite à votre appareil Siemens Industrial Edge via le portail Siemens Industrial Edge Management (IEM) et téléchargez le fichier de configuration sur l'appareil sur lequel vous souhaitez installer la passerelle SiteWise Edge.

Résolution des problèmes

Pour résoudre les problèmes liés à la passerelle SiteWise Edge de votre appareil Siemens Industrial Edge, vous pouvez accéder aux journaux de l'application via les portails Siemens Industrial Edge Management (IEM) ou Siemens Industrial Edge Device (IED). Pour plus d'informations, consultez la section Téléchargement des journaux dans la documentation de Siemens.

Je vois « SESSION_TAKEN_OVER » ou « com.aws.greengrass.mqttclient ». MqttClient: Impossible de publier le message via Spooler et je vais réessayer. ' dans les journaux

Si un avertissement `SESSION_TAKEN_OVER` ou une erreur s'affiche `com.aws.greengrass.mqttclient.MqttClient: Failed to publish the message via Spooler and will retry.` dans vos journaux à l'adresse `/greengrass/v2/logs/`

`greengrass.log`, vous essayez peut-être d'utiliser le même fichier de configuration pour plusieurs passerelles SiteWise Edge sur plusieurs appareils. Chaque passerelle SiteWise Edge a besoin d'un fichier de configuration unique pour se connecter à votre Compte AWS.

Je vois « com.aws.greengrass.deployment ». IotJobsHelper: aucune tâche de déploiement n'a été trouvée. ' ou « Le résultat du déploiement a déjà été signalé ». dans les journaux

Si vous voyez `com.aws.greengrass.deployment.IotJobsHelper: No deployment job found.` ou `Deployment result already reported.` dans vos journaux à l'`/greengrass/v2/logs/greengrass.log`adresse, vous essayez peut-être de réutiliser le même fichier de configuration.

Les solutions sont multiples :

- Si vous souhaitez réutiliser le fichier de configuration, procédez comme suit :
  1. Accédez à la console AWS IoT SiteWise.
  2. Dans le volet de navigation, choisissez Passerelles.
  3. Choisissez la passerelle SiteWise Edge que vous souhaitez réutiliser.
  4. Choisissez l'onglet Mises à jour.
  5. Sélectionnez une autre version de Publisher et choisissez Déployer.
- Suivez les étapes décrites Créez le fichier de configuration pour créer un nouveau fichier de configuration.

Je vois « AWS_REGION manquant dans le fichier de configuration » dans les journaux.

Si vous voyez `Config file missing AWS_REGION` dans les journaux de Siemens que le JSON du fichier de configuration est endommagé. Vous devez créer un nouveau fichier de configuration. Suivez les étapes décrites Créez le fichier de configuration pour créer un nouveau fichier de configuration.

Nous contacter

- Si vous souhaitez demander l'accès à l'application, accédez à la AWS IoT SiteWise console et choisissez Demander l'accès.

- Si vous souhaitez obtenir de l'aide pour résoudre les problèmes liés à l'application, accédez à la AWS IoT SiteWise console, accédez à la page de détails de la passerelle SiteWise Edge, puis choisissez Obtenir de l'aide.

Filtrer les actifs sur une passerelle SiteWise Edge

Vous pouvez utiliser le filtrage périphérique pour gérer plus efficacement vos actifs en n'envoyant qu'un sous-ensemble d'actifs à une passerelle SiteWise Edge spécifique pour une utilisation dans le traitement des données. Si vos actifs sont organisés dans une structure arborescente, ou parent-enfant, vous pouvez configurer une politique IAM attachée au rôle IAM d'une passerelle SiteWise Edge qui autorise uniquement l'envoi de la racine de l'arborescence, ou parent, et de ses enfants à une passerelle Edge spécifique. SiteWise

> **Note**
>
> Si vous organisez des actifs existants dans une arborescence, après avoir créé la structure, accédez à chaque actif existant que vous avez ajouté à la structure et choisissez Modifier, puis cliquez sur Enregistrer pour vous assurer que la AWS IoT SiteWise nouvelle structure est reconnue.

Configuration du filtrage des bords

Configurez le filtrage SiteWise Edge sur votre passerelle Edge en ajoutant la politique IAM suivante au rôle IAM de la passerelle SiteWise Edge, en remplaçant *< root-asset-id >* par l'ID de la ressource racine que vous souhaitez envoyer à la passerelle SiteWise Edge.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "iotsitewise:DescribeAsset",
                "iotsitewise:ListAssociatedAssets"
            ],
            "Resource": "arn:aws:iotsitewise:*:*:asset/*",
            "Condition": {
                "StringNotLike": {
```

```
                    "iotsitewise:assetHierarchyPath": "/<root-asset-id>*"
                }
            }
        }
    ]
}
```

Si vous souhaitez supprimer des actifs se trouvant actuellement sur votre passerelle SiteWise Edge, connectez-vous à votre passerelle SiteWise Edge et exécutez la commande suivante pour forcer la passerelle SiteWise Edge à se synchroniser avec celle-ci AWS IoT SiteWise en supprimant le cache.

```
sudo rm /greengrass/v2/work/aws.iot.SiteWiseEdgeProcessor/sync-app/
sync_resource_bundles/edge.json
```

Utilisation d'AWS IoT SiteWiseAPI à la périphérie

Vous pouvez utiliser un sous-ensemble des AWS IoT SiteWise API disponibles ainsi que des API spécifiques à la périphérie pour interagir avec les modèles d'actifs et leurs actifs en périphérie. Les modèles d'actifs doivent être configurés pour fonctionner en périphérie. Pour plus d'informations, consultez Traitement des données à la périphérie.

Utilisez ces API pour collecter des données sur vos modèles d'actifs et vos actifs, surveiller vos portails déployés et les indicateurs de votre tableau de bord, et obtenir des données sur les actifs collectées à la périphérie. Cela fournit un hôte central dans votre réseau pour les interactions AWS IoT SiteWise sans nécessiter un appel d'API Web.

Rubriques

- Toutes les API disponibles pour une utilisation avec les appareils de AWS IoT SiteWise pointe
- API Edge uniquement destinées à être utilisées avec des appareils Edge AWS IoT SiteWise
- Tutoriel : Obtenir une liste de modèles d'actifs sur une passerelle SiteWise Edge

Toutes les API disponibles pour une utilisation avec les appareils de AWS IoT SiteWise pointe

Lorsque vous travaillez avec des appareils en périphérie, vous pouvez utiliser diverses API pour interagir avec l'appareil AWS IoT SiteWise et effectuer des tâches localement sur celui-ci.

AWS IoT SiteWiseAPI disponibles

Les AWS IoT SiteWise API suivantes sont disponibles sur les appareils Edge :

- ListAssetModels
- DescribeAssetModel
- ListAssets
- DescribeAsset
- DescribeAssetProperty
- ListAssociatedAssets
- GetAssetPropertyAggregates
- GetAssetPropertyValue
- GetAssetPropertyValueHistory
- ListDashboards
- ListPortals
- ListProjectAssets
- ListProjects
- DescribeDashboard
- DescribePortal
- DescribeProject

API disponibles uniquement en périphérie

Les API suivantes sont utilisées localement sur les appareils en périphérie :

- Authentifier— Utilisez cette API pour obtenir les informations d'identification temporaires SigV4 que vous utiliserez pour effectuer des appels d'API.

API Edge uniquement destinées à être utilisées avec des appareils Edge AWS IoT SiteWise

Outre les AWS IoT SiteWise API disponibles en périphérie, il existe des API spécifiques à la périphérie. Ces API spécifiques à la périphérie sont décrites ci-dessous.

Authentifier

Obtient les informations d'identification de la passerelle SiteWise Edge. Vous devez ajouter des utilisateurs locaux ou vous connecter à votre système via LDAP ou un groupe d'utilisateurs Linux. Pour plus d'informations sur l'ajout d'utilisateurs, consultez LDAP ou groupe d'utilisateurs Linux.

Syntaxe de demande

```
POST /authenticate HTTP/1.1
Content-type: application/json
{
  "username": "string",
  "password": "string",
  "authMechanism": "string"
}
```

Paramètres de demande d'URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

nom d'utilisateur

Le nom d'utilisateur utilisé pour valider l'appel de demande.

Type : chaîne

Obligatoire : oui

mot de passe

Le mot de passe de l'utilisateur demandant les informations d'identification.

Type : chaîne

Obligatoire : oui

authMechanism

Méthode d'authentification permettant de valider cet utilisateur sur l'hôte.

Type : chaîne

Valeurs valides: `ldap`, `linux`, `winnt`

Obligatoire : oui

Syntaxe de réponse

```
HTTP/1.1 200
Content-type: application/json
{
  "accessKeyId": "string",
  "secretAccessKey": "string",
  "sessionToken": "string",
  "region": "edge"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON.

accessKeyId

L'ID de clé d'accès qui identifie les informations d'identification de sécurité temporaires.

Contraintes de longueur : longueur minimale de 16. Longueur maximum de 128.

Modèle : `[\w]*`

secretAccessKey

La clé d'accès secrète qui peut être utilisée pour signer les demandes.

Type : chaîne

sessionToken

Le jeton que les utilisateurs doivent transmettre à l'API du service pour utiliser les informations d'identification temporaires.

Type : chaîne

region

La région que vous ciblez pour les appels d'API.

Type : CONSTANT - edge

Erreurs

IllegalArgumentException

La demande a été rejetée car le corps du document fourni était mal formé. Le message d'erreur décrit l'erreur spécifique.

Code d'état HTTP : 400

AccessDeniedException

L'utilisateur ne dispose pas d'informations d'identification valides basées sur le fournisseur d'identité actuel. Le message d'erreur décrit le mécanisme d'authentification.

Code d'état HTTP : 403

TooManyRequestsException

La demande a atteint sa limite de tentatives d'authentification. Le message d'erreur indique le temps d'attente avant que de nouvelles tentatives d'authentification ne soient effectuées.

Code d'état HTTP : 429

Tutoriel : Obtenir une liste de modèles d'actifs sur une passerelle SiteWise Edge

Vous pouvez utiliser un sous-ensemble des AWS IoT SiteWise API disponibles ainsi que des API spécifiques à la périphérie pour interagir avec les modèles d'actifs et leurs actifs en périphérie. Ce didacticiel vous expliquera comment obtenir des informations d'identification temporaires sur une passerelle AWS IoT SiteWise Edge et comment obtenir une liste des modèles d'actifs sur la passerelle SiteWise Edge.

Prérequis

Dans les étapes de ce didacticiel, vous pouvez utiliser une variété d'outils. Pour utiliser ces outils, assurez-vous que les prérequis correspondants sont installés.

Pour suivre ce didacticiel, vous aurez besoin des éléments suivants :

- Un déployé et en cours d'exécution SiteWise Exigences relatives à la passerelle Edge

- Accédez à votre passerelle SiteWise Edge sur le même réseau via le port 443.
- OpenSSL installé
- (AWS OpsHubpourAWS IoT SiteWise) L'AWS OpsHubAWS IoT SiteWiseapplication
- (curl) curl installé
- (Python) urllib3 installé
- (Python) Python3 installé
- (Python) Boto3 installé
- (Python) BotoCoreinstallé

Étape 1 : obtenir un certificat signé du service SiteWise Edge Gateway

Pour établir une connexion TLS avec les API disponibles sur la passerelle SiteWise Edge, vous avez besoin d'un certificat fiable. Vous pouvez générer ce certificat à l'aide d'un OpenSSL ou pourAWS OpsHub. AWS IoT SiteWise

OpenSSL

> **Note**
>
> OpenSSL doit être installé pour exécuter cette commande.

Ouvrez un terminal et exécutez la commande suivante pour obtenir un certificat signé auprès de la passerelle SiteWise Edge. `<sitewise_gateway_ip>`Remplacez-le par l'adresse IP de la passerelle 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

Vous pouvez utiliser AWS OpsHub pourAWS IoT SiteWise. Pour plus d'informations, consultez Gestion des passerelles SiteWise Edge.

Le chemin absolu vers le certificat de passerelle SiteWise Edge téléchargé est utilisé dans ce didacticiel. Exécutez la commande suivante pour exporter le chemin complet de votre certificat, en le `<absolute_path_to_certificate>` remplaçant par le chemin d'accès au certificat :

```
export PATH_TO_CERTIFICATE='<absolute_path_to_certificate>'
```

Étape 2 : obtenir le nom d'hôte de votre passerelle SiteWise Edge

> **Note**
>
> OpenSSL doit être installé pour exécuter cette commande.

Pour terminer le didacticiel, vous aurez besoin du nom d'hôte de votre passerelle SiteWise Edge. Pour obtenir le nom d'hôte de votre passerelle SiteWise Edge, exécutez ce qui suit, en le `<sitewise_gateway_ip>` remplaçant par l'adresse IP de la passerelle SiteWise Edge :

```
openssl s_client -connect <sitewise_gateway_ip>:443 </dev/null 2>/dev/null | grep -Po
 'CN = \K.*'| head -1
```

Exécutez la commande suivante pour exporter le nom d'hôte à utiliser ultérieurement, en le `<your_edge_gateway_hostname>` remplaçant par le nom d'hôte de votre passerelle SiteWise Edge :

```
export GATEWAY_HOSTNAME='<your_edge_gateway_hostname>'
```

Étape 3 : obtenir des informations d'identification temporaires pour votre passerelle SiteWise Edge

Maintenant que vous avez le certificat signé et le nom d'hôte de votre passerelle SiteWise Edge, vous devez obtenir des informations d'identification temporaires afin de pouvoir exécuter des API sur la passerelle. Vous pouvez obtenir ces informations d'identification via AWS OpsHub AWS IoT SiteWise ou directement depuis la passerelle SiteWise Edge à l'aide d'API.

> **Important**
>
> Les informations d'identification expirent toutes les 4 heures. Vous devez donc les obtenir juste avant d'utiliser les API de votre passerelle SiteWise Edge. Ne mettez pas les informations d'identification en cache pendant plus de 4 heures.

Obtenez des informations d'identification temporaires à l'aide AWS OpsHub de AWS IoT SiteWise

> **Note**
>
> Vous devez installer l'AWS IoT SiteWiseapplication AWS OpsHub for.

AWS OpsHubPour utiliser l'AWS IoT SiteWiseapplication afin d'obtenir vos informations d'identification temporaires, procédez comme suit :

1. Connectez-vous à l'application.
2. Sélectionnez Settings (Paramètres).
3. Pour Authentification, choisissez Copier les informations d'identification.
4. Développez l'option adaptée à votre environnement et choisissez Copier.
5. Enregistrez les informations d'identification pour les utiliser ultérieurement.

Obtenez des informations d'identification temporaires à l'aide de l'API de passerelle SiteWise Edge

Pour utiliser l'API de passerelle SiteWise Edge afin d'obtenir les informations d'identification temporaires, vous pouvez utiliser un script Python ou un curl. Vous devez d'abord disposer d'un nom d'utilisateur et d'un mot de passe pour votre passerelle SiteWise Edge. Les passerelles SiteWise Edge utilisent l'authentification et l'autorisation SigV4. Pour plus d'informations sur l'ajout d'utilisateurs, consultez LDAP ou groupe d'utilisateurs Linux. Ces informations d'identification seront utilisées dans les étapes suivantes pour obtenir les informations d'identification locales sur votre passerelle SiteWise Edge qui sont nécessaires pour utiliser les AWS IoT SiteWise API.

Python

> **Note**
>
> Vous devez installer urllib3 et Python3.

Pour obtenir les informations d'identification à l'aide de Python

1. Créez un fichier appelé get_credentials.py et copiez-y le code suivant.

```
'''
```

```
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. Exécutez get_credentials.py depuis le terminal en remplaçant <gateway_username> et en utilisant <gateway_password> les informations d'identification que vous avez créées.

```
python3 get_credentials.py -e https://$GATEWAY_HOSTNAME -c $PATH_TO_CERTIFICATE
 -u '<gateway_username>' -p '<gateway_password>' -m 'linux'
```

curl

> **Note**
>
> Vous devez installer Curl.

Pour obtenir les informations d'identification à l'aide de curl

1. Exécutez la commande suivante depuis le terminal en remplaçant <gateway_username>et en utilisant <gateway_password>les informations d'identification que vous avez créées.

   ```
   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"
   }'
   ```

   Les résultats doivent avoir l'aspect suivant :

   ```
   {
       "username": "sweuser",
       "accessKeyId": "<accessKeyId>",
       "secretAccessKey": "<secretAccessKey>",
       "sessionToken": "<sessionToken>",
       "sessionExpiryTime": "2022-11-17T04:51:40.927095Z",
       "authMechanism": "linux",
       "role": "edge-user"
   }
   ```

2. Exécutez la commande suivante à partir de votre terminal.

   ```
   export AWS_ACCESS_KEY_ID=<accessKeyId>
   ```

```
export AWS_SECRET_ACCESS_KEY=<secretAccessKey>
export AWS_SESSION_TOKEN=<sessionToken>
export AWS_REGION=edge
```

Étape 4 : obtenir une liste des modèles d'actifs sur la passerelle SiteWise Edge

Maintenant que vous disposez d'un certificat signé, du nom d'hôte de votre passerelle SiteWise Edge et des informations d'identification temporaires pour votre passerelle SiteWise Edge, vous pouvez utiliser l'`ListAssetModels`API pour obtenir une liste des modèles d'actifs de votre passerelle SiteWise Edge.

Python

> **Note**
>
> Vous avez besoin de Python3, Boto3 et d'une installation. BotoCore

Pour obtenir la liste des modèles d'actifs à l'aide de Python

1. Créez un fichier appelé list_asset_model.py et copiez-y le code suivant.

```
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. Exécutez list_asset_model.py depuis le terminal.

```
python3 list_asset_model.py
```

curl

> **Note**
>
> Vous devez installer Curl.

Pour obtenir la liste des modèles d'actifs à l'aide de curl

Exécutez la commande suivante depuis le 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"
```

Les résultats doivent avoir l'aspect suivant :

```
{
    "assetModelSummaries": [
        {
            "arn": "arn:aws:iotsitewise:{region}:{account-id}:asset-model/{asset-
model-id}",
            "creationDate": 1.669245291E9,
            "description": "This is a small example asset model",
            "id": "{asset-model-id}",
            "lastUpdateDate": 1.669249038E9,
            "name": "Some Metrics Model",
            "status": {
                "error": null,
                "state": "ACTIVE"
            }
        },
        .
        .
```

```
        .
    ],
    "nextToken": null
}
```

Backup et restauration des passerelles SiteWise Edge

Cette rubrique explique comment restaurer les passerelles SiteWise Edge et sauvegarder vos données métriques. Si vous rencontrez des problèmes liés à une passerelle SiteWise Edge défaillante sur le même ordinateur et que vous devez résoudre le problème, veuillez lire la AWS IoT SiteWise documentation Résolution des problèmes liés à la passerelle SiteWise Edge.

> **Note**
>
> Les conseils présentés dans cette rubrique concernent les passerelles SiteWise Edge installées sur la AWS IoT Greengrass V2 version 2.1.0 ou supérieure.

Sauvegardes quotidiennes des données métriques

La création d'une sauvegarde est importante si vous souhaitez transférer ou restaurer les données sur un nouvel ordinateur. La sauvegarde de vos données réduit considérablement le risque de perte de données d'exploitation lors d'un processus de transfert ou de restauration.

Le chemin du dossier influxdb est le suivant :

Linux

```
/greengrass/v2/work/aws.iot.SiteWiseEdgeProcessor/influxdb
```

Windows

```
C:\greengrass\v2\work\aws.iot.SiteWiseEdgeProcessor\influxdb
```

Nous vous recommandons de sauvegarder l'intégralité du dossier avec tout ce qui se trouve en dessous.

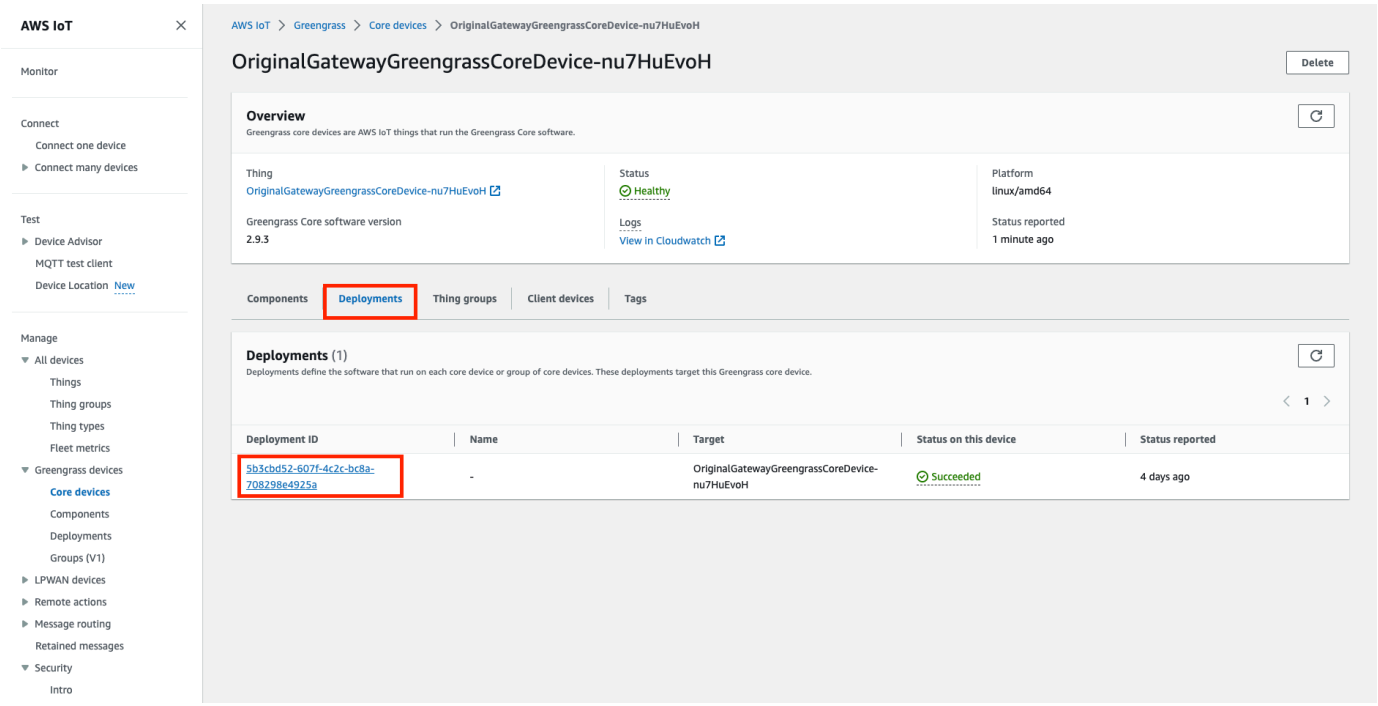
Nous vous recommandons de sauvegarder régulièrement vos données métriques depuis le 1.0 SiteWise Edge sur un disque dur externe ou sur le AWS cloud.

Restaurer une passerelle SiteWise Edge

Utilisez la procédure suivante pour restaurer une passerelle SiteWise Edge :

1. Utilisez le script d'installation téléchargé lors de la création de la passerelle SiteWise Edge pour restaurer la passerelle SiteWise Edge sur le nouvel ordinateur. Lisez la procédure d'installation du logiciel de passerelle SiteWise Edge sur votre appareil local pour configurer la passerelle SiteWise Edge.

   Si vous perdez ou ne trouvez pas le script d'installation, contactez AWS le Support client.
2. Une fois la passerelle SiteWise Edge installée, connectez-vous à la AWS IoT Greengrass console.
3. Pour redéployer les composants, accédez à Gérer, puis sous AWS IoT Greengrass Appareils, sélectionnez Appareils principaux.
4. Dans le tableau des appareils AWS IoT Greengrass principaux, sélectionnez le périphérique principal correspondant à votre passerelle SiteWise Edge.
5. Une fois sur la page de l'appareil, ouvrez l'onglet Déploiements et sélectionnez votre ID de déploiement, cela ouvrira la page Déploiements avec l'ID que vous avez sélectionné.



6. Une fois que vous êtes sur la page Déploiements, en haut à droite, appuyez sur le bouton Actions et sélectionnez l'option Réviser pour lancer un nouveau déploiement. Configurez le

déploiement. Si vous souhaitez conserver le déploiement tel quel, passez à la section Révision et déploiement.

7. Attendez que le statut de déploiement devienne le même`Completed`.

> **Note**
>
> Il faudra également quelques minutes pour que tous les composants de l' SiteWise Edge soient complètement configurés et opérationnels.

Restaurer AWS IoT SiteWise les données

Pour restaurer les données sur une nouvelle machine, procédez comme suit.

1. Copiez le `influxdb` dossier sur le nouvel ordinateur.
2. Arrêtez le SiteWise EdgeProcessor composant en exécutant la commande suivante dans votre 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. Localisez le chemin où vous avez sauvegardé vos données, puis exécutez la commande suivante :

   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. Redémarrez le SiteWiseEdgeProcessor composant :

   Linux

   ```
   sudo /greengrass/v2/bin/greengrass-cli component restart -n
   aws.iot.SiteWiseEdgeProcessor
   ```

   Windows

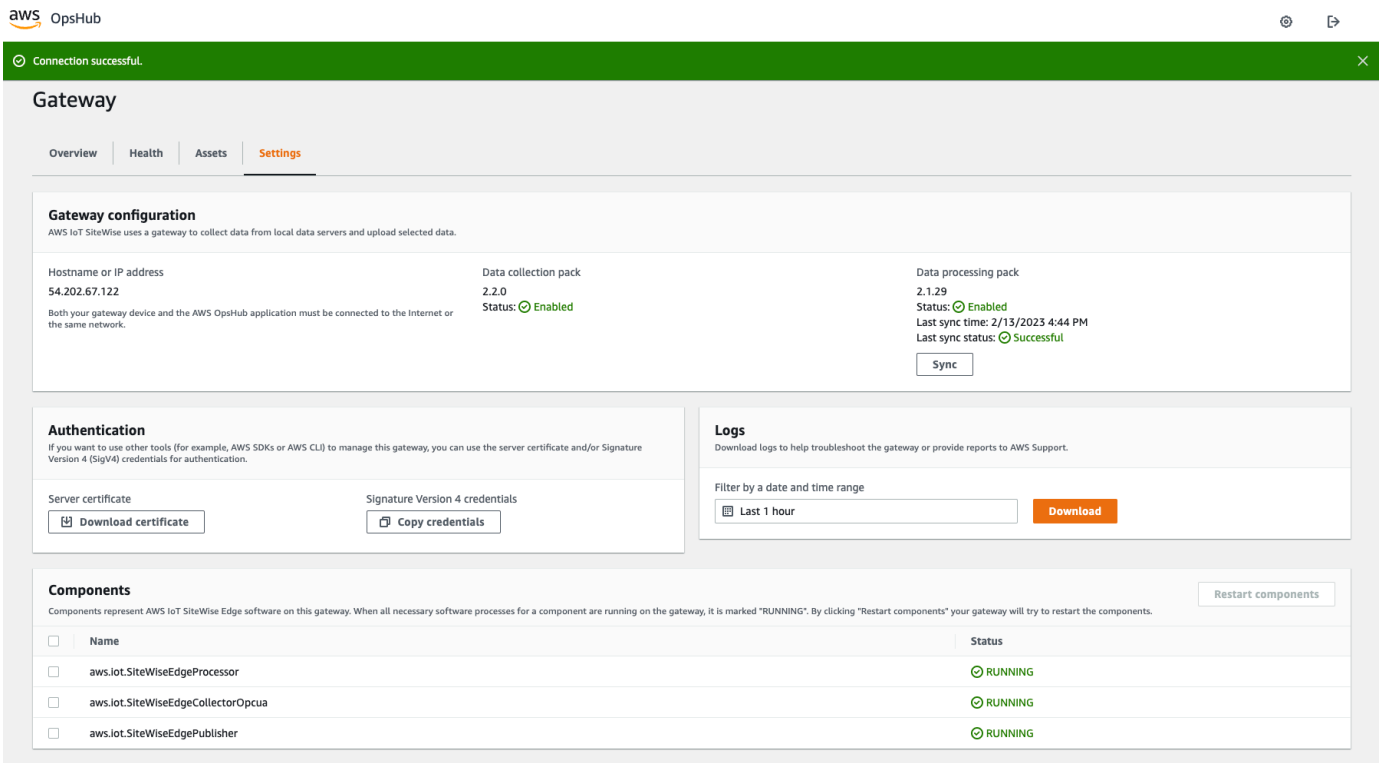
   ```
   C:\greengrass\v2\bin\greengrass-cli component restart -n
   aws.iot.SiteWiseEdgeProcessor
   ```

Validez les sauvegardes et restaurations réussies

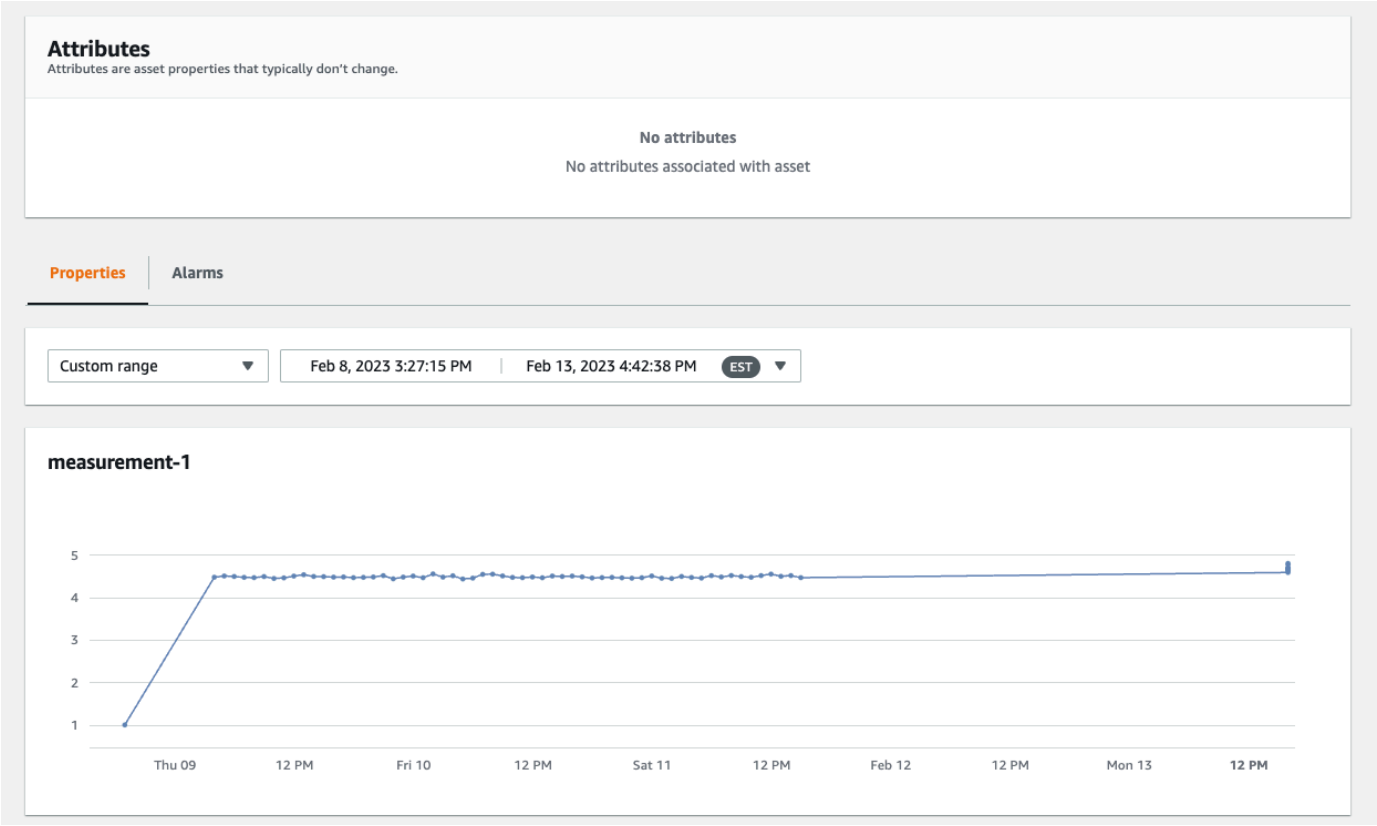
Utilisez cette procédure pour valider vos données sauvegardées et les restaurations de la passerelle SiteWise Edge.

> **Note**
>
> Cette procédure nécessite que vous ayez installé AWS OpsHub pour AWS IoT SiteWise. Pour plus d'informations, voir Gestion des passerelles SiteWise Edge à l'aide de AWS OpsHub for AWS IoT SiteWise.

1. Ouvert AWS OpsHub pour AWS IoT SiteWise.
2. Sur la page Paramètres d' SiteWise Edge Gateway, vérifiez l'état de chaque composant répertorié dans le tableau des composants. Vérifiez que la couleur d'état est verte et que l'affichage affiche RUNNING.



3. Validez vos anciennes données sur le tableau de bord du portail pour vérifier que les données passées et les nouvelles données sont correctement configurées. Il y aura un temps d'arrêt entre les données passées et les nouvelles données. Vous devriez, sauf pour voir une durée pendant laquelle aucun point de données n'est collecté.



Si vous rencontrez des problèmes lors de la sauvegarde ou de la restauration d'une passerelle SiteWise Edge, consultez les rubriques de résolution des problèmes suivantes. Résolution des problèmes liés à une passerelle AWS IoT SiteWise Edge.

Configuration des passerelles SiteWise Edge ()AWS IoT Greengrass Version 1

> **Note**
>
> SiteWise Les passerelles Edge exécutées ne AWS IoT Greengrass V1 sont disponibles que si vous avez commencé à utiliser cette fonctionnalité avant le 29 juillet 2021. Dans le cas contraire, vous configurez les passerelles SiteWise Edge qui s'exécutent sur AWS IoT Greengrass V2.

Vous pouvez envoyer des données industrielles à AWS IoT SiteWise l'aide d'une passerelle SiteWise Edge pour télécharger des données depuis des équipements industriels. La passerelle SiteWise

Edge sert d'intermédiaire entre AWS IoT SiteWise et vos équipements industriels de données. AWS IoT SiteWise fournit des AWS IoT Greengrass composants que vous pouvez déployer sur n'importe quel appareil pouvant être exécuté AWS IoT Greengrass pour configurer une passerelle SiteWise Edge. AWS IoT SiteWise prend en charge la liaison avec le protocole de serveur OPC-UA.

Si vous avez des passerelles AWS IoT SiteWise Edge qui s'exécutent sur AWS IoT Greengrass V1, vous pouvez mettre à niveau vos passerelles SiteWise Edge vers. AWS IoT Greengrass V2 Pour plus d'informations, consultez les instructions relatives à la mise à niveau des passerelles SiteWise Edge de AWS IoT Greengrass V1 vers AWS IoT Greengrass V2.

Rubriques

- Choix d'un AWS IoT Greengrass V1 SiteWise périphérique de passerelle Edge
- Configuration d'une passerelle AWS IoT Greengrass V1 SiteWise Edge
- Configuration des sources de données sur les passerelles AWS IoT Greengrass V1 SiteWise Edge

Choix d'un AWS IoT Greengrass V1 SiteWise périphérique de passerelle Edge

Choisissez un appareil local qui convient le mieux à votre activité industrielle. Vous pouvez configurer une passerelle SiteWise Edge sur n'importe quel appareil capable de fonctionner AWS IoT Greengrass. Tous les appareils locaux doivent répondre aux exigences suivantes :

- Supporte le logiciel AWS IoT Greengrass Core v1.10.2 ou version ultérieure. Pour plus d'informations, consultez la section Plateformes prises en charge et exigences dans le Guide du AWS IoT Greengrass Version 1 développeur.
- Dispose d'au moins 4 Go de RAM.
- Ayez au moins 10 Go d'espace disque libre.
- Prend en charge une machine virtuelle Java 8 (JVM).

Si vous envisagez de traiter des données en périphérie AWS IoT SiteWise, votre appareil local doit également répondre aux exigences suivantes :

- Dispose d'un processeur quadricœur x86 64 bits.
- Dispose d'au moins 16 Go de RAM.
- Dispose d'au moins 32 Go de RAM si vous utilisez Windows.

- Disposait d'au moins 256 Go d'espace disque libre.

L'espace disque requis pour la mise en cache des données pour une connectivité Internet intermittente dépend des facteurs suivants :

- Nombre de flux de données chargés
- Points de données par flux de données par seconde
- Taille de chaque point de données
- Vitesses de communication
- Temps d'arrêt du réseau attendu

La capacité de calcul requise pour interroger et charger les données dépend des facteurs suivants :

- Nombre de flux de données chargés
- Points de données par flux de données par seconde

Configuration d'une passerelle AWS IoT Greengrass V1 SiteWise Edge

Une passerelle AWS IoT SiteWise Edge sert d'intermédiaire entre votre équipement industriel et AWS IoT SiteWise. Vous pouvez déployer le logiciel de passerelle SiteWise Edge sur n'importe quel appareil capable de fonctionner AWS IoT Greengrass. Pour plus d'informations, consultez Choix d'un AWS IoT Greengrass V1 SiteWise périphérique de passerelle Edge.

Vous pouvez AWS IoT SiteWise activer le traitement des données localement sur vos appareils Edge en utilisant le pack de traitement des données sur votre passerelle SiteWise Edge. Vous le faites lorsque vous ajoutez votre passerelle SiteWise Edge à AWS IoT SiteWise. Pour plus d'informations sur le traitement des données en périphérie, consultezthe section called "Permettre le traitement des données de pointe".

> **Note**
>
> Nous vous recommandons d'effectuer les étapes suivantes avec une personne disposant des droits d'accès d'administrateur informatique à vos réseaux local et d'entreprise. Ces étapes peuvent nécessiter une personne connaissant votre équipement industriel et habilitée à configurer les paramètres du pare-feu.

Rubriques

- Configuration de l'environnement de passerelle SiteWise Edge
- Création d'une politique et d'un rôle IAM
- Configuration d'un AWS IoT Greengrass groupe
- Configuration du AWS IoT SiteWise connecteur
- Ajout de la passerelle SiteWise Edge à AWS IoT SiteWise

Configuration de l'environnement de passerelle SiteWise Edge

Dans cette procédure, vous allez installer AWS IoT Greengrass et configurer votre passerelle SiteWise Edge à utiliser avec AWS IoT SiteWise.

> **Note**
>
> Cette section contient des instructions pour installer des paquets à l'aide de la commande `apt`. Ceci s'applique aux systèmes exécutant Ubuntu ou similaire. Si vous n'utilisez pas un système similaire, consultez la documentation de votre distribution et utilisez le programme d'installation recommandé.

Pour configurer la passerelle SiteWise Edge

1. Le cas échéant, modifiez les paramètres du BIOS de la passerelle SiteWise Edge comme suit.
   a. Assurez-vous que la passerelle SiteWise Edge redémarre automatiquement après une éventuelle panne de courant, le cas échéant.
   b. Assurez-vous que la passerelle SiteWise Edge ne sera pas mise en veille prolongée ou ne dormira pas, le cas échéant.
2. Assurez-vous que la passerelle SiteWise Edge est connectée à Internet.
3. (Facultatif) Pour utiliser la passerelle SiteWise Edge sans souris, clavier et écran, procédez comme suit pour la configurer `ssh` sur la passerelle SiteWise Edge :
   a. Si vous n'avez pas déjà installé le package SSH, exécutez la commande suivante.

      ```
      sudo apt install ssh
      ```

   b. Exécutez la commande suivante.

```
service ssh status
```

c. Pour confirmer que le serveur SSH est en cours d'exécution, recherchez `Active: active (running)` dans la sortie.

d. Appuyez sur Q pour quitter.

Exécutez la commande suivante pour utiliser SSH pour vous connecter à la passerelle SiteWise Edge depuis un autre ordinateur. *Remplacez le nom d'utilisateur par le nom d'utilisateur et l'adresse IP par l'adresse IP de la passerelle SiteWise Edge.*

```
ssh username@IP
```

Vous pouvez utiliser l'argument `-p port-number` pour vous connecter à un port autre que le port 22 par défaut.

4. Téléchargez et installez le logiciel AWS IoT Greengrass Core v1.10.2 ou version ultérieure, puis créez un AWS IoT Greengrass groupe pour votre passerelle SiteWise Edge. Pour ce faire, suivez les instructions de la section Premiers pas avec AWS IoT Greengrass dans le Guide du développeur AWS IoT Greengrass .

   Nous vous recommandons d'exécuter le script AWS IoT Greengrass device setup pour une mise en route rapide. Si vous souhaitez examiner les AWS IoT Greengrass exigences et les processus de plus près, vous pouvez suivre les étapes des modules 1 et 2 pour les configurer AWS IoT Greengrass.

   > **Important**
   >
   > Passez en revue les AWS régions dans lesquelles le AWS IoT SiteWise support est pris en charge. Lorsque vous choisissez une région pour AWS IoT Greengrass, assurez-vous que la région prend également en charge AWS IoT SiteWise. Dans le cas contraire, vous ne pouvez pas connecter votre passerelle SiteWise Edge à AWS IoT SiteWise.

   Avant de passer à l'étape suivante, le logiciel AWS IoT Greengrass Core doit être installé sur votre passerelle SiteWise Edge.

5. Exécutez les commandes suivantes pour installer Java 8.

```
sudo apt update
      sudo apt install openjdk-8-jre
```

Le logiciel de passerelle SiteWise Edge que vous installerez ultérieurement dans ce guide utilise un environnement d'exécution Java 8.

6. Exécutez les commandes suivantes pour vérifier que l'installation de Java a réussi.

```
java -version
```

7. Le logiciel de AWS IoT Greengrass base suppose un `java8` répertoire. Exécutez la commande suivante pour lier votre installation Java à ce répertoire `java8`.

```
sudo ln -s /usr/bin/java /usr/bin/java8
```

8. Exécutez la commande suivante pour créer un répertoire de `/var/sitewise` données et octroyer les `ggc_user` autorisations pour ce répertoire. AWS IoT SiteWise stocke les données dans ce répertoire. Vous l'avez créé `ggc_user` lorsque vous l'avez configuré AWS IoT Greengrass plus tôt dans cette procédure.

```
sudo mkdir /var/sitewise
      sudo chown ggc_user /var/sitewise
      sudo chmod 700 /var/sitewise
```

`/var/sitewise`Il s'agit du répertoire par défaut qui AWS IoT SiteWise utilise. Vous pouvez personnaliser le chemin du répertoire (par exemple, le `/var/sitewise` remplacer par/ `var/`*`custom`*`/`*`path`*`/`), mais cela nécessite des étapes supplémentaires après la création de la passerelle SiteWise Edge. Pour plus d'informations, consultez l'étape 6 dans Configuration du AWS IoT SiteWise connecteur.

9. Si nécessaire, demandez à votre administrateur informatique d'ajouter les points de terminaison et ports suivants à votre liste d'autorisation du réseau local :

   - Ports 443, 8443 et 8883

   > **Important**
   >
   > Vous pouvez configurer AWS IoT Greengrass Core pour utiliser uniquement le port 443 pour toutes les communications réseau. Pour de plus amples informations,

veuillez consulter Connexion sur le port 443 ou via un proxy réseau ans le Guide du développeur AWS IoT Greengrass .

- Adresse IP de votre passerelle SiteWise Edge (port 443). Pour obtenir l'adresse IP, exécutez la commande `ip address` ou `ifconfig` et notez la valeur `inet` (par exemple, `203.0.113.0`).
- Le point AWS IoT SiteWise de terminaison des données : `data.iotsitewise.`*`region`*`.amazonaws.com` (port 443).
- Les AWS points de terminaison suivants utilisés par la passerelle SiteWise Edge. Vous trouverez ceux-ci dans le fichier `/`*`greengrass-root`*`/config/config.json`. Remplacez *`greengrass-root`* par la racine de votre installation AWS IoT Greengrass .
  - ggHost : `greengrass-ats.iot.`*`region`*`.amazonaws.com` (ports 443, 8443 et 8883).
  - iotHost : *`prefix`*`-ats.iot.`*`region`*`.amazonaws.com` (ports 443, 8443 et 8883).

  Pour plus d'informations, consultez Points de terminaison et quotas AWS IoT Greengrass.

10. Si le logiciel AWS IoT Greengrass Core n'est pas déjà en cours d'exécution, exécutez la commande suivante pour démarrer le logiciel AWS IoT Greengrass Core. Remplacez *`greengrass-root`* par la racine de votre installation. AWS IoT Greengrass La racine *`greengrass-root`* par défaut est `/greengrass`.

    ```
    cd /greengrass-root/ggc/core
          sudo ./greengrassd start
    ```

    Vous devriez voir ce message : `Greengrass successfully started with PID:` *`some-PID-number`*

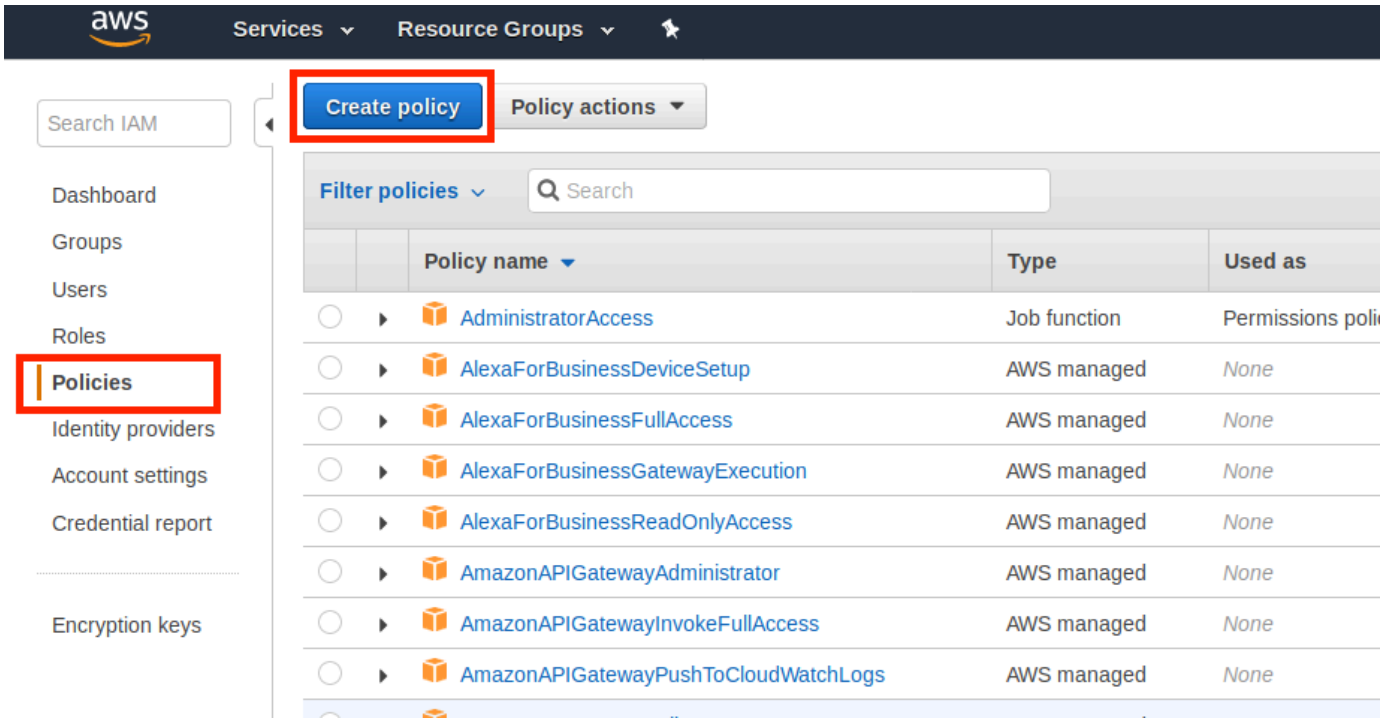
11. Configurez le logiciel AWS IoT Greengrass Core pour qu'il démarre automatiquement lorsque votre passerelle SiteWise Edge est activée. Consultez la documentation du système d'exploitation de votre passerelle SiteWise Edge.

Création d'une politique et d'un rôle IAM

Vous devez créer une politique et un rôle AWS Identity and Access Management (IAM) pour autoriser la passerelle SiteWise Edge à accéder en votre AWS IoT SiteWise nom.

Pour créer une politique et un rôle IAM

1. Accédez à la Console IAM.
2. Dans le volet de navigation, sélectionnez Politiques, puis Créer une politique.



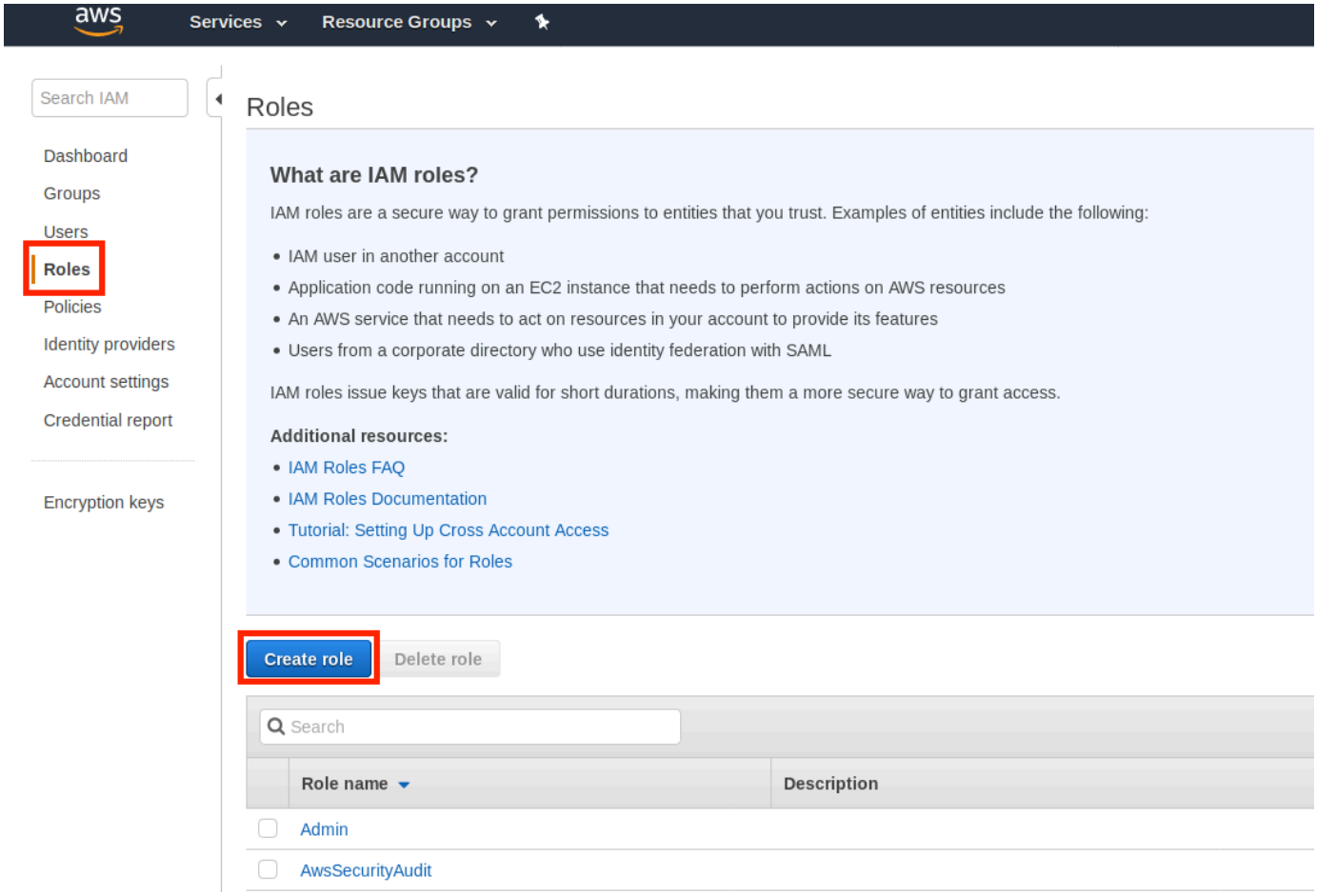
3. Sur l'onglet JSON, supprimez le contenu actuel du champ de stratégie, puis collez les informations suivantes dans le champ.

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

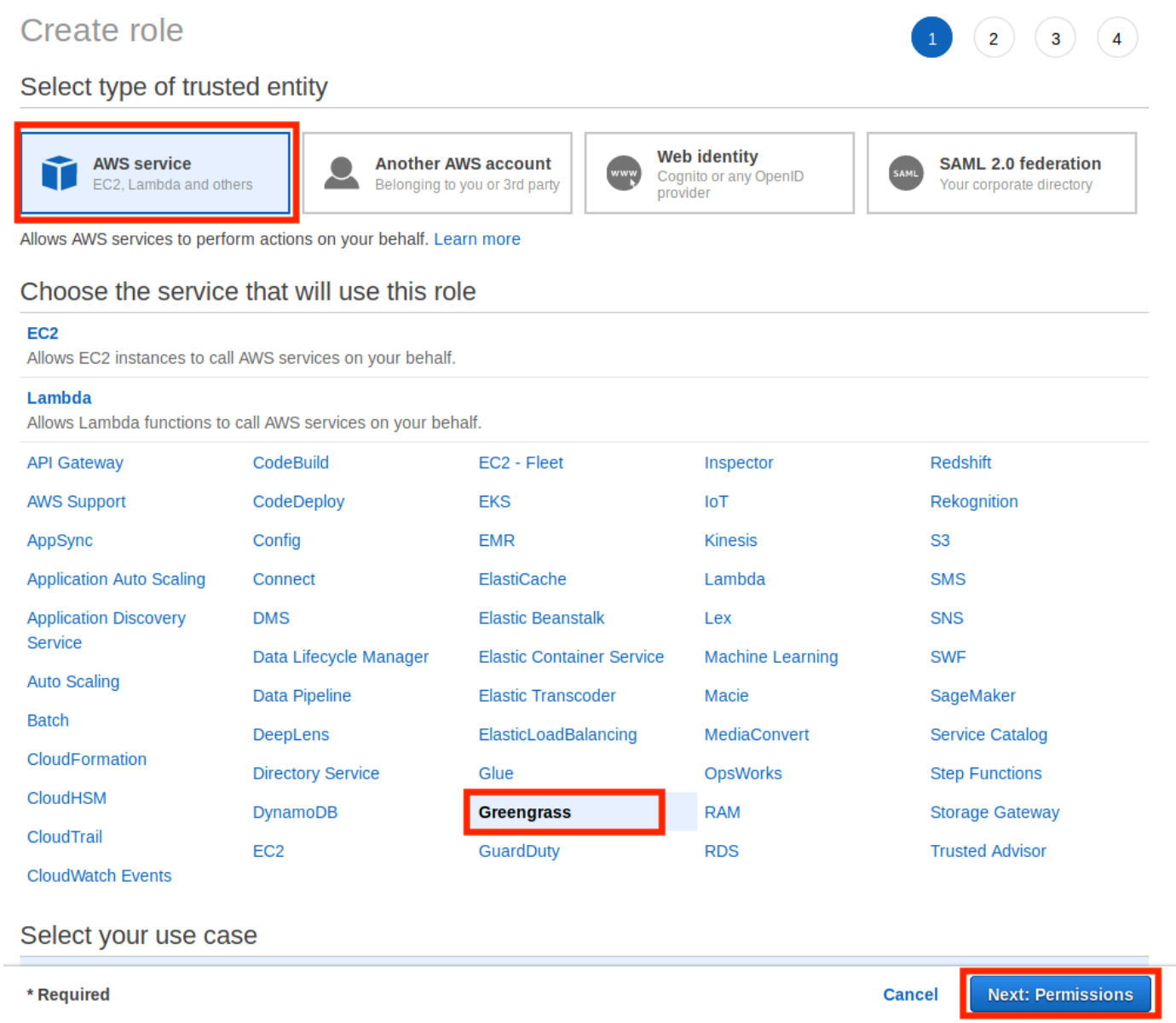
> **Note**
>
> Pour améliorer la sécurité, vous pouvez spécifier un chemin hiérarchique des AWS IoT SiteWise actifs dans la `Condition` propriété. L'exemple suivant est une stratégie d'approbation qui spécifie un chemin de hiérarchie de ressource.

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

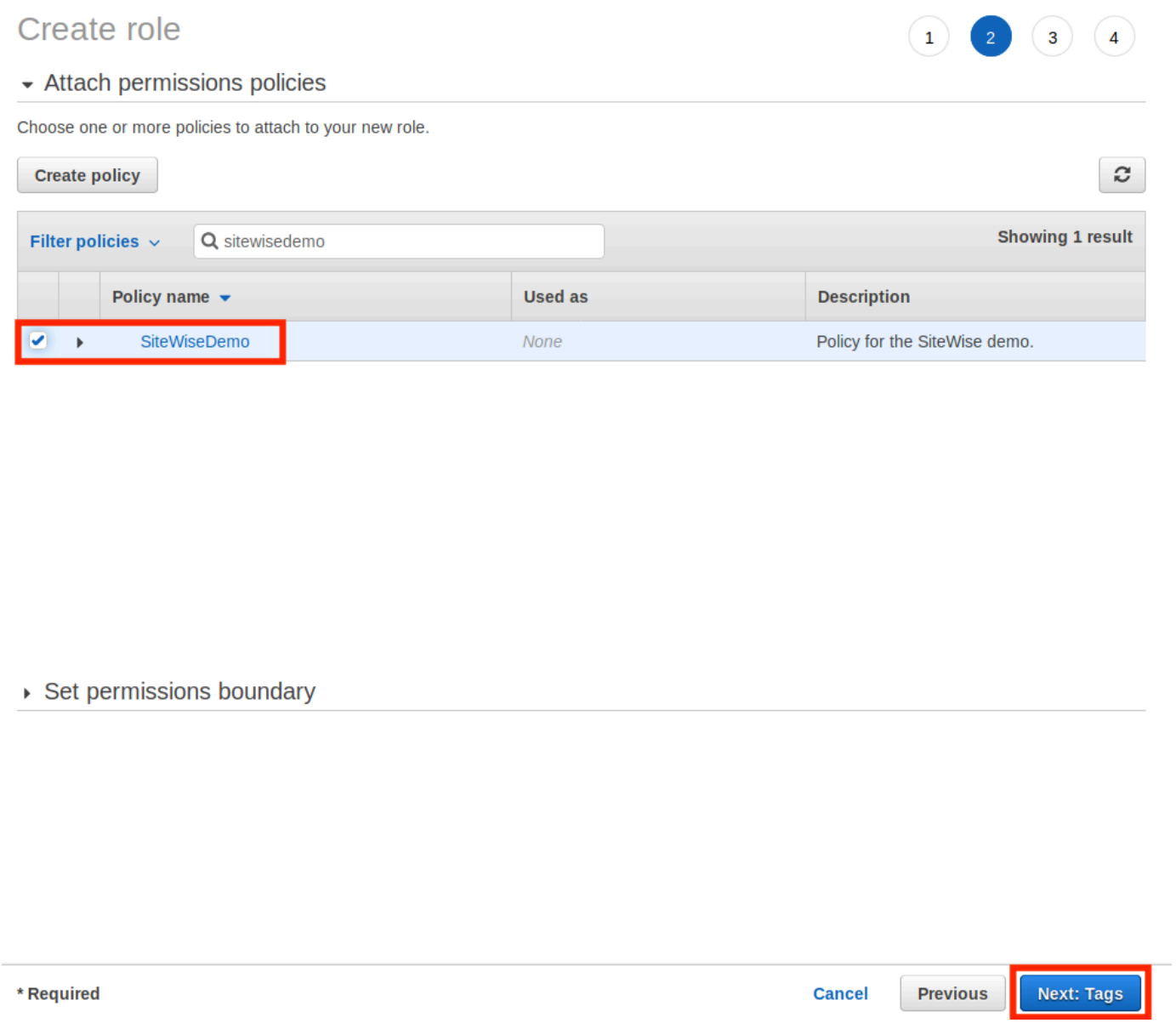
4. Choisissez Examiner une politique.
5. Entrez un nom et une description pour la stratégie, puis choisissez Créer une stratégie.
6. Dans le volet de navigation, sélectionnez Rôles, puis Créer un rôle.



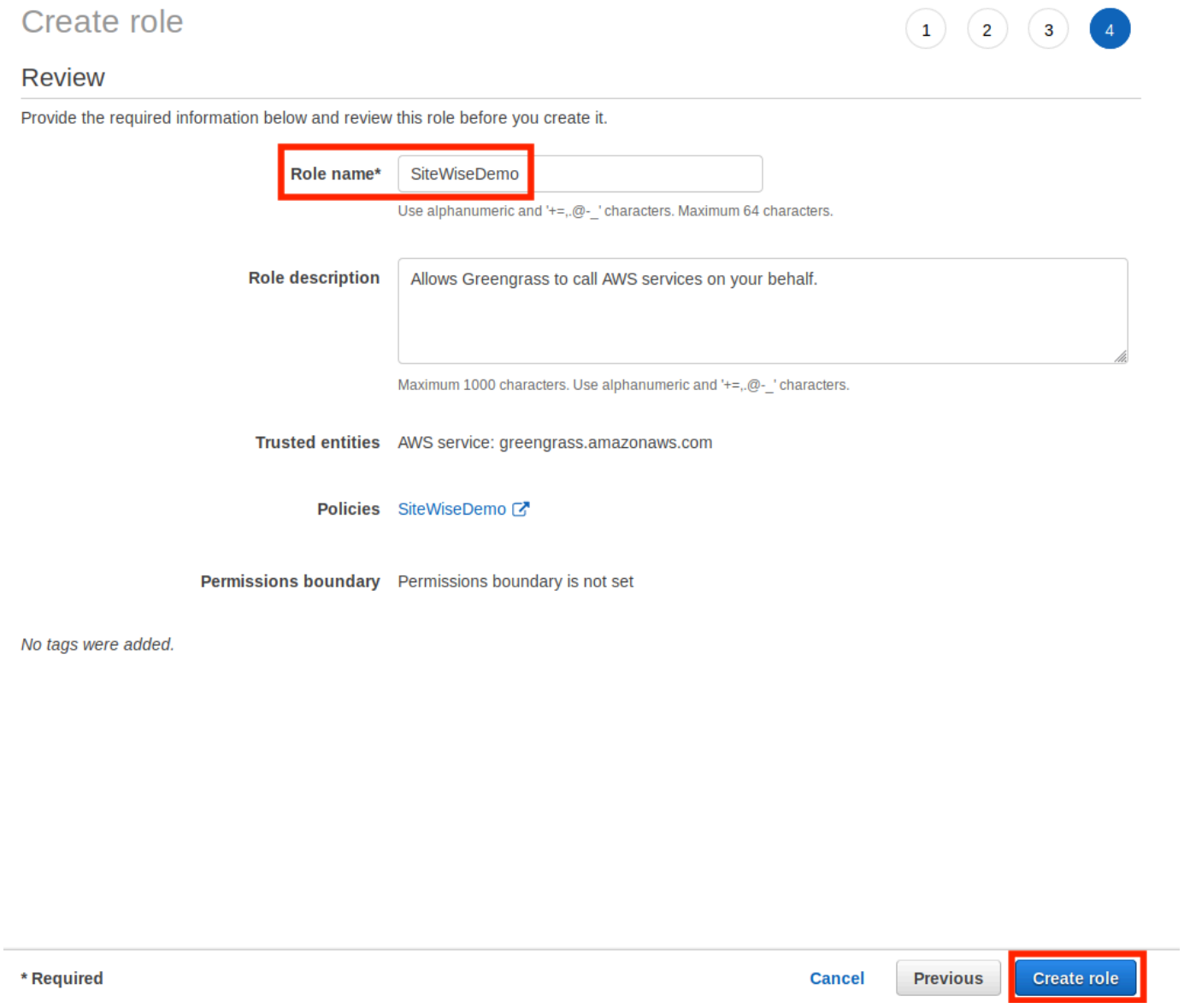
7. Sous Select type of trusted entity (Sélectionner le type d'entité approuvée), choisissez service AWS . Sous Choose the service that will use this role (Choisir le service qui utilisera ce rôle), choisissez Greengrass comme service qui utilisera le rôle, puis Next: Permissions (Suivant : Autorisations).



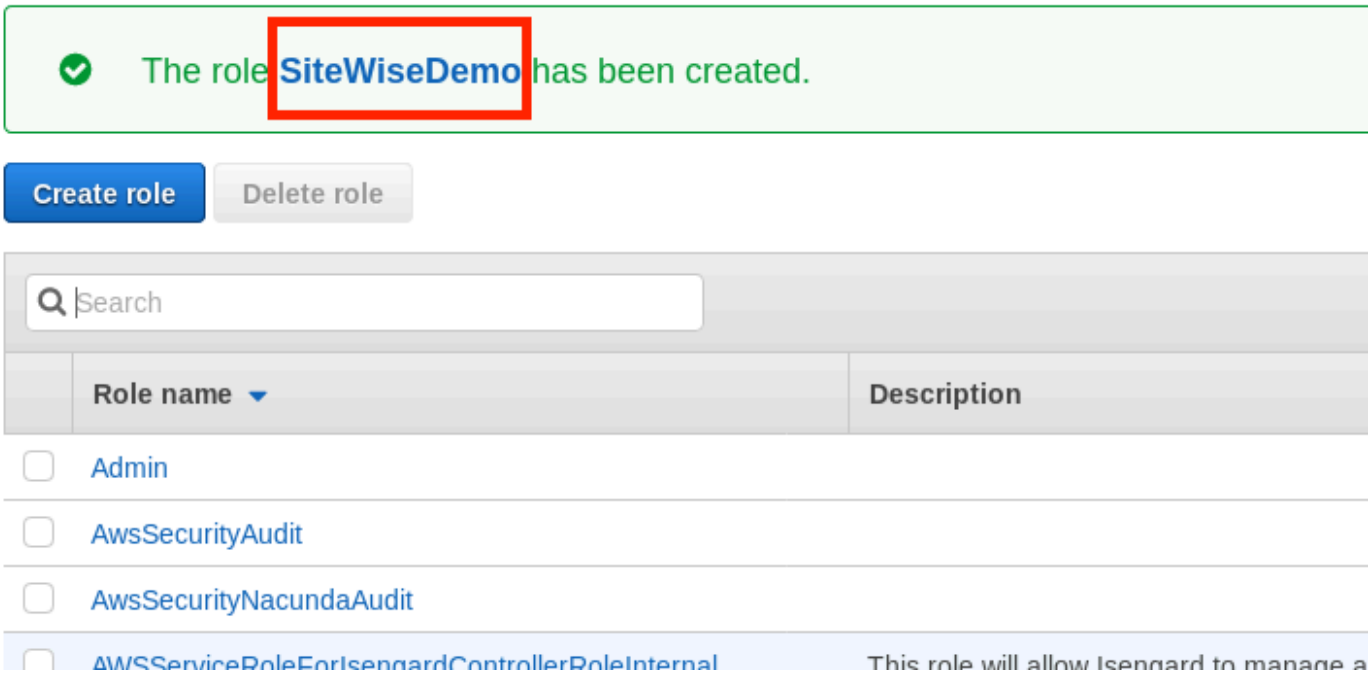
8. Recherchez la politique que vous avez créée, cochez la case, puis choisissez Next : Tags.



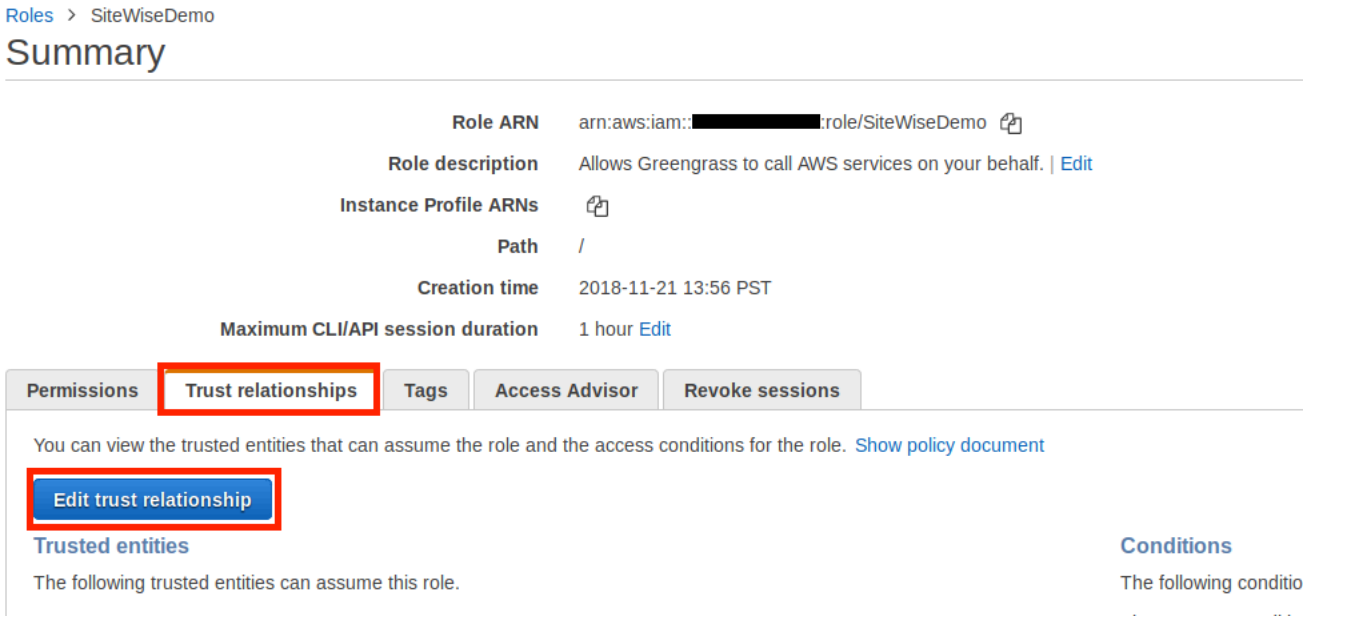
9. (Facultatif) Ajoutez des balises à votre rôle, puis choisissez Suivant : Vérification.
10. Entrez un nom et une description pour le rôle, puis choisissez Créer un rôle.



11. Dans la bannière verte, choisissez le lien vers votre nouveau rôle. Vous pouvez également utiliser le champ de recherche pour trouver le rôle.



12. Sélectionnez l'onglet Relations d'approbation, puis Modifier la relation d'approbation.



13. Remplacez le contenu actuel du champ de stratégie par ce qui suit, puis choisissez Mettre à jour la stratégie de confiance.

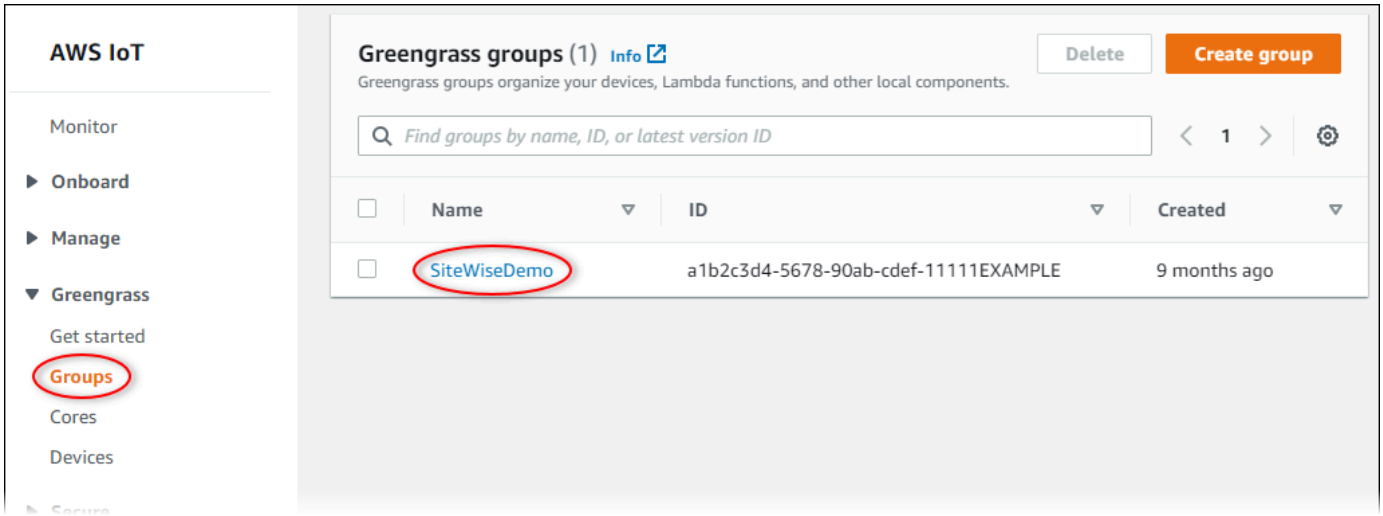
```
{
        "Version": "2012-10-17",
        "Statement": [
          {
            "Effect": "Allow",
```

```
            "Principal": {
              "Service": "greengrass.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
          }
        ]
      }
```

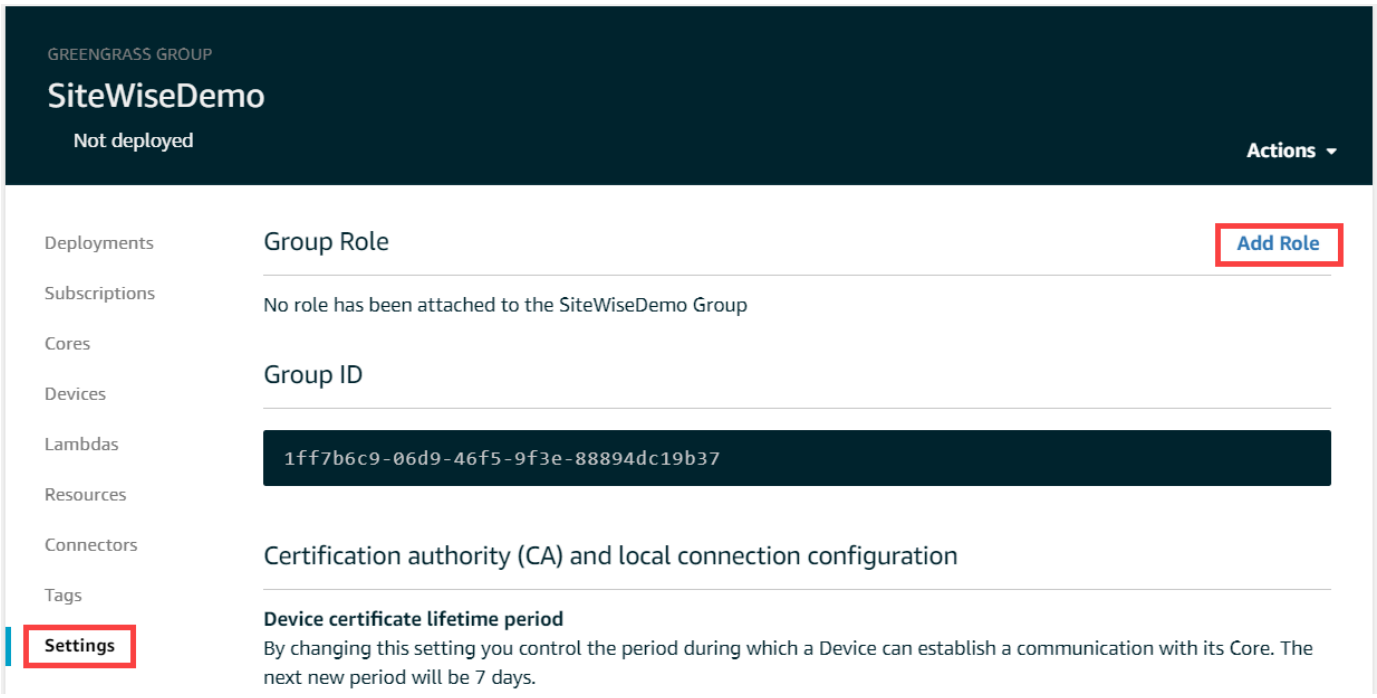
Configuration d'un AWS IoT Greengrass groupe

Pour associer un rôle IAM à un groupe et activer le gestionnaire de flux

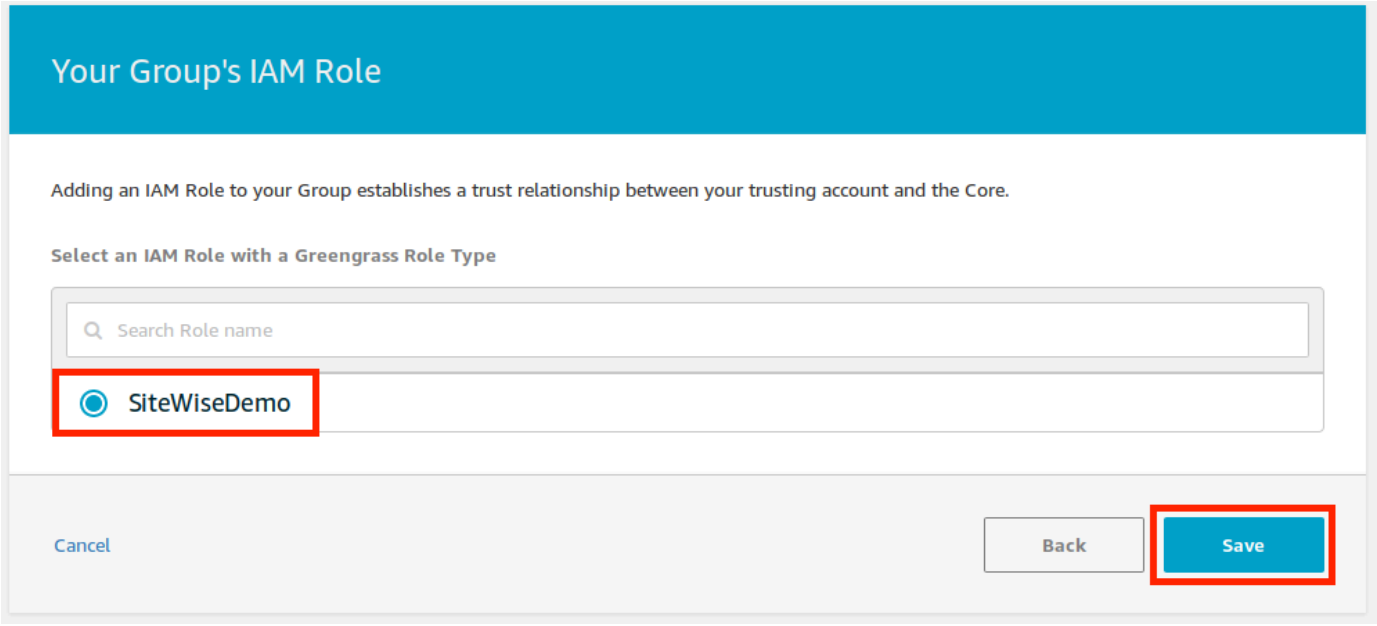
1. Accédez à la console AWS IoT Greengrass.
2. Dans le panneau de navigation de gauche, sous Greengrass, choisissez Groupes, puis choisissez le groupe que vous avez créé dans Configuration de l'environnement de passerelle SiteWise Edge.



3. Dans le panneau de navigation de gauche, choisissez Paramètres. Dans la section Rôle de groupe, choisissez Ajouter un rôle.



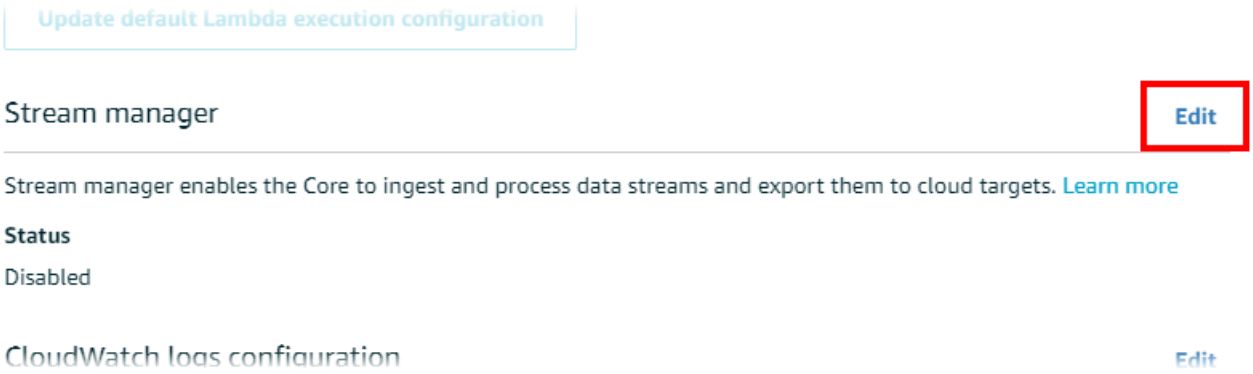
4. Choisissez le rôle que vous avez créé dans Création d'une politique et d'un rôle IAM, puis choisissez Enregistrer.



5. Dans la page Paramètres de la section Gestionnaire de flux, choisissez Modifier.

   Le gestionnaire de flux est une fonctionnalité AWS IoT Greengrass qui permet à votre AWS IoT Greengrass Core de diffuser des données vers le AWS cloud. SiteWise Les passerelles Edge nécessitent que le gestionnaire de flux soit activé. Pour plus d'informations, consultez la

section Gérer les flux de données sur le AWS IoT Greengrass Core dans le guide du AWS IoT Greengrass Version 1 développeur.



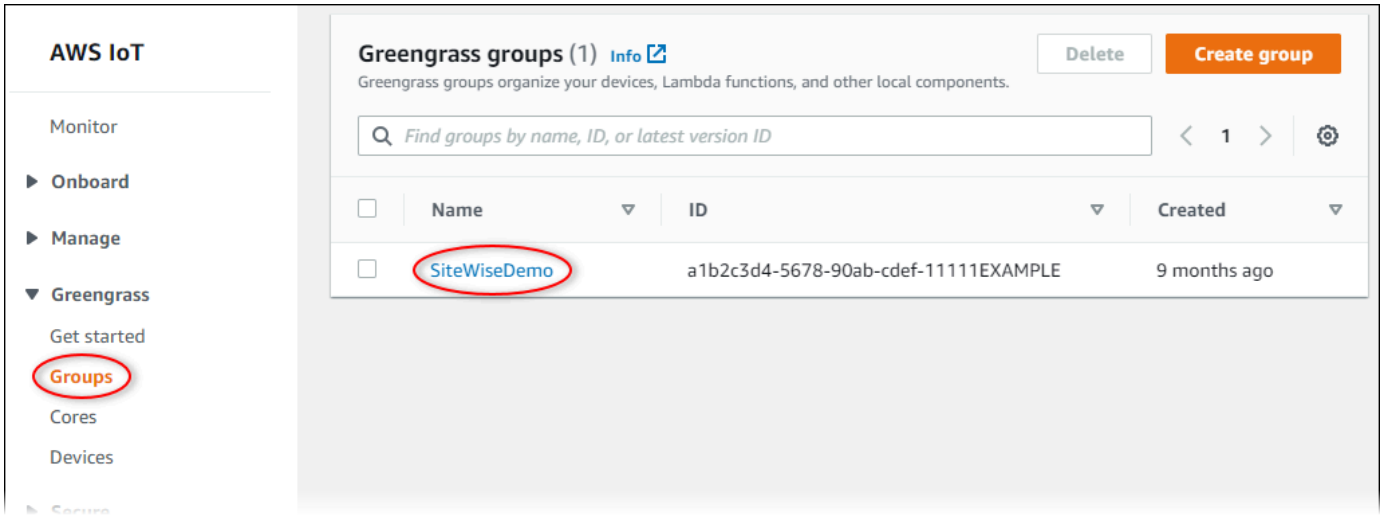
6. Choisissez Activer, puis Enregistrer.
7. Dans le coin supérieur gauche, choisissez Services pour vous préparer à l'étape suivante.

Configuration du AWS IoT SiteWise connecteur

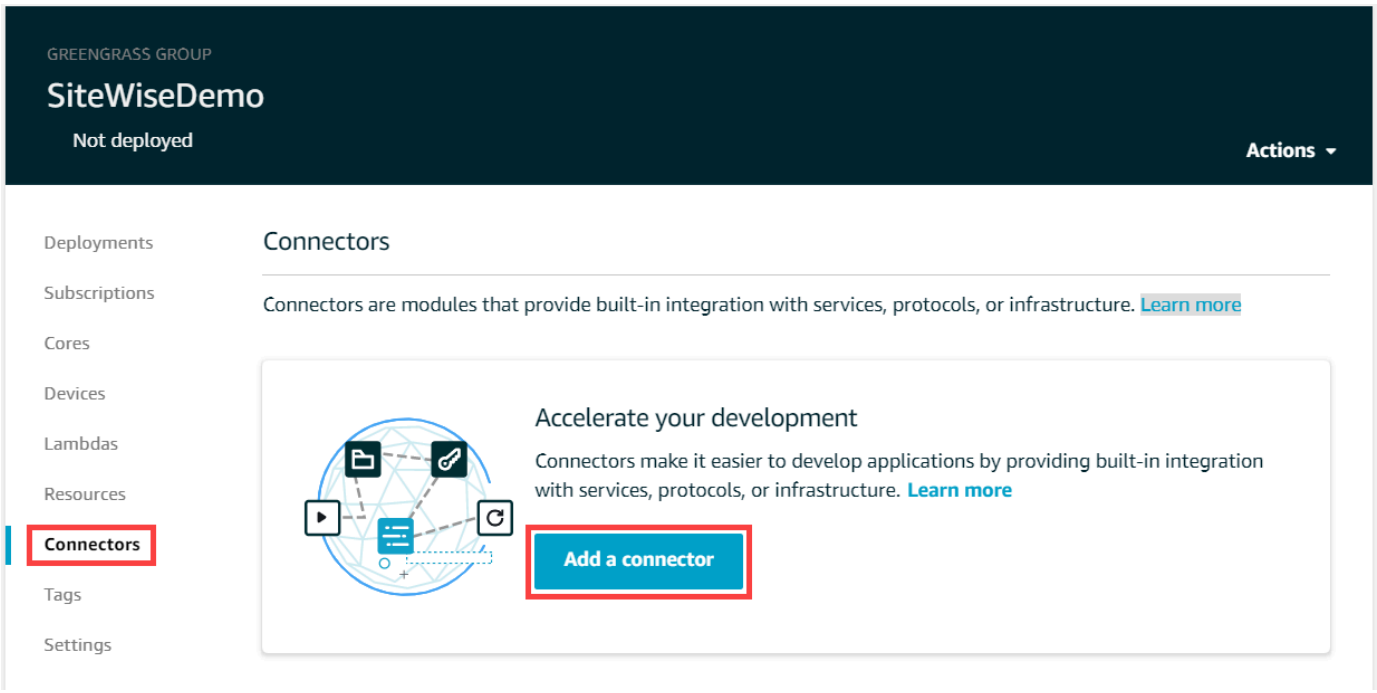
Dans cette procédure, vous allez configurer le AWS IoT SiteWise connecteur sur votre groupe Greengrass. Les composants sont des modules prédéfinis qui accélèrent le cycle de développement pour les scénarios de périphérie courants. Pour plus d'informations, consultez la section AWS IoT Greengrass Connecteurs dans le Guide du AWS IoT Greengrass Version 1 développeur.

Pour configurer le AWS IoT SiteWise connecteur

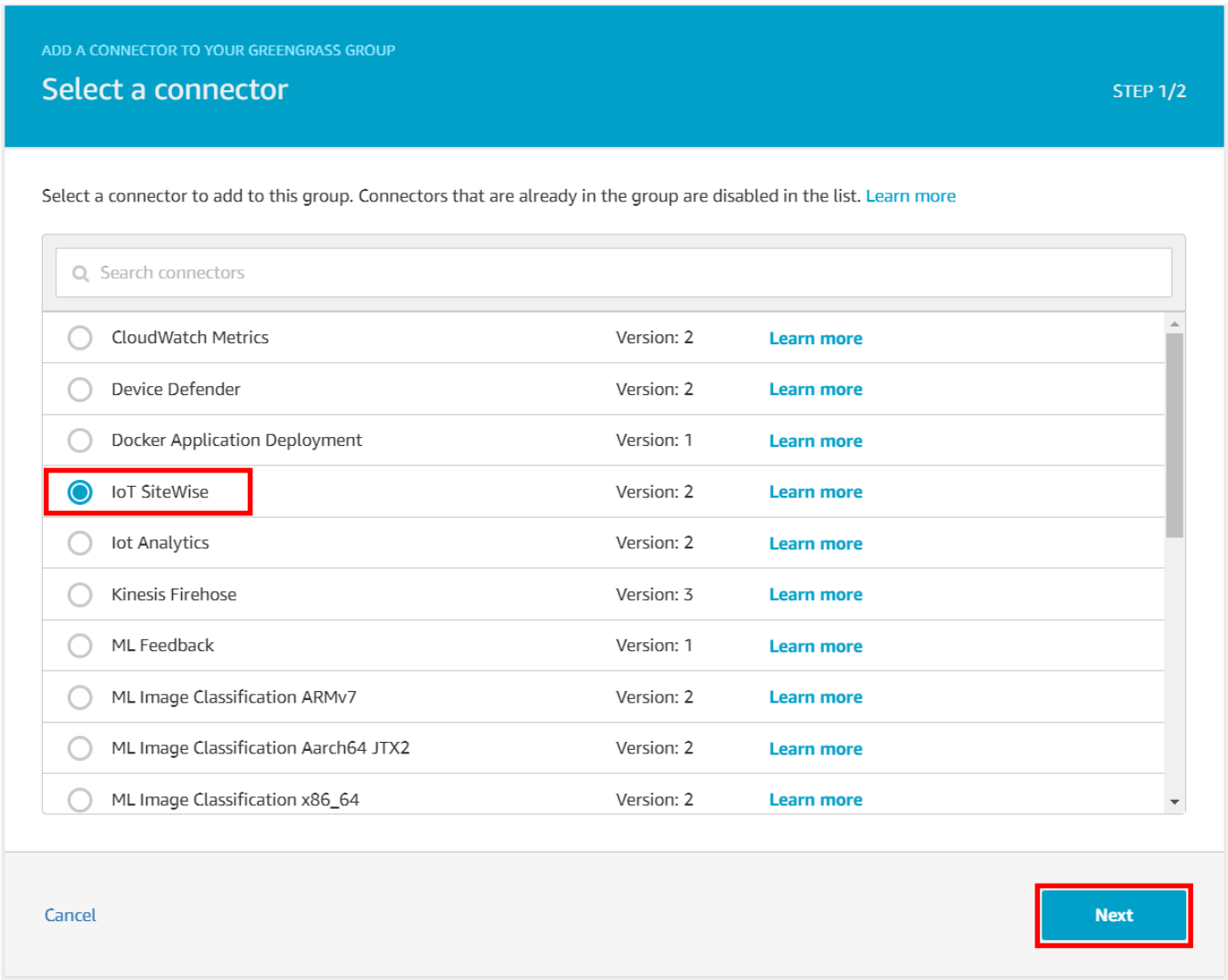
1. Accédez à la console AWS IoT Greengrass.
2. Dans le panneau de navigation de gauche, sous Greengrass, choisissez Groupes, puis choisissez le groupe que vous avez créé dans Configuration de l'environnement de passerelle SiteWise Edge.



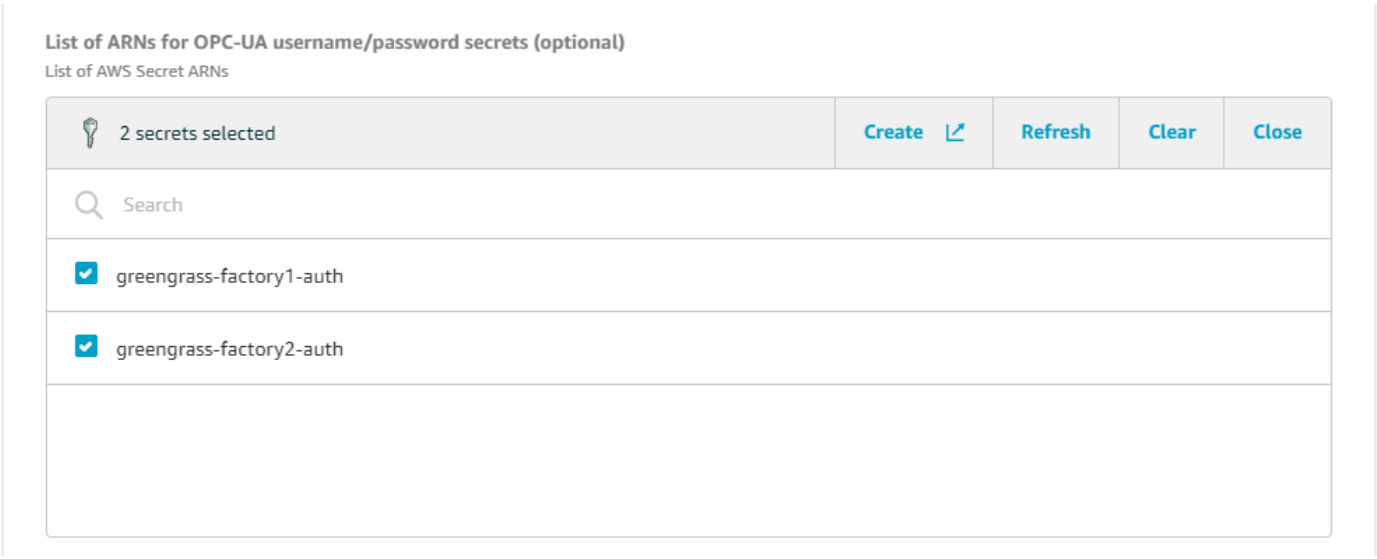
3. Dans la page de navigation de gauche, choisissez Connecteurs. Sur la page Connecteurs choisissez Ajouter un connecteur.



4. Choisissez IoT dans SiteWise la liste, puis cliquez sur Next.



5. Si votre serveur nécessite une authentification, vous pouvez créer des AWS Secrets Manager secrets à l'aide du nom d'utilisateur et du mot de passe du serveur. Ensuite, vous pouvez associer chaque secret à votre groupe Greengrass et le choisir sous Liste des ARN pour les secrets de nom d'utilisateur/mot de passe. Pour de plus amples informations sur la création et la configuration du rôle, veuillez consulter Configuration de l'authentification source. Vous pouvez également ajouter des secrets à votre connecteur ultérieurement.



6. Si vous avez configuré votre passerelle SiteWise Edge avec un chemin différent de celui-ci/`var/sitewise`, entrez ce chemin pour le chemin de stockage local.
7. (Facultatif) Entrez la taille maximale du tampon disque pour le connecteur. Si le AWS IoT Greengrass cœur perd la connexion au AWS Cloud, le connecteur met en cache les données jusqu'à ce qu'il puisse se connecter correctement. Si la taille du cache dépasse la taille maximale du tampon disque, le connecteur supprime les données les plus anciennes de la file d'attente.
8. Choisissez Ajouter.
9. Dans le coin supérieur droit de la page, dans le menu Actions choisissez Déployer.
10. Choisissez Détection automatique pour démarrer le déploiement.

    Si le déploiement échoue, choisissez à nouveau Déployer . Si le déploiement continue d'échouer, veuillez consulter Dépannage du déploiement AWS IoT Greengrass.

Ajout de la passerelle SiteWise Edge à AWS IoT SiteWise

Dans cette procédure, vous ajoutez le groupe Greengrass de votre passerelle SiteWise Edge à. AWS IoT SiteWise Après avoir enregistré votre passerelle SiteWise Edge auprès de celle-ci AWS IoT SiteWise, le service peut déployer les configurations de vos sources de données sur votre passerelle SiteWise Edge.

Pour ajouter la passerelle SiteWise Edge à AWS IoT SiteWise

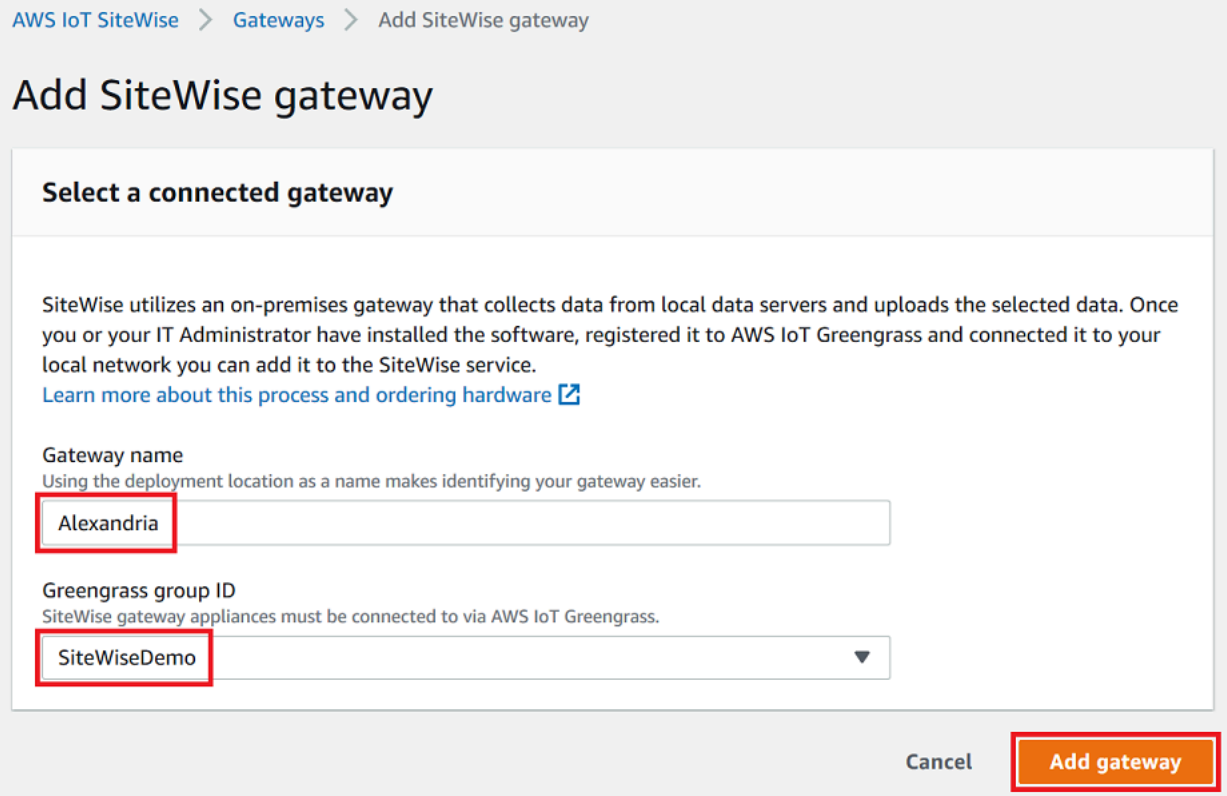
1. Accédez à la console AWS IoT SiteWise.
2. Choisissez Add gateway (Ajouter une passerelle).

3. Sur la page Ajouter une SiteWise passerelle, procédez comme suit :

   a. Entrez un nom pour la passerelle SiteWise Edge. Pensez à inclure l'emplacement de la passerelle SiteWise Edge dans le nom afin de pouvoir l'identifier facilement.

   b. Pour l'ID de groupe Greengrass, choisissez le groupe Greengrass que vous avez créé précédemment.

      Example



   c. (Facultatif) Pour les fonctionnalités Edge, sélectionnez Data processing pack. Cela permet la communication entre votre passerelle SiteWise Edge et tous les modèles d'actifs et actifs configurés pour la périphérie. Pour plus d'informations, consultez the section called "Permettre le traitement des données de pointe".

      > **Important**
      >
      > Si vous ajoutez le pack de traitement des données à votre passerelle SiteWise Edge, vous devez configurer et déployer le connecteur SiteWise Edge sur votre AWS IoT Greengrass groupe. Suivez les étapes suivantes.

   d. Choisissez Add gateway (Ajouter une passerelle).

4. Si vous ajoutez le pack de traitement des données à votre passerelle SiteWise Edge, configurez et déployez le connecteur du processeur de AWS IoT SiteWise données sur votre AWS IoT Greengrass groupe. Suivez les étapes décrites the section called "Configuration du AWS IoT SiteWise connecteur" pour configurer le connecteur du processeur de AWS IoT SiteWise données :

   a. Pour Sélectionner un connecteur dans la AWS IoT Greengrass console, choisissez AWS IoT SiteWise Data Processor.
   b. Dans le champ Chemin de stockage local, entrez le chemin d'accès à votre passerelle SiteWise Edge.
   c. Choisissez Ajouter.
   d. Dans le coin supérieur droit, dans le menu Actions, choisissez Déployer, puis sélectionnez Détection automatique pour démarrer le déploiement.

Une fois votre passerelle SiteWise Edge déployée, vous pouvez ajouter une source pour chaque équipement industriel à partir duquel vous souhaitez que votre passerelle SiteWise Edge ingère des données. Pour plus d'informations, consultez Configuration des sources de données.

Vous pouvez consulter CloudWatch les statistiques Amazon pour vérifier que votre passerelle SiteWise Edge se connecte à AWS IoT SiteWise. Pour plus d'informations, consultez AWS IoT Greengrass Version 1 métriques de passerelle.

Configuration des sources de données sur les passerelles AWS IoT Greengrass V1 SiteWise Edge

Après avoir configuré une passerelle AWS IoT SiteWise Edge, vous pouvez configurer des sources de données afin que votre passerelle SiteWise Edge puisse ingérer des données provenant d'équipements industriels locaux vers AWS IoT SiteWise. Chaque source représente un serveur local, tel qu'un serveur OPC-UA, auquel votre passerelle SiteWise Edge connecte et récupère les flux de données industriels. Pour plus d'informations sur la configuration d'une passerelle SiteWise Edge, consultezConfiguration d'une passerelle AWS IoT Greengrass V1 SiteWise Edge.

> **Note**
>
> AWS IoT SiteWise redémarre votre passerelle SiteWise Edge chaque fois que vous ajoutez ou modifiez une source. Votre passerelle SiteWise Edge n'ingère pas de données lors du redémarrage. Le délai de redémarrage de votre passerelle SiteWise Edge dépend du

nombre de balises figurant sur les sources de votre passerelle SiteWise Edge. Le temps de redémarrage peut aller de quelques secondes (pour une passerelle SiteWise Edge avec peu de balises) à plusieurs minutes (pour une passerelle SiteWise Edge avec de nombreuses balises).

Après avoir créé les sources, vous pouvez associer vos flux de données aux propriétés des actifs. Pour plus d'informations sur la création et l'utilisation de ressources, reportez-vous aux sections Modélisation des ressources industrielles etMappage des flux de données industrielles avec des propriétés de ressources.

Vous pouvez consulter CloudWatch les métriques pour vérifier qu'une source de données est connectée à AWS IoT SiteWise. Pour plus d'informations, consultez AWS IoT Greengrass Version 1 métriques de passerelle.

Actuellement, AWS IoT SiteWise prend en charge les protocoles de source de données suivants :

- OPC-UA — Protocole de communication machine-to-machine (M2M) pour l'automatisation industrielle.
- Modbus TCP — Protocole de communication de données utilisé pour interfacer avec des contrôleurs logiques programmables (PLC).
- EtherNet/IP (EIP) : protocole de réseau industriel qui adapte le protocole industriel commun (CIP) à l'Ethernet standard.

> **Note**
>
> SiteWise Les passerelles Edge exécutées AWS IoT Greengrass V2 actuellement ne prennent pas en charge les sources IP Modbus TCP et Ethernet.

Rubriques

- Configuration d'une source Modbus TCP
- Configuration d'une source EtherNet/IP (EIP)
- Configuration de l'authentification source
- Mise à niveau d'un connecteur

Configuration d'une source Modbus TCP

Vous pouvez utiliser la AWS IoT SiteWise console ou une fonctionnalité de passerelle AWS IoT SiteWise Edge pour définir et ajouter une source TCP Modbus à votre passerelle SiteWise Edge. Cette source représente un serveur Modbus TCP local.

> **Note**
>
> - SiteWise Les passerelles Edge exécutées AWS IoT Greengrass V2 actuellement ne prennent pas en charge les sources Modbus TCP.
> - Vous devez installer le AWS IoT SiteWise connecteur pour utiliser une source Modbus TCP.

Vous pouvez utiliser la source Modbus TCP pour convertir le type de données de votre source en un autre type de données lorsqu'il est reçu sur votre passerelle SiteWise Edge. Le type de données source détermine les types de données que vous pouvez choisir pour vos données de destination. Vous pouvez également choisir d'échanger des octets à l'aide de la source Modbus TCP. Le tableau suivant fournit plus d'informations sur les types de données source, les types de données de destination et les modes d'échange compatibles.

Pour plus d'informations sur les modes d'échange, consultez l'article Comment les données réelles (à virgule flottante) et 32 bits sont encodées dans les messages Modbus RTU sur le codage des messages Modbus.

Type de données source	Types de données de destination compatibles	Modes d'échange compatibles	Versions de connecteurs compatibles
ASCII	Chaîne	Pas d'échange	2
UTF8	Chaîne	Pas d'échange	2
ISO8859	Chaîne	Pas d'échange	2
Int16	Entier, double, chaîne	Pas d'échange	1 et 2

Type de données source	Types de données de destination compatibles	Modes d'échange compatibles	Versions de connecteurs compatibles
Int32	Entier, double, chaîne	NoSwap, ByteSwap byteWordSwap, WordSwap	1 et 2
Float	Double, Corde	NoSwap, ByteSwap byteWordSwap, WordSwap	1 et 2
Booléen	Booléen	Pas d'échange	1 et 2
Hex-Dump	Chaîne	Pas d'échange	1 et 2

Rubriques

- Configuration d'une source Modbus TCP (console)
- Configuration d'une source Modbus TCP (CLI)

Configuration d'une source Modbus TCP (console)

Pour configurer une source Modbus TCP

1. Accédez à la console AWS IoT SiteWise.
2. Dans le volet de navigation de gauche, sélectionnez Passerelles.
3. Sur la passerelle SiteWise Edge pour laquelle vous souhaitez créer une source, choisissez Gérer, puis Afficher les détails.
4. Choisissez Nouvelle source dans le coin supérieur droit.
5. Pour les options de protocole, choisissez Modbus TCP.
6. Pour la configuration de la source Modbus TCP, entrez le nom de la source.
7. Pour l'adresse IP, entrez l'adresse IP du serveur de source de données.
8. (Facultatif) Entrez le port et l'ID d'unité du serveur source.
9. (Facultatif) Dans Durée minimale entre les demandes, entrez l'intervalle de temps entre les demandes suivantes envoyées à votre serveur. Votre passerelle SiteWise Edge calcule

automatiquement l'intervalle minimum autorisé en fonction de votre appareil et du nombre de registres dont vous disposez.

10. Pour les groupes de propriétés, entrez un nom.
11. Pour les propriétés :

    a. Pour Tag, entrez un alias de propriété pour votre ensemble de registres. Par exemple, **`TT-001`**.

    b. Dans Adresse du registre, entrez l'adresse du registre qui lance le jeu de registres.

    c. Pour le type de données source, choisissez le type de données Modbus TCP à partir duquel vous souhaitez convertir les données. La valeur par défaut est Hex dump.

    > **Note**
    >
    > Le type de données source que vous choisissez détermine la taille des données, le type de données de destination et le mode d'échange que vous pouvez choisir. Pour plus d'informations, consultez the section called "Configuration d'une source Modbus TCP".

    d. Pour Taille des données, entrez le nombre de registres à lire en partant de l'adresse du registre. Ceci est déterminé par le type de données source que vous choisissez pour cette source.

    e. Pour Type de données de destination, choisissez le type de AWS IoT SiteWise données vers lequel vous souhaitez que vos données soient converties. La valeur par défaut est String. Le type de destination doit être compatible avec le type de données source que vous avez choisi pour cette source. Pour plus d'informations, consultez the section called "Configuration d'une source Modbus TCP".

    f. Pour le mode Swap, choisissez le mode d'échange de données que vous souhaitez utiliser pour lire les données de votre ensemble de registres. Le mode d'échange doit être compatible avec le type de données source que vous avez choisi pour cette source. Pour plus d'informations, consultez the section called "Configuration d'une source Modbus TCP".

12. Pour le taux de numérisation, mettez à jour le taux auquel vous souhaitez que la passerelle SiteWise Edge lise vos registres. AWS IoT SiteWise calcule automatiquement le taux de numérisation minimum autorisé pour votre passerelle SiteWise Edge.
13. (Facultatif) Dans Destination, choisissez l'endroit où les données source sont envoyées. Par défaut, votre source envoie des données vers AWS IoT SiteWise.Vous pouvez utiliser un AWS

IoT Greengrass flux pour exporter vos données vers une destination locale ou vers le AWS Cloud.

> **Note**
>
> Vous devez choisir AWS IoT SiteWise la destination de vos données source si vous souhaitez traiter les données provenant de cette source à la périphérie AWS IoT SiteWise. Pour plus d'informations sur le traitement des données en périphérie, consultezthe section called “Permettre le traitement des données de pointe”.

Pour envoyer vos données vers une autre destination :

a. Pour les options de destination, sélectionnez Autres destinations.

b. Pour le nom du flux Greengrass, entrez le nom exact de votre AWS IoT Greengrass flux.

> **Note**
>
> Vous pouvez utiliser un flux que vous avez déjà créé ou créer un nouveau AWS IoT Greengrass flux pour exporter vos données. Si vous souhaitez utiliser un flux existant, vous devez saisir le nom exact du flux, sinon un nouveau flux sera créé. Pour plus d'informations sur l'utilisation des AWS IoT Greengrass flux, consultez la section Gérer les flux de données dans le guide du AWS IoT Greengrass développeur.

14. Choisissez Add source (Ajouter une source).

AWS IoT SiteWise déploie la configuration de la passerelle SiteWise Edge vers votre AWS IoT Greengrass cœur. Il n'est pas nécessaire de lancer manuellement un déploiement.

Configuration d'une source Modbus TCP (CLI)

Vous pouvez définir des sources de données Modbus TCP dans une fonctionnalité de passerelle SiteWise Edge. Vous devez définir toutes vos sources Modbus TCP dans une configuration de fonctionnalité unique.

> **Note**
>
> Vous devez installer le AWS IoT SiteWise connecteur pour utiliser une source Modbus TCP.

Cette capacité a les versions suivantes.

Version	Espace de noms
1	`iotsitewise:modbuscollector:1`

Paramètres de configuration de la fonctionnalité Modbus TCP

Lorsque vous définissez des sources Modbus TCP dans une configuration de fonctionnalité, vous devez spécifier les informations suivantes dans le document `capabilityConfiguration` JSON :

sources

Liste des structures de définition de source Modbus-TCP contenant chacune les informations suivantes :

nom

Nom unique et convivial pour la source.

measurementDataStreamPréfixe

(Facultatif) Chaîne à ajouter à tous les flux de données provenant de la source. La passerelle SiteWise Edge ajoute ce préfixe à tous les flux de données provenant de cette source. Utilisez un préfixe de flux de données pour distinguer les flux de données portant le même nom mais provenant de sources différentes. Chaque flux de données doit avoir un nom unique dans votre compte.

destination

Une structure de destination contenant les informations suivantes :

type

Type de destination.

Nom du flux

Le nom du AWS IoT Greengrass flux.

streamBufferSize

Taille de la mémoire tampon du flux.

point de terminaison

Structure de point de terminaison contenant les informations suivantes :

Adresse IP

Adresse IP de la source TCP Modbus.

port

(Facultatif) Le port de la source Modbus TCP.

ID de l'unité

(Facultatif) L'identifiant de l'unité. La valeur par défaut est 1.

minimumInterRequestDurée

Durée minimale entre chaque demande en millisecondes.

Groupes de propriétés

Liste des groupes de propriétés qui définissent la définition de balise demandée par le protocole.

nom

Nom du groupe de propriétés. Il doit s'agir d'un identifiant unique.

tagPathDefinitions

Emplacement de la mesure dans la source. Par exemple, l'ordre des octets et des mots, l'adresse et le type de transformation. La structure de chacun `MeasurementPathDefinition` est définie par le connecteur.

Mode de numérisation

Définit le comportement du mode de numérisation et les paramètres configurables pour la source.

Configuration d'une source EtherNet/IP (EIP)

Vous pouvez utiliser la AWS IoT SiteWise console ou une fonctionnalité de passerelle SiteWise Edge pour définir et ajouter une source IP Ethernet à votre passerelle SiteWise Edge. Cette source représente un serveur IP Ethernet local.

> **Note**
>
> - SiteWise Les passerelles Edge qui s'exécutent AWS IoT Greengrass V2 actuellement ne prennent pas en charge les sources IP Ethernet.
> - Vous devez installer le AWS IoT SiteWise connecteur pour utiliser une source IP Ethernet.

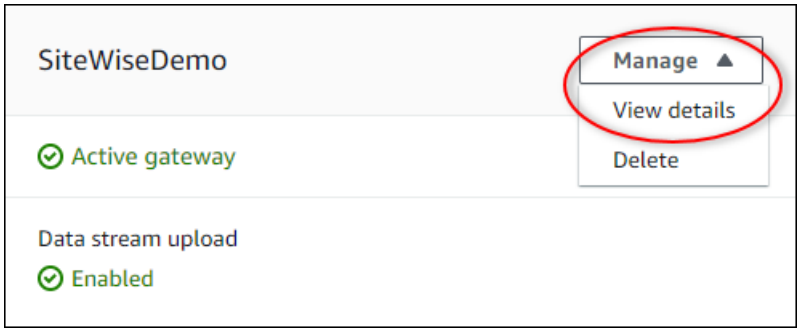
Rubriques

- Configuration d'une source EtherNet/IP (console)
- Configuration d'une source EtherNet/IP (CLI)

Configuration d'une source EtherNet/IP (console)

Pour configurer une source EtherNet/IP

1. Accédez à la console AWS IoT SiteWise.
2. Dans le volet de navigation de gauche, sélectionnez Passerelles.
3. Sur la passerelle SiteWise Edge pour laquelle vous souhaitez créer une source, choisissez Gérer, puis Afficher les détails.



4. Choisissez Nouvelle source dans le coin supérieur droit.
5. Pour les options de protocole, choisissez EtherNet/IP (EIP).
6. Pour la configuration de la source EtherNet /IP, entrez le nom de la source.

7. Pour l'adresse IP, entrez l'adresse IP du serveur de source de données.
8. (Facultatif) Entrez le port du serveur source.
9. Pour Durée minimale entre les requêtes, entrez l'intervalle de temps entre les demandes suivantes envoyées à votre serveur. Votre passerelle SiteWise Edge calcule automatiquement l'intervalle minimum autorisé en fonction de votre appareil et du nombre de registres dont vous disposez.
10. Pour les groupes de propriétés, entrez un nom.
11. Pour les propriétés :

    a. Pour Tag, entrez l'alias de propriété de votre ensemble de registres. Par exemple, **`boiler.inlet.temperature.value`**.

    b. Pour Type de données de destination, choisissez le type de AWS IoT SiteWise données vers lequel vous souhaitez que vos données soient converties. La valeur par défaut est String.
12. Pour le taux de numérisation, mettez à jour le taux auquel vous souhaitez que la passerelle SiteWise Edge lise vos registres. AWS IoT SiteWise calcule automatiquement le taux de numérisation minimum autorisé pour votre passerelle SiteWise Edge.
13. (Facultatif) Dans Destination, choisissez l'endroit où les données source sont envoyées. Par défaut, votre source envoie des données vers AWS IoT SiteWise.Vous pouvez utiliser un AWS IoT Greengrass flux pour exporter vos données vers une destination locale ou vers le AWS Cloud.

    > **Note**
    >
    > Vous devez choisir AWS IoT SiteWise la destination de vos données source si vous souhaitez traiter les données provenant de cette source à la périphérie AWS IoT SiteWise. Pour plus d'informations sur le traitement des données en périphérie, consultezthe section called “Permettre le traitement des données de pointe”.

    Pour envoyer vos données vers une autre destination :

    a. Pour les options de destination, sélectionnez Autres destinations.

    b. Pour le nom du flux Greengrass, entrez le nom exact de votre AWS IoT Greengrass flux.

> **Note**
>
> Vous pouvez utiliser un flux que vous avez déjà créé ou créer un nouveau AWS IoT Greengrass flux pour exporter vos données. Si vous souhaitez utiliser un flux existant, vous devez saisir le nom exact du flux, sinon un nouveau flux sera créé. Pour plus d'informations sur l'utilisation des AWS IoT Greengrass flux, consultez la section Gérer les flux de données dans le guide du AWS IoT Greengrass développeur.

14. Choisissez Add source (Ajouter une source).

    AWS IoT SiteWise déploie la configuration de la passerelle SiteWise Edge vers votre AWS IoT Greengrass cœur. Il n'est pas nécessaire de lancer manuellement un déploiement.

Configuration d'une source EtherNet/IP (CLI)

Vous pouvez définir des sources de données EIP dans une fonctionnalité de passerelle SiteWise Edge. Vous devez définir toutes vos sources EIP dans une configuration de fonctionnalité unique.

> **Note**
>
> Vous devez installer le AWS IoT SiteWise connecteur pour utiliser une source IP Ethernet.

Cette capacité a les versions suivantes.

Version	Espace de noms
1	`iotsitewise:eipcollector:1`

Paramètres de configuration de la capacité EIP

Lorsque vous définissez des sources EIP dans une configuration de fonctionnalité, vous devez spécifier les informations suivantes dans le document `capabilityConfiguration` JSON :

sources

Liste des structures de définition de source EIP contenant chacune les informations suivantes :

nom

Nom unique et convivial pour la source. Cela peut comporter jusqu'à 256 caractères.

destinationPathPrefix

(Facultatif) Chaîne à ajouter à tous les flux de données provenant de la source. La passerelle SiteWise Edge ajoute ce préfixe à tous les flux de données provenant de cette source. Utilisez un préfixe de flux de données pour distinguer les flux de données portant le même nom mais provenant de sources différentes. Chaque flux de données doit avoir un nom unique dans votre compte.

destination

Une structure de destination contenant les informations suivantes :

type

Type de destination.

Nom du flux

Le nom du AWS IoT Greengrass flux.

streamBufferSize

Taille de la mémoire tampon du flux.

point de terminaison

Structure de point de terminaison contenant les informations suivantes :

Adresse IP

Adresse IP de la source EIP.

port

(Facultatif) Le port de la source EIP. Les valeurs acceptées sont des nombres compris entre 1 et 65535.

minimumInterRequestDurée

(Facultatif) Durée minimale entre chaque demande, en millisecondes.

Groupes de propriétés

Liste des groupes de propriétés qui définissent la définition de balise demandée par le protocole. Chaque source peut avoir un groupe de propriétés.

nom

Nom du groupe de propriétés. Il doit s'agir d'un identifiant unique d'une longueur maximale de 256 caractères.

tagPathDefinitions

La liste des structures spécifiant les données à collecter à partir du périphérique EtherNet/IP et la manière de les transformer pour la sortie.

type

Type de l'élément `tagPathDefinition`. Par exemple, `EIPTagPath`.

chemin

Le chemin du`tagPathDefinition`. Chaque balise d'un chemin peut comporter au maximum 40 caractères et peut commencer par une lettre ou un trait de soulignement. Les balises ne peuvent pas contenir de traits de soulignement consécutifs ou finaux. Le chemin est préfixé par une valeur quelconque de. destinationPathPrefix

dstDataType

Type de données à utiliser pour générer les données de balise. Les valeurs acceptées sont `integer`,`double`,`string`, et`boolean`.

Mode de numérisation

Définit le comportement du mode de numérisation et les paramètres configurables pour la source.

type

Type de comportement du mode de numérisation. Les valeurs acceptées sont`POLL`.

taux

Fréquence en millisecondes pendant laquelle le connecteur doit lire les balises provenant de la source EtherNet/IP.

Configuration de l'authentification source

Si vos serveurs OPC-UA nécessitent des informations d'authentification pour se connecter, vous pouvez définir un nom d'utilisateur et un mot de passe dans un secret pour chaque source dans AWS

Secrets Manager. Vous ajoutez ensuite le secret à votre groupe Greengrass et à votre SiteWise connecteur IoT pour le rendre accessible à votre passerelle SiteWise Edge. Pour plus d'informations, consultez la section Déployer des secrets vers le AWS IoT Greengrass noyau dans le Guide du AWS IoT Greengrass Version 1 développeur.

Une fois qu'un secret est disponible pour votre passerelle SiteWise Edge, vous pouvez le choisir lorsque vous configurez une source. La passerelle SiteWise Edge utilise ensuite les informations d'authentification du secret lorsqu'elle se connecte à la source. Pour plus d'informations, consultez Configuration des sources de données.

Rubriques

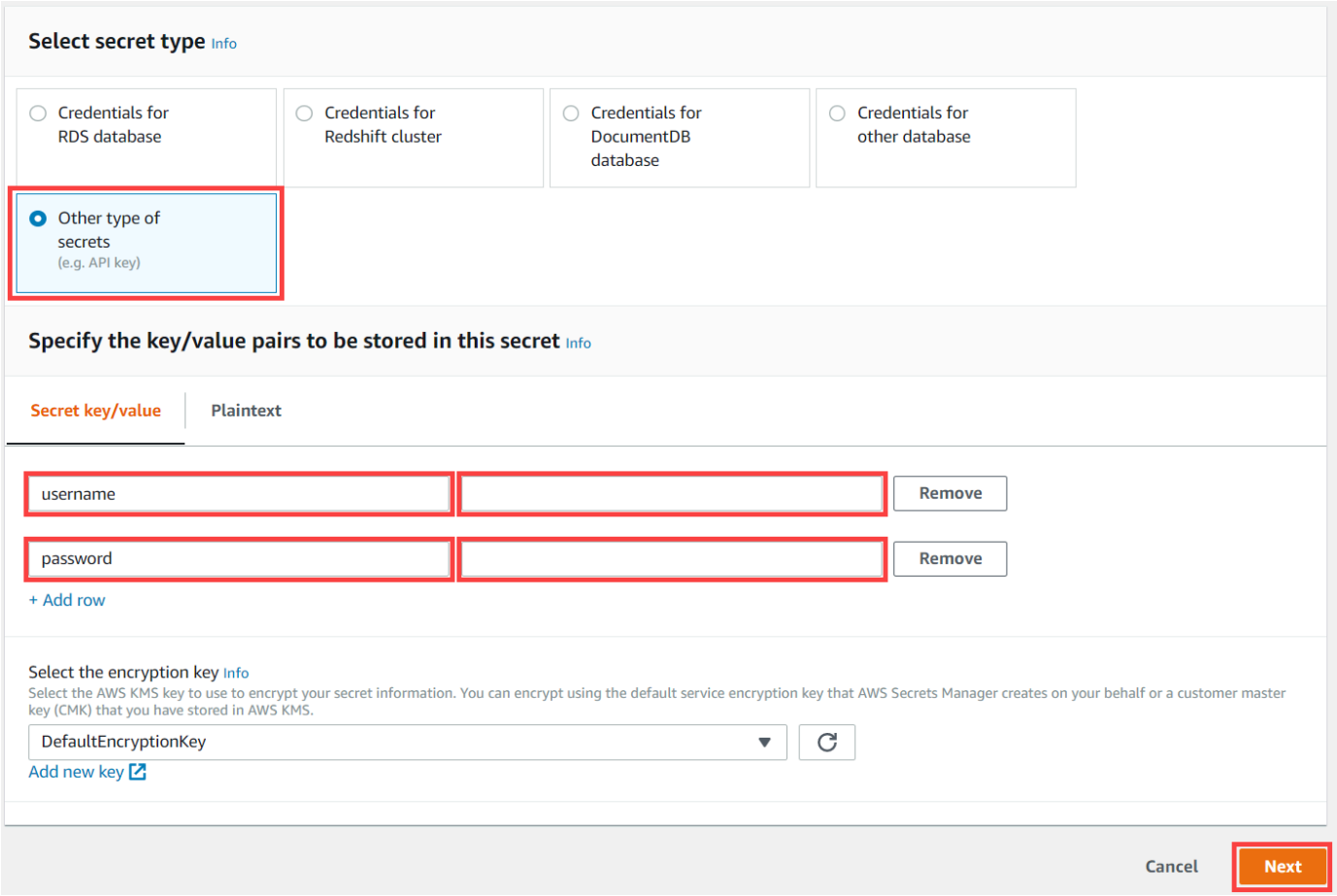
- Création de secrets d'authentification source
- Ajouter des secrets à un groupe Greengrass
- Ajouter des secrets à un SiteWise connecteur IoT

Création de secrets d'authentification source

Dans cette procédure, vous allez créer un secret d'authentification pour votre source dans Secrets Manager. Dans le secret, définissez des paires clé-valeur **`username`** et **`password`** qui contiennent les détails d'authentification de votre source.

Pour créer un secret d'authentification source

1. Accédez à la console Secrets Manager.
2. Choisissez Store a new secret (Stocker un nouveau secret).
3. Pour Select secret type (Sélectionner un type de secret), choisissez Other type of secrets (Autre type de secrets).
4. Entrez **`username`** et des paires clé-valeur **`password`** comme valeurs d'authentification de votre serveur OPC-UA, puis choisissez Suivant.



5. Entrez un nom secret commençant par `greengrass-`, par exemple **`greengrass-factory1-auth`**.

> **Important**
>
> Vous devez utiliser le préfixe `greengrass-` du rôle de service AWS IoT Greengrass par défaut pour accéder à vos secrets. Si vous souhaitez attribuer un nom à vos secrets sans ce préfixe, vous devez accorder des autorisations AWS IoT Greengrass personnalisées pour accéder à vos secrets. Pour plus d'informations, voir AWS IoT Greengrass Autoriser l'obtention de valeurs secrètes dans le Guide du AWS IoT Greengrass Version 1 développeur.

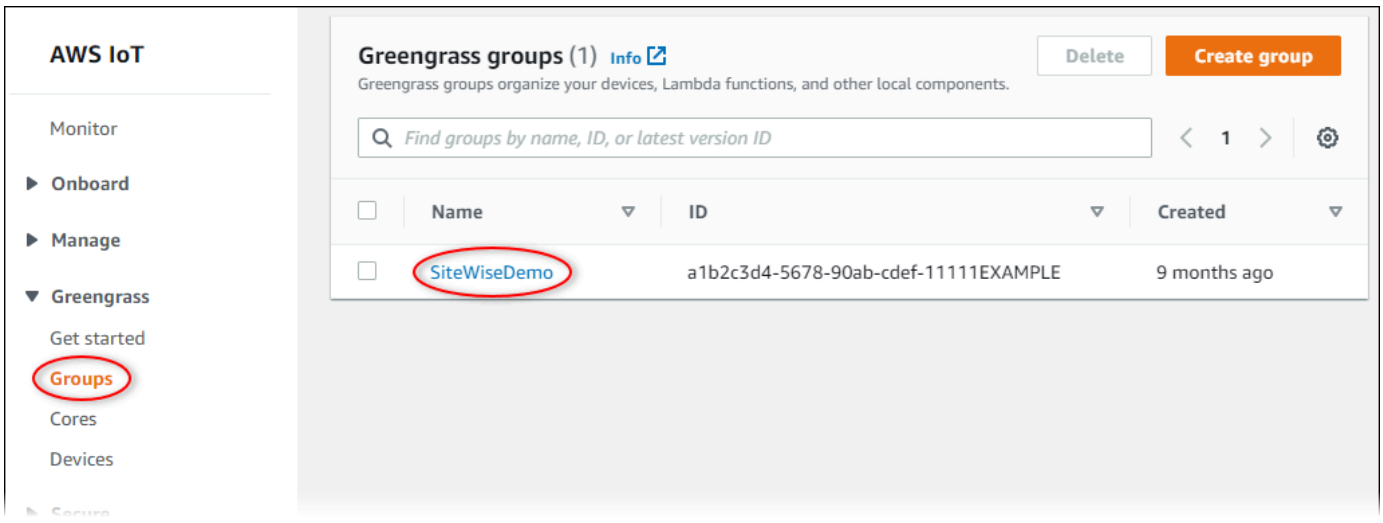
6. Entrez une description et choisissez Suivant.
7. (Facultatif) Dans la page Configurer la rotation automatique, configurez la rotation automatique pour vos secrets. Si vous configurez la rotation automatique, vous devez redéployer votre groupe Greengrass à chaque rotation d'un secret.
8. Dans la page Configurer la rotation automatique, choisissez Suivant.
9. Passez en revue votre nouveau secret et choisissez Magasin.

Ajouter des secrets à un groupe Greengrass

Dans cette procédure, vous ajoutez les secrets d'authentification de votre source à votre AWS IoT Greengrass groupe pour les mettre à la disposition de votre SiteWise connecteur IoT.

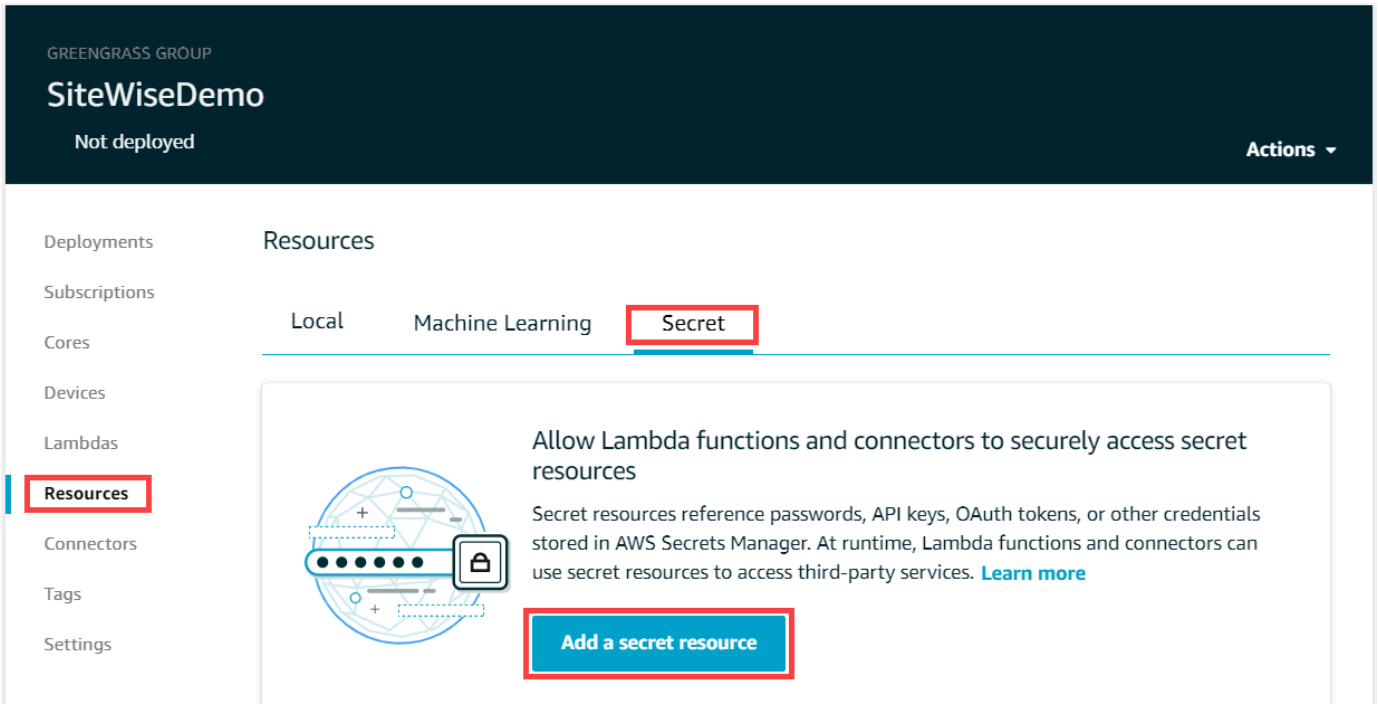
Pour ajouter un secret à votre groupe Greengrass

1. Accédez à la console AWS IoT Greengrass.
2. Dans le volet de navigation, sous Greengrass, choisissez Groups, puis choisissez votre groupe.

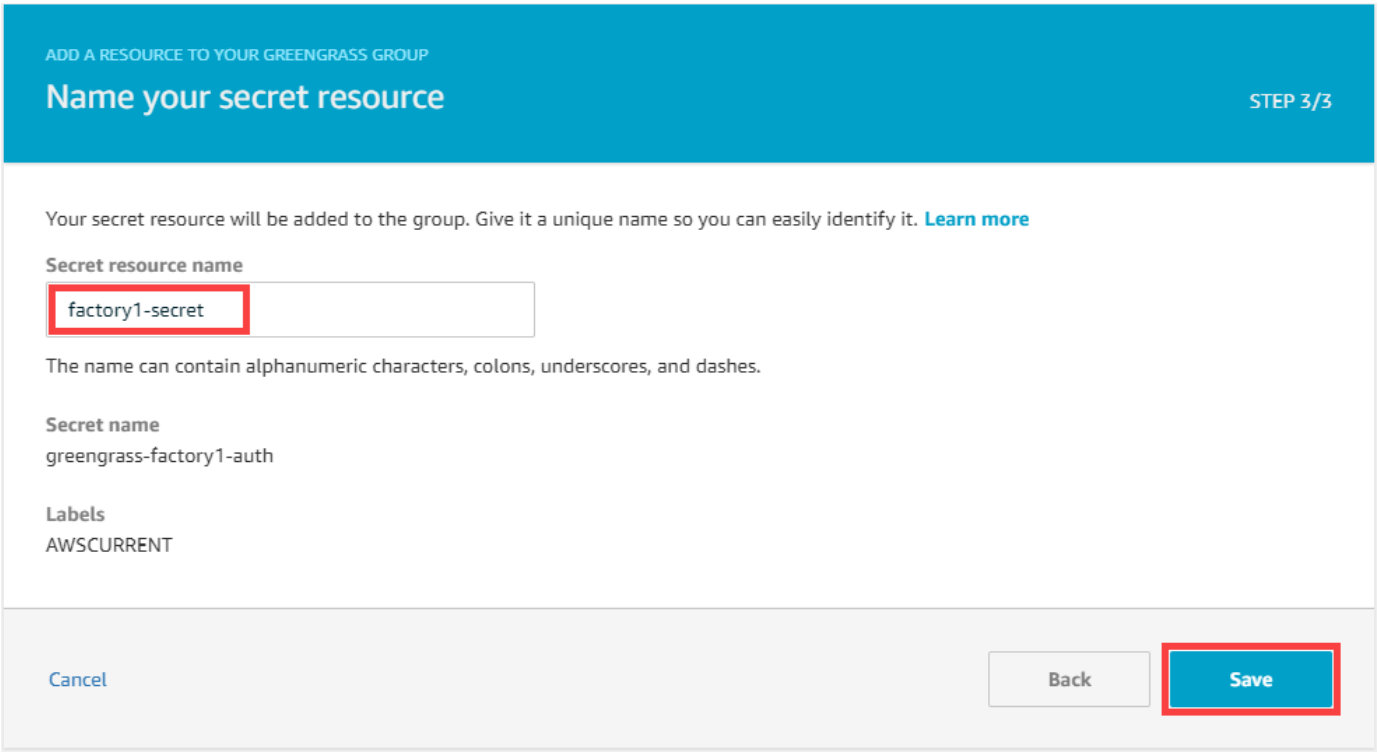


3. Sur la page de navigation, sélectionnez Ressources.

4. Sur la page Ressources choisissez l'onglet Secret puis Ajouter une ressource secrète.



5. Choisissez Sélectionner et choisissez votre secret dans la liste.
6. Choisissez Suivant.
7. Dans Nom de ressource secrète, entrez un nom pour votre ressource secrète et choisissez Enregistrer.

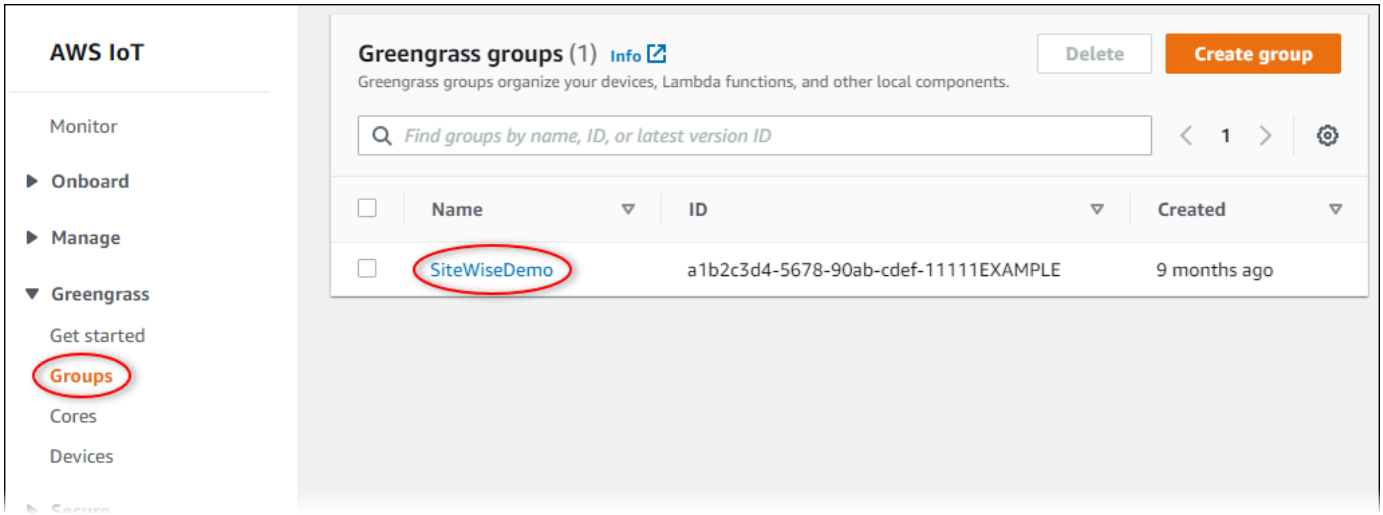


Ajouter des secrets à un SiteWise connecteur IoT

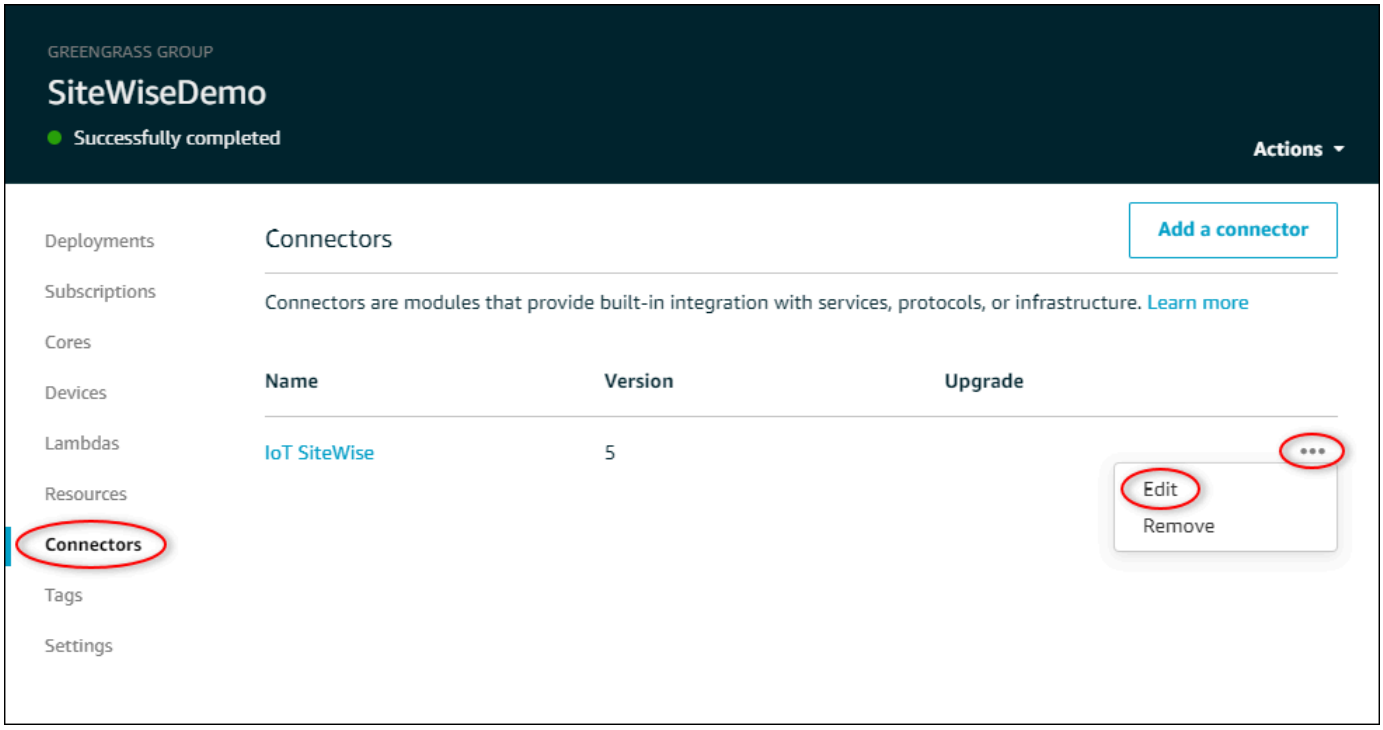
Dans cette procédure, vous ajoutez les secrets d'authentification de votre source à votre SiteWise connecteur IoT pour les mettre à la disposition de votre passerelle SiteWise Edge AWS IoT SiteWise et de la mettre à la disposition de celle-ci.

Pour ajouter un secret à votre SiteWise connecteur IoT

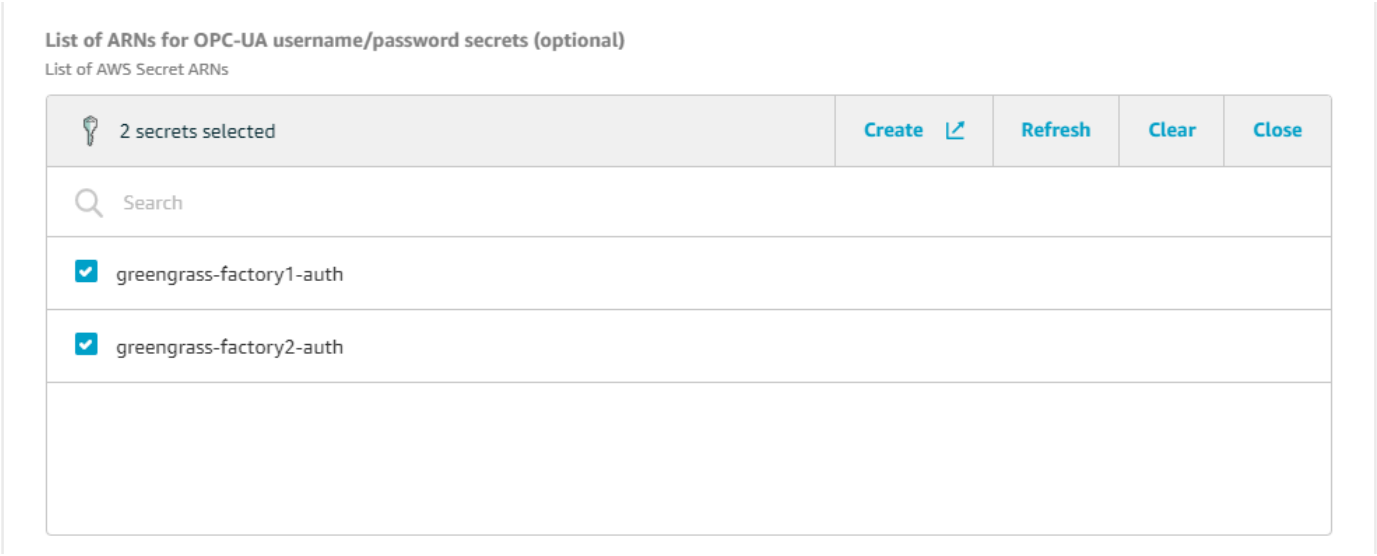
1. Accédez à la console AWS IoT Greengrass.
2. Dans le volet de navigation, sous Greengrass, choisissez Groups, puis choisissez votre groupe.



3. Dans la page de navigation, sélectionnez Connectors.
4. Choisissez l'icône représentant des points de suspension pour le SiteWise connecteur IoT pour ouvrir le menu des options, puis choisissez Modifier.



5. Sous Liste des ARN pour les secrets de nom d'utilisateur/mot de passe OPC-UA, choisissez Select, puis sélectionnez chaque secret à ajouter à cette passerelle Edge. SiteWise Si vous avez besoin de créer des secrets, veuillez consulter Création de secrets d'authentification source.



   Si votre secret n'apparaît pas, choisissez Actualiser. Si votre secret n'apparaît toujours pas, vérifiez que vous l'avez ajouté à votre groupe Greengrass.

6. Choisissez Enregistrer.
7. Dans le coin supérieur droit de la page, dans le menu Actions choisissez Déployer.
8. Choisissez Détection automatique pour démarrer le déploiement.

Si le déploiement échoue, choisissez à nouveau Déployer . Si le déploiement continue d'échouer, veuillez consulter Dépannage du déploiement AWS IoT Greengrass.

Une fois votre groupe déployé, vous pouvez configurer une source qui utilise le nouveau secret. Pour plus d'informations, consultez Configuration des sources de données.

Mise à niveau d'un connecteur

Important

La version 6 du SiteWise connecteur IoT introduit de nouvelles exigences : le logiciel de AWS IoT Greengrass base v1.10.0 et le gestionnaire de flux. Avant de mettre à niveau votre connecteur, vérifiez que votre passerelle SiteWise Edge répond à ces exigences, sinon vous ne pourrez pas déployer votre passerelle SiteWise Edge.

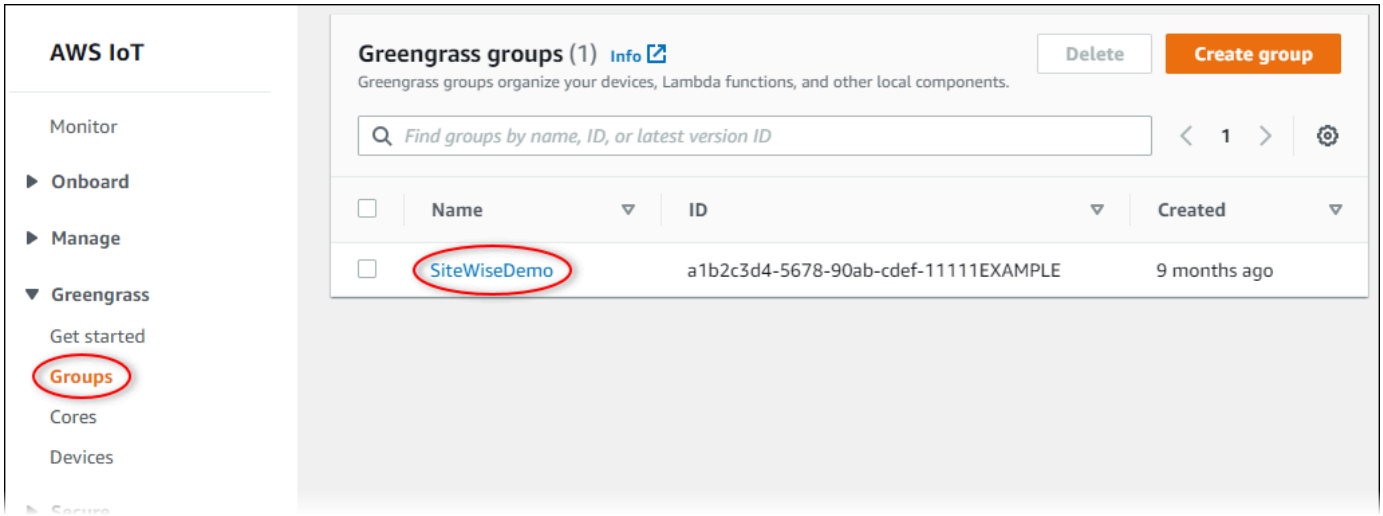
Vous pouvez facilement mettre à niveau le connecteur de votre passerelle SiteWise Edge après la sortie d'une nouvelle version SiteWise du connecteur IoT.

Note

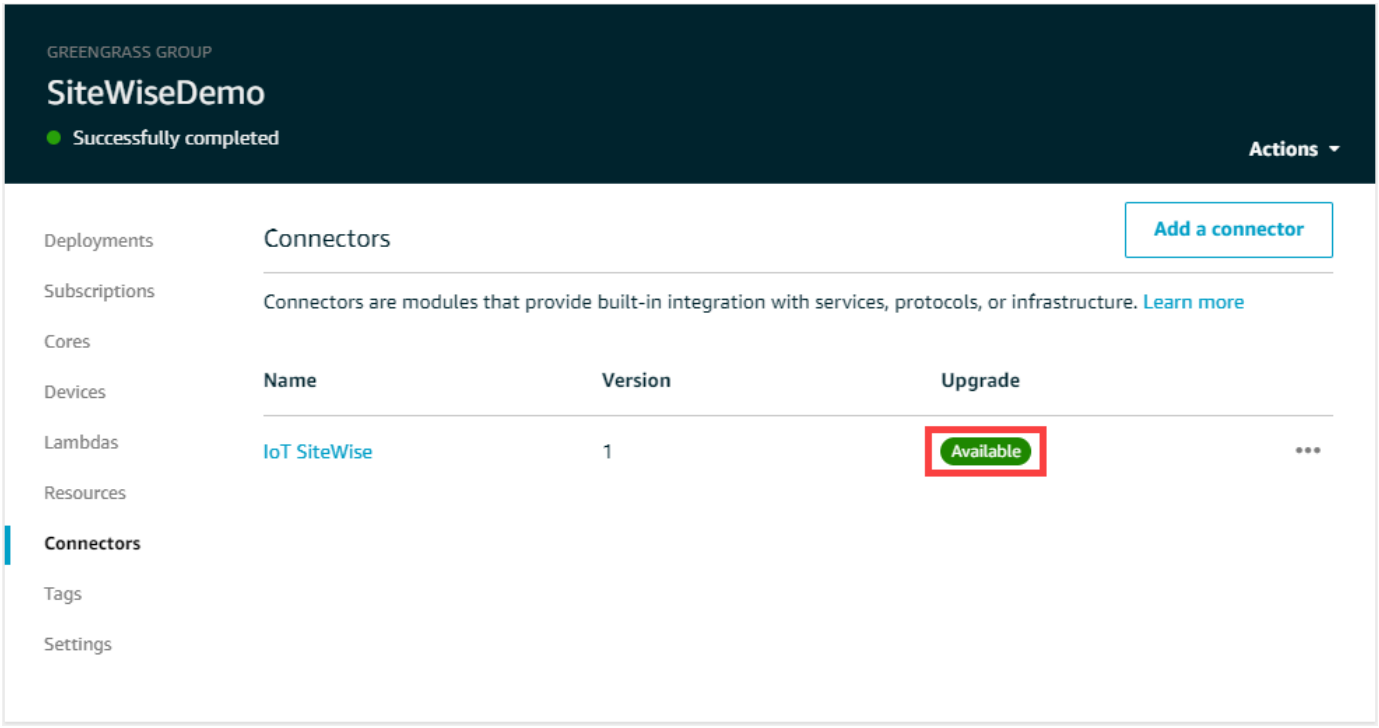
Dans cette procédure, vous devez redéployer votre groupe Greengrass et redémarrer SiteWise votre passerelle Edge. Votre passerelle SiteWise Edge n'ingère pas de données lors du redémarrage. Le délai de redémarrage de votre passerelle SiteWise Edge dépend du nombre de balises figurant sur les sources de votre passerelle SiteWise Edge. Le temps de redémarrage peut aller de quelques secondes (pour une passerelle SiteWise Edge avec peu de balises) à plusieurs minutes (pour une passerelle SiteWise Edge avec de nombreuses balises).

Pour mettre à niveau un SiteWise connecteur IoT

1. Accédez à la console AWS IoT Greengrass.
2. Dans le volet de navigation, sous Greengrass, choisissez Groups, puis choisissez le groupe que vous avez créé lors de la configuration de votre passerelle SiteWise Edge.



3. Dans le volet de navigation, sélectionnez Connectors.
4. Sur la page Connecteurs, sélectionnez Disponible à côté du SiteWise connecteur IoT.



Si vous ne voyez pas l'élément Available (Disponible), votre connecteur correspond déjà à la dernière version.

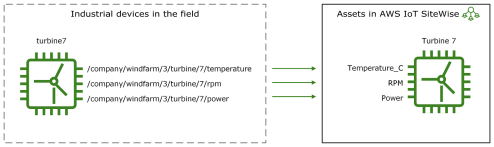
5. Dans la page Upgrade connector (Mettre à niveau le connecteur), entrez les paramètres de votre connecteur, puis choisissez Upgrade (Mettre à niveau).
6. Dans le coin supérieur droit de la page, dans le menu Actions choisissez Déployer.
7. Choisissez Détection automatique pour démarrer le déploiement.

Si le déploiement échoue, choisissez à nouveau Déployer . Si le déploiement continue d'échouer, veuillez consulter Dépannage du déploiement AWS IoT Greengrass.

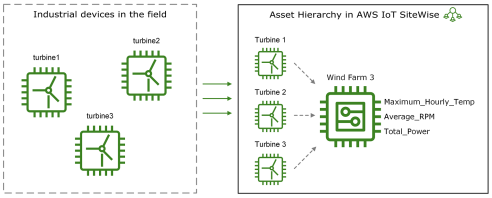
Modélisation des ressources industrielles

Vous pouvez créer des représentations virtuelles de votre activité industrielle à l'aide d' AWS IoT SiteWise actifs. Un actif représente un appareil, un équipement ou un processus qui télécharge un ou plusieurs flux de données vers le AWS Cloud. Par exemple, un appareil ressource peut être une éolienne qui envoie des mesures en séries chronologiques de la température de l'air, de la vitesse de rotation de l'hélice et de la puissance de sortie vers les propriétés des ressources dans AWS IoT SiteWise.

Chaque flux de données correspond à un alias de propriété unique. Par exemple, l'alias `/company/windfarm/3/turbine/7/temperature` identifie de manière unique le flux de données de température provenant de la turbine n° 7 dans le parc éolien n° 3. Vous pouvez configurer AWS IoT SiteWise des actifs pour transformer les données de mesure entrantes à l'aide d'expressions mathématiques, par exemple pour convertir les données de température de degrés Celsius en degrés Fahrenheit.



Une ressource peut également représenter un regroupement logique de dispositifs, par exemple un parc éolien entier. Vous pouvez associer des actifs à d'autres actifs pour créer des hiérarchies d'actifs représentant des opérations industrielles complexes. Les actifs peuvent accéder aux données contenues dans leurs actifs enfants associés. Ce faisant, vous pouvez utiliser des AWS IoT SiteWise expressions pour calculer des mesures agrégées, telles que la puissance de production nette d'un parc éolien.



Vous devez créer chaque actif à partir d'un modèle d'actif. Les modèles de ressources sont des structures déclaratives qui normalisent le format de vos ressources. Les modèles d'actifs appliquent des informations cohérentes sur plusieurs actifs du même type afin que vous puissiez traiter les données dans des actifs qui représentent des groupes d'appareils. Dans le diagramme précédent,

vous utilisez le même modèle de ressource pour les trois turbines car toutes les turbines partagent un ensemble commun de propriétés.

Vous pouvez également créer des modèles de composants. Un modèle de composant est un type spécial de modèle d'actif que vous pouvez inclure dans des modèles d'actifs ou d'autres modèles de composants. Vous pouvez utiliser des modèles de composants pour définir des sous-assemblages réutilisables communs, tels que des capteurs, des moteurs, etc., que vous partagez entre plusieurs modèles d'actifs.

Après avoir défini vos modèles de ressources, vous pouvez créer vos ressources industrielles. Pour créer une ressource, sélectionnez un modèle de ressources `ACTIVE` afin de créer une ressource à partir de ce modèle. Ensuite, vous pouvez remplir des informations spécifiques aux ressources, telles que les alias de flux de données et les attributs. Dans le diagramme précédent, vous créez trois ressources de turbine à partir d'un modèle de ressource, puis vous associez des alias de flux de données comme `/company/windfarm/3/turbine/7/temperature` pour chaque turbine.

Vous pouvez également mettre à jour et supprimer des actifs, des modèles d'actifs et des modèles de composants existants. Lorsque vous mettez à jour un modèle de ressource, chaque ressource basée sur ce modèle de ressource reflète toutes les modifications que vous apportez au modèle sous-jacent. Lorsque vous mettez à jour un modèle de composant, cela s'applique à chaque actif en fonction de chaque modèle d'actif qui fait référence au modèle de composant.

Vos modèles d'actifs peuvent être très complexes, par exemple lorsque vous modélisez un équipement complexe comportant de nombreux sous-composants. Pour que ces modèles d'actifs restent organisés et maintenables, vous pouvez utiliser des modèles composites personnalisés pour regrouper les propriétés associées ou pour réutiliser des composants partagés. Pour plus d'informations, consultez Modèles composites personnalisés (composants).

Rubriques

- État des ressources et des modèles
- Modèles composites personnalisés (composants)
- Utilisation des identifiants d'objets
- Création de modèles d'actifs et de modèles de composants
- Création de ressources
- Recherche de ressources
- Mappage des flux de données industrielles avec des propriétés de ressources
- Mise à jour des valeurs d'attribut

- Association et dissociation de ressources
- Mise à jour des ressources et des modèles
- Suppression des ressources et des modèles
- Opérations groupées avec actifs et modèles

État des ressources et des modèles

Lorsque vous créez, mettez à jour ou supprimez une ressource, un modèle de ressource ou un modèle de composant, les modifications mettent du temps à se propager. AWS IoT SiteWise résout ces opérations de manière asynchrone et met à jour le statut de chaque ressource. Chaque actif, modèle d'actif et modèle de composant possède un champ d'état qui contient l'état de la ressource et tout message d'erreur, le cas échéant. L'état peut avoir l'une des valeurs suivantes :

- `ACTIVE`— La ressource est active. Il s'agit du seul état dans lequel vous pouvez interroger et interagir avec les actifs, les modèles d'actifs et les modèles de composants.
- `CREATING`— La ressource est en cours de création.
- `UPDATING`— La ressource est en cours de mise à jour.
- `DELETING`— La ressource est en cours de suppression.
- `PROPAGATING`— (Modèles d'actifs et modèles de composants uniquement) Les modifications se propagent à toutes les ressources dépendantes (du modèle d'actif aux actifs, ou du modèle de composant aux modèles d'actifs).
- `FAILED`— La ressource n'a pas pu être validée lors d'une opération de création ou de mise à jour, probablement en raison d'une référence circulaire dans une expression. Vous pouvez supprimer les ressources qui se trouvent dans `FAILED` cet état.

Certaines des opérations de création, de mise à jour et de suppression mettent en AWS IoT SiteWise place un actif, un modèle d'actif ou un modèle de composant dans un état autre que celui `ACTIVE` pendant la résolution de l'opération. Pour interroger ou interagir avec une ressource après avoir effectué l'une de ces opérations, vous devez attendre que son état passe à`ACTIVE`. Sinon, vos demandes échouent.

Rubriques

- Vérification de l'état d'une ressource
- Vérification de l'état d'un modèle d'actif ou d'un modèle de composant

Vérification de l'état d'une ressource

Vous pouvez utiliser la AWS IoT SiteWise console ou l'API pour vérifier l'état d'un actif.

Rubriques

- Vérification de l'état d'une ressource (console)
- Vérifier l'état d'un actif (AWS CLI)

Vérification de l'état d'une ressource (console)

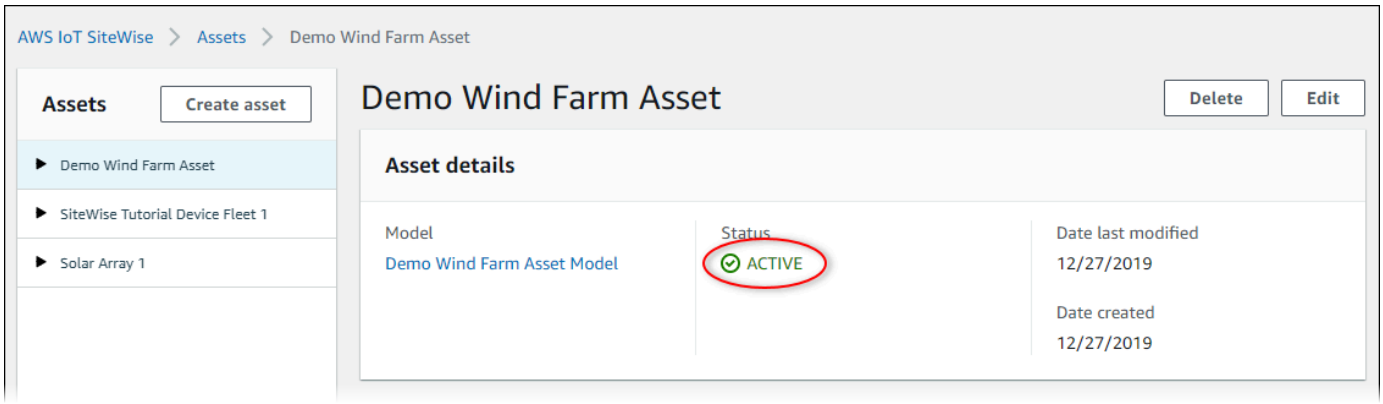
Utilisez la procédure suivante pour vérifier l'état d'une ressource dans la console AWS IoT SiteWise .

Pour vérifier l'état d'une ressource (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Ressources.
3. Choisissez la ressource à vérifier.

> **Tip**
>
> Vous pouvez cliquer sur l'icône en forme de flèche pour développer une hiérarchie de ressources afin de trouver votre ressource.

4. Recherchez l'état dans le volet Informations relatives à la ressource.



Vérifier l'état d'un actif (AWS CLI)

Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour vérifier l'état d'un actif.

Pour vérifier l'état d'un actif, utilisez l'DescribeAssetopération avec le `assetId` paramètre.

Pour vérifier l'état d'un actif (AWS CLI)

- Exécutez la commande suivante pour décrire la ressource. Remplacez *`asset-id`* par l'ID de l'actif ou par l'ID externe. L'identifiant externe est un identifiant défini par l'utilisateur. Pour plus d'informations, consultez Référencement d'objets avec des identifiants externes dans le Guide de l'utilisateur AWS IoT SiteWise .

  ```
  aws iotsitewise describe-asset --asset-id asset-id
  ```

  L'opération renvoie une réponse qui contient les détails de la ressource. La réponse contient un `assetStatus` objet dont la structure est la suivante :

  ```
  {
      ...
      "assetStatus": {
        "state": "String",
        "error": {
           "code": "String",
           "message": "String"
        }
      }
    }
  ```

  L'état de la ressource est dans `assetStatus.state` dans l'objet JSON.

Vérification de l'état d'un modèle d'actif ou d'un modèle de composant

Vous pouvez utiliser la AWS IoT SiteWise console ou l'API pour vérifier l'état d'un modèle d'actif ou d'un modèle de composant.

Rubriques

- Vérification de l'état d'un modèle d'actif ou d'un modèle de composant (console)
- Vérification de l'état d'un modèle d'actif ou d'un modèle de composant (AWS CLI)

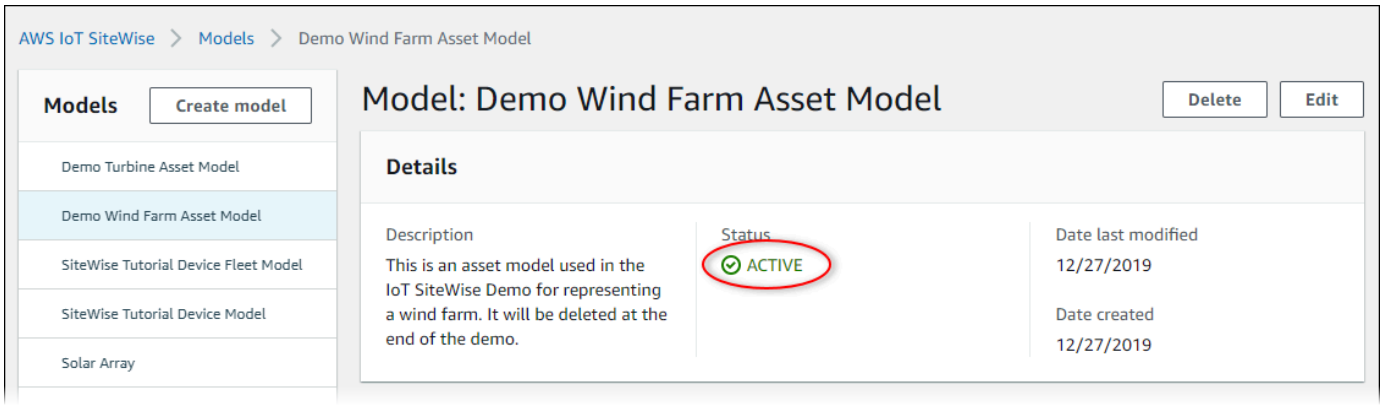
Vérification de l'état d'un modèle d'actif ou d'un modèle de composant (console)

Utilisez la procédure suivante pour vérifier l'état d'un modèle de ressource ou d'un modèle de composant dans la AWS IoT SiteWise console.

> **Tip**
>
> Les modèles d'actifs et les modèles de composants sont tous deux répertoriés sous Modèles dans le volet de navigation. Le panneau Détails du modèle d'actif ou du modèle de composant sélectionné indique de quel type il s'agit.

Pour vérifier l'état d'un modèle d'actif ou d'un modèle de composant (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Models (Modèles).
3. Choisissez le modèle à vérifier.
4. Recherchez État dans le volet Détails.



Vérification de l'état d'un modèle d'actif ou d'un modèle de composant (AWS CLI)

Vous pouvez utiliser le AWS CLI pour vérifier l'état d'un modèle d'actif ou d'un modèle de composant.

Pour vérifier l'état d'un modèle d'actif ou d'un modèle de composant, utilisez l'opération DescribeAssetModel avec le `assetModelId` paramètre.

> **Tip**
>
> AWS CLI définit les modèles de composants comme un type de modèle d'actif. Par conséquent, vous utilisez la même opération de DescribeAssetmodèle pour les deux types de modèles. Le `assetModelType` champ de la réponse indique s'il s'agit d'un `ASSET_MODEL` ou d'un`COMPONENT_MODEL`.

Pour vérifier l'état d'un modèle d'actif ou d'un modèle de composant (AWS CLI)

- Exécutez la commande suivante pour décrire le modèle. Remplacez *`asset-model-id par l'ID`* ou l'ID externe du modèle d'actif ou du modèle de composant. L'identifiant externe est un identifiant défini par l'utilisateur. Pour plus d'informations, consultez Référencement d'objets avec des identifiants externes dans le Guide de l'utilisateur AWS IoT SiteWise .

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

  L'opération renvoie une réponse contenant les détails du modèle. La réponse contient un objet `assetModelStatus` qui présente la structure suivante.

  ```
  {
      ...
      "assetModelStatus": {
        "state": "String",
        "error": {
           "code": "String",
           "message": "String"
        }
      }
    }
  ```

  L'état du modèle se trouve `assetModelStatus.state` dans l'objet JSON.

Modèles composites personnalisés (composants)

Lorsque vous modélisez un actif industriel particulièrement complexe, tel qu'une machine complexe comportant de nombreuses pièces, il peut être difficile de garder vos modèles d'actifs organisés et maintenables.

Dans ce cas, vous pouvez ajouter des modèles composites personnalisés, ou des composants si vous utilisez la console, à vos modèles d'actifs et modèles de composants existants. Ils vous aident à rester organisé en regroupant les propriétés associées et en réutilisant les définitions de sous-composants.

Il existe deux types de modèles composites personnalisés :

- Les modèles composites personnalisés en ligne définissent un ensemble de propriétés groupées qui s'appliquent au modèle d'actif ou au modèle de composant auquel appartient le modèle composite personnalisé. Vous les utilisez pour regrouper les propriétés associées. Ils se composent d'un nom, d'une description et d'un ensemble de propriétés du modèle d'actif. Ils ne sont pas réutilisables.
- Les modèles composites personnalisés basés sur des modèles de composants font référence à un modèle de composant que vous souhaitez inclure dans votre modèle d'actif ou de composant. Vous les utilisez pour inclure des sous-assemblages standard dans votre modèle. Ils se composent d'un nom, d'une description et de l'ID du modèle de composant auquel il fait référence. Ils n'ont aucune propriété propre ; le modèle de composant référencé fournit ses propriétés associées à tous les actifs créés.

Les sections suivantes montrent comment utiliser des modèles composites personnalisés dans vos conceptions.

Rubriques

- Modèles composites personnalisés en ligne
- Modèles composites omponent-model-based personnalisés C
- Utilisation de chemins pour référencer les propriétés de modèles composites personnalisés

Modèles composites personnalisés en ligne

Les modèles composites personnalisés en ligne permettent d'organiser votre modèle d'actifs en regroupant les propriétés associées.

Supposons, par exemple, que vous souhaitiez modéliser un actif robotique. Le robot comprend un servomoteur, une alimentation électrique et une batterie. Chacun de ces éléments constitutifs possède ses propres propriétés que vous souhaitez inclure dans le modèle. Vous pouvez définir un modèle d'actif appelé `robot_model` qui possède des propriétés telles que les suivantes.

- `robot_model`
  - `servo_status` (entier)
  - `servo_position` (double)
  - `powersupply_status` (entier)
  - `powersupply_temperature` (double)
  - `battery_status` (entier)
  - `battery_charge` (double)

Toutefois, dans certains cas, il peut y avoir de nombreux sous-assemblages ou les sous-assemblages eux-mêmes peuvent avoir de nombreuses propriétés. Dans ces cas, le nombre de propriétés peut être tel qu'il devient difficile de les référencer et de les gérer dans une seule liste plate à la racine du modèle, comme dans l'exemple précédent.

Pour faire face à de telles situations, vous pouvez utiliser un modèle composite personnalisé en ligne pour regrouper les propriétés. Un modèle composite personnalisé en ligne est un modèle composite personnalisé qui définit ses propres propriétés. Par exemple, vous pouvez modéliser votre robot comme suit.

- `robot_model`
  - `servo`
    - `status`(entier)
    - `position`(double)
  - `powersupply`
    - `status`(entier)
    - `temperature` (double)
  - `battery`
    - `status`(entier)
    - `charge`(double)

Dans l'exemple précédent, `servopowersupply`, et `battery` sont les noms des modèles composites personnalisés en ligne définis dans le modèle `robot_model` d'actif. Chacun de ces modèles composites définit ensuite ses propres propriétés.

> **Note**
>
> Dans ce cas, chaque modèle composite personnalisé définit ses propres propriétés, de sorte que toutes les propriétés font partie du modèle de ressources lui-même (`robot_model`dans ce cas). Ces propriétés ne sont partagées avec aucun autre modèle d'actif ou modèle de composant. Par exemple, si vous avez créé un autre modèle d'actif qui portait également le nom de modèle composite personnalisé en ligne`servo`, le fait d'apporter une modification au modèle interne `servo` n'`robot_model`affecterait pas la `servo` définition de l'autre modèle d'actif.
>
> Si vous souhaitez implémenter un tel partage (par exemple, pour n'avoir qu'une seule définition pour un servo, que tous vos modèles d'actifs peuvent partager), vous devez plutôt créer un modèle de composant pour celui-ci, puis créer des modèles composites basés sur des modèles de composants qui le référencent. Consultez la section suivante pour plus de détails.

Pour plus d'informations sur la création de modèles composites personnalisés en ligne, consultezCréation de modèles composites personnalisés (composants).

Modèles composites omponent-model-based personnalisés C

Vous pouvez créer un modèle de composant AWS IoT SiteWise pour définir un sous-assemblage standard réutilisable. Une fois que vous avez créé un modèle de composant, vous pouvez y ajouter des références dans vos autres modèles d'actifs et modèles de composants. Pour ce faire, ajoutez un modèle composite component-model-based personnalisé à n'importe quel modèle dans lequel vous souhaitez référencer le composant. Vous pouvez ajouter des références à votre composant à partir de nombreux modèles ou à plusieurs reprises dans le même modèle.

De cette façon, vous pouvez éviter de dupliquer les mêmes définitions entre les modèles. Cela simplifie également la maintenance de vos modèles, car toute modification apportée à un modèle de composant sera répercutée sur tous les modèles d'actifs qui l'utilisent.

Supposons, par exemple, que votre installation industrielle possède de nombreux types d'équipements qui utilisent tous le même type de servomoteur. Certains d'entre eux ont de nombreux servomoteurs dans un seul équipement. Vous créez un modèle d'actif pour chaque type d'équipement, mais vous ne souhaitez pas dupliquer la définition à `servo` chaque fois. Vous souhaitez le modéliser une seule fois et l'utiliser dans vos différents modèles d'actifs. Si vous modifiez ultérieurement la définition de`servo`, elle sera mise à jour pour tous vos modèles et actifs.

Pour modéliser le robot de l'exemple précédent de cette manière, vous pouvez définir des servomoteurs, des alimentations et des batteries en tant que modèles de composants, comme ceci.

- `servo_component_model`
  - `status`(entier)
  - `position`(double)

- `powersupply_component_model`
  - `status`(entier)
  - `temperature` (double)

- `battery__component_model`
  - `status`(entier)
  - `charge`(double)

Vous pouvez ensuite définir des modèles d'actifs`robot_model`, tels que ceux qui font référence à ces composants. Plusieurs modèles d'actifs peuvent faire référence au même modèle de composant. Vous pouvez également référencer le même modèle de composant plusieurs fois dans un même modèle d'actif, par exemple si votre robot comporte plusieurs servomoteurs.

- `robot_model`
  - `servo1`(référence :`servo_component_model`)
  - `servo2`(référence :`servo_component_model`)
  - `servo3`(référence :`servo_component_model`)
  - `powersupply` (référence :`powersupply_component_model`)
  - `battery`(référence :`battery_component_model`)

Pour plus d'informations sur la création de modèles de composants, consultezCréation de modèles de composants.

Pour plus d'informations sur la façon de référencer vos modèles de composants dans d'autres modèles, consultezCréation de modèles composites personnalisés (composants).

Utilisation de chemins pour référencer les propriétés de modèles composites personnalisés

Lorsque vous créez une propriété sur un modèle d'actif, un modèle de composant ou un modèle composite personnalisé, vous pouvez la référencer à partir d'autres propriétés qui utilisent sa valeur, telles que les transformations et les métriques.

AWS IoT SiteWise vous propose différentes manières de référencer votre propriété. La méthode la plus simple consiste souvent à utiliser son identifiant de propriété. Toutefois, si la propriété que vous souhaitez référencer se trouve sur un modèle composite personnalisé, il peut être préférable de la référencer par chemin.

Un chemin est une séquence ordonnée de segments de chemin qui spécifie une propriété en termes de position parmi les modèles composites imbriqués au sein d'un modèle d'actif et d'un modèle composite.

Obtenir des chemins de propriété

Vous pouvez obtenir le chemin d'une propriété à partir du `path` champ de sa AssetModelpropriété.

Supposons, par exemple, que vous disposiez d'un modèle `robot_model` d'actif contenant un modèle `servo` composite personnalisé doté d'une propriété`position`. Si vous appelez DescribeAssetModelCompositeModel on`servo`, la `position` propriété listera un `path` champ qui ressemble à ceci :

```
"path": [
    {
       "id": "asset model ID",
       "name": "robot_model"
    },
    {
       "id": "composite model ID",
       "name": "servo"
    },
    {
       "id": "property ID",
       "name": "position"
```

```
    }
]
```

Utilisation des chemins de propriété

Vous pouvez utiliser un chemin de propriété lorsque vous définissez une propriété qui fait référence à d'autres propriétés, telles qu'une transformation ou une métrique.

Une propriété utilise une variable pour référencer une autre propriété. Pour plus d'informations sur l'utilisation des variables, consultezUtilisation de variables dans des expressions de formule.

Lorsque vous définissez une variable pour référencer une propriété, vous pouvez utiliser l'ID de la propriété ou son chemin.

Pour définir une variable qui utilise le chemin de la propriété référencée, spécifiez le `propertyPath` champ de sa valeur.

Par exemple, pour définir un modèle d'actif dont une métrique fait référence à une propriété à l'aide d'un chemin, vous pouvez transmettre une charge utile comme celle-ci à CreateAssetModel :

```
{
    ...
    "assetModelProperties": [
        {
            ...
            "type": {
                "metric": {
                    ...
                    "variables": [
                        {
                            "name": "variable name",
                            "value": {
                                "propertyPath": [
                                    path segments
                                ]
                            }
                        }
                    ],
                    ...
                }
            },
            ...
```

```
        },
        ...
    ],
    ...
}
```

Utilisation des identifiants d'objets

AWS IoT SiteWise définit différents types d'objets persistants, tels que les actifs, les modèles d'actifs, les propriétés et les hiérarchies. Tous ces objets possèdent des identifiants uniques que vous pouvez utiliser pour les récupérer, les mettre à jour et les supprimer.

AWS IoT SiteWise propose différentes options aux clients pour la création d'un identifiant. AWS IoT SiteWise en génère un pour vous par défaut au moment de la création de l'objet. Les utilisateurs peuvent également fournir leurs propres identifiants à vos objets.

Rubriques

- Utilisation des UUID d'objets
- Utilisation d'identifiants externes

Utilisation des UUID d'objets

Chaque objet persistant AWS IoT SiteWise possède un UUID pour l'identifier. Par exemple, les modèles d'actifs ont un ID de modèle d'actif, les actifs ont un ID d'actif, etc. Cet identifiant est attribué au moment de la création de l'objet et reste inchangé pendant toute la durée de vie de l'objet.

Lorsque vous créez un nouvel objet, il AWS IoT SiteWise génère un identifiant unique pour vous par défaut. Vous pouvez également fournir votre propre identifiant au moment de la création au format UUID.

> **Note**
>
> Les UUID doivent être globalement uniques dans la AWS région où ils ont été créés, et pour le même type d'objet. Lorsque vous AWS IoT SiteWise générez automatiquement un identifiant, celui-ci est toujours unique. Si vous choisissez votre propre identifiant, assurez-vous qu'il est unique.

Par exemple, si vous créez un nouveau modèle d'actif en appelant CreateAssetModel, vous pouvez fournir votre propre UUID dans le `assetModelId` champ facultatif de la demande.

En revanche, si vous omettez `assetModelId` de le faire dans la demande, AWS IoT SiteWise génère un UUID pour le nouveau modèle d'actif.

Utilisation d'identifiants externes

Pour définir votre propre identifiant dans un format autre que l'UUID, vous pouvez attribuer un identifiant externe. Par exemple, vous pouvez le faire si vous réutilisez un identifiant que vous utilisez dans un système qui ne l'est pas AWS, ou pour qu'il soit plus lisible par l'homme. Les identifiants externes ont un format plus flexible. Vous pouvez les utiliser pour référencer vos objets dans des opérations AWS IoT SiteWise d'API où vous utiliseriez autrement l'UUID.

Comme les UUID, chaque identifiant externe doit être unique dans son contexte. Par exemple, vous ne pouvez pas avoir deux modèles d'actifs avec le même ID externe. De plus, comme les UUID, un objet ne peut avoir qu'un seul identifiant externe au cours de sa durée de vie, qui ne peut pas changer.

Différences entre les identifiants externes et les UUID

Les identifiants externes diffèrent des UUID de la manière suivante :

- Chaque objet possède un UUID, mais les identifiants externes sont facultatifs.
- AWS IoT SiteWise ne génère jamais d'identifiants externes. Vous les fournissez vous-même.
- Si l'objet n'en possède pas déjà un, vous pouvez attribuer un identifiant externe à tout moment.

Format des identifiants externes

Un identifiant externe valide possède les propriétés suivantes :

- Comporte entre 2 et 128 caractères.
- Les premier et dernier caractères doivent être alphanumériques (A-Z, a-z, 0-9).
- Les caractères autres que le premier et le dernier doivent être alphanumériques ou être l'un des suivants : `_-.:`

Par exemple, un identifiant externe doit être conforme à l'expression régulière suivante :

`[a-zA-Z0-9][a-zA-Z0-9_\-.:]*[a-zA-Z0-9]+`

Référencement d'objets avec des identifiants externes

Dans de nombreux endroits où vous pouvez référencer un objet à l'aide de son UUID, vous pouvez utiliser son identifiant externe à la place, s'il en possède un. Pour ce faire, ajoutez l'ID externe à la chaîne`externalId:`.

Supposons, par exemple, que vous disposiez d'un modèle d'actif dont l'UUID (ID de modèle d'actif) est`a1b2c3d4-5678-90ab-cdef-11111EXAMPLE`, qui possède également l'ID externe. `myExternalId` Appelez DescribeAssetModel pour obtenir des informations à ce sujet. Vous pouvez utiliser l'une des valeurs suivantes comme valeur de `assetModelId` :

- Avec l'identifiant du modèle d'actif (UUID) lui-même : `a1b2c3d4-5678-90ab-cdef-11111EXAMPLE`
- Avec l'ID externe : `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**
>
> Le `externalId:` préfixe ne fait pas lui-même partie de l'identifiant externe. Vous devez uniquement fournir le préfixe lorsque vous fournissez un identifiant externe à une opération d'API qui accepte des UUID ou des identifiants externes. Par exemple, fournissez le préfixe lorsque vous interrogez ou mettez à jour un objet existant.
> Lorsque vous définissez un ID externe pour un objet, par exemple lorsque vous créez un modèle de ressource, n'incluez pas le préfixe.

Vous pouvez utiliser des identifiants externes à la place des UUID de cette manière pour de nombreuses opérations d'API AWS IoT SiteWise, mais pas pour toutes. Par exemple, le GetAssetPropertyValue, doit utiliser des UUID ; il ne prend pas en charge l'utilisation d'identifiants externes.

Pour déterminer si une opération d'API particulière prend en charge cette utilisation, consultez la référence des API.

Création de modèles d'actifs et de modèles de composants

AWS IoT SiteWise les modèles d'actifs et les modèles de composants favorisent la standardisation de vos données industrielles. Un modèle d'actif ou un modèle de composant contient un nom, une description, des propriétés d'actif et (éventuellement) des modèles composites personnalisés qui regroupent les propriétés ou qui font référence à des modèles de composants pour des sous-assemblages.

- Vous utilisez un modèle d'actifs pour créer des actifs. Outre les fonctionnalités répertoriées ci-dessus, un modèle d'actifs peut également contenir des définitions hiérarchiques qui définissent les relations entre les actifs.
- Un modèle de composant représente un sous-assemblage au sein d'un modèle d'actif ou d'un autre modèle de composant. Lorsque vous créez un modèle de composant, vous pouvez y ajouter des références dans des modèles d'actifs et dans d'autres modèles de composants. Toutefois, vous ne pouvez pas créer de ressources directement à partir de modèles de composants.

Après avoir créé un modèle d'actif ou un modèle de composant, vous pouvez créer des modèles composites personnalisés pour qu'il regroupe des propriétés ou fasse référence à des modèles de composants existants.

Pour plus d'informations sur la création de modèles d'actifs et de modèles de composants, consultez les sections suivantes.

Rubriques

- Création de modèles de ressources
- Création de modèles de composants
- Définition des propriétés des données
- Création de modèles composites personnalisés (composants)

Création de modèles de ressources

AWS IoT SiteWise les modèles d'actifs favorisent la standardisation de vos données industrielles. Un modèle de ressource contient un nom, une description, des propriétés de ressource et des définitions de hiérarchie de ressources. Par exemple, vous pouvez définir un modèle d'éolienne avec des propriétés de température, de rotation par minute (tr/min) et de puissance. Ensuite, vous pouvez

définir un modèle de parc éolien avec une propriété de puissance de sortie nette et une définition de hiérarchie d'éoliennes.

> **Note**
>
> - Nous vous recommandons de modéliser votre opération en commençant par les nœuds de niveau inférieur. Par exemple, créez votre modèle d'éolienne avant de créer votre modèle de parc éolien. Les définitions de hiérarchie des ressources contiennent des références à des modèles de ressources existants. En suivant cette approche, vous pouvez définir des hiérarchies de ressources lors de la création de vos modèles.
> - Les modèles d'actifs ne peuvent pas contenir d'autres modèles d'actifs. Si vous devez définir un modèle auquel vous pouvez faire référence en tant que sous-assemblage au sein d'un autre modèle, vous devez plutôt créer un modèle composant-->. Pour plus d'informations, consultez Création de modèles de composants.

Les sections suivantes décrivent comment utiliser la AWS IoT SiteWise console ou l'API pour créer des modèles d'actifs. Les sections suivantes décrivent également les différents types de propriétés et de hiérarchies de ressources que vous pouvez utiliser pour créer des modèles.

Rubriques

- Création d'un modèle de ressource (console)
- Création d'un modèle d'actifs (AWS CLI)
- Exemples de modèles de ressources
- Définition de hiérarchies de modèles d'actifs

Création d'un modèle de ressource (console)

Vous pouvez utiliser la AWS IoT SiteWise console pour créer un modèle d'actif. La AWS IoT SiteWise console fournit diverses fonctionnalités, telles que la saisie automatique des formules, qui peuvent vous aider à définir des modèles d'actifs valides.

Pour créer un modèle de ressource (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Models (Modèles).

3. Sélectionnez Create model.
4. Sur la page Créer un modèle, procédez comme suit :

   a. Saisissez un nom pour le modèle de ressource, tel que **`Wind Turbine`** ou **`Wind Turbine Model`**. Ce nom doit être unique pour tous les modèles de votre compte dans cette région.

   b. (Facultatif) Ajoutez un ID externe pour le modèle. Il s'agit d'un identifiant défini par l'utilisateur. Pour plus d'informations, consultez Référencement d'objets avec des identifiants externes dans le Guide de l'utilisateur AWS IoT SiteWise .

   c. (Facultatif) Ajoutez des définitions de mesures pour le modèle. Les mesures représentent des flux de données provenant de votre équipement. Pour plus d'informations, consultez Définition des flux de données provenant des équipements (mesures).

   d. (Facultatif) Ajoutez des définitions de transformations pour le modèle. Les transformations sont des formules qui font correspondre les données d'un formulaire à un autre. Pour plus d'informations, consultez Transformation des données (transformations).

   e. (Facultatif) Ajoutez des définitions de métriques pour le modèle. Les métriques sont des formules qui regroupent les données sur des intervalles de temps. Les métriques peuvent saisir des données provenant des actifs associés, afin que vous puissiez calculer des valeurs représentant votre activité ou un sous-ensemble de celle-ci. Pour plus d'informations, consultez Agrégation de données provenant de propriétés et d'autres actifs (métriques).

   f. (Facultatif) Ajoutez des définitions de hiérarchies pour le modèle. Les hiérarchies sont des relations entre les actifs. Pour plus d'informations, consultez Définition de hiérarchies de modèles d'actifs.

   g. (Facultatif) Ajoutez des balises pour le modèle de ressource. Pour plus d'informations, consultez Marquer vos ressources AWS IoT SiteWise.

   h. Sélectionnez Create model.

   Lorsque vous créez un modèle de ressource, la AWS IoT SiteWise console accède à la page du nouveau modèle. Sur cette page, vous pouvez voir l'état du modèle, qui est initialement CRÉATION. Cette page est automatiquement mise à jour, de sorte que vous pouvez attendre la mise à jour de l'état du modèle.

> **Note**
>
> Le processus de création de modèles de ressources peut prendre jusqu'à quelques minutes pour les modèles complexes. Une fois que le statut du modèle d'actif est ACTIF, vous pouvez utiliser le modèle d'actif pour créer des actifs. Pour plus d'informations, consultez État des ressources et des modèles.

5. (Facultatif) Après avoir créé votre modèle d'actif, vous pouvez configurer votre modèle d'actif pour la périphérie. Pour plus d'informations sur SiteWise Edge, consultezPermettre le traitement des données de pointe.

   a. Sur la page du modèle, choisissez Configurer pour Edge.

   b. Sur la page de configuration du modèle, choisissez la configuration des bords pour votre modèle. Cela contrôle les endroits où les propriétés associées à ce modèle d'actif AWS IoT SiteWise peuvent être calculées et stockées. Pour plus d'informations sur la configuration de votre modèle pour le bord, consultezthe section called “Configuration de la fonctionnalité Edge”.

   c. Pour la configuration personnalisée de la périphérie, choisissez l'emplacement où vous AWS IoT SiteWise souhaitez calculer et stocker chacune des propriétés de votre modèle d'actifs.

      > **Note**
      >
      > Les transformations et les métriques associées doivent être configurées pour le même emplacement. Pour plus d'informations sur la configuration de votre modèle pour le bord, consultezthe section called “Configuration de la fonctionnalité Edge”.

   d. Choisissez Enregistrer. Sur la page du modèle, votre configuration Edge doit maintenant être configurée.

Création d'un modèle d'actifs (AWS CLI)

Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour créer un modèle d'actif.

Utilisez l'opération CreateAssetModel pour créer un modèle d'actif avec des propriétés et des hiérarchies. Cette opération attend une charge utile avec la structure suivante.

```
{
  "assetModelType": "ASSET_MODEL",
  "assetModelName": "String",
  "assetModelDescription": "String",
  "assetModelProperties": Array of AssetModelProperty,
  "assetModelHierarchies": Array of AssetModelHierarchyDefinition
}
```

Pour créer un modèle d'actif (AWS CLI)

1. Créez un fichier nommé `asset-model-payload.json` et copiez l'objet JSON suivant dans le fichier.

   ```
   {
     "assetModelType": "ASSET_MODEL",
     "assetModelName": "",
     "assetModelDescription": "",
     "assetModelProperties": [

     ],
     "assetModelHierarchies": [

     ],
     "assetModelCompositeModels": [

     ]
   }
   ```

2. Utilisez votre éditeur de texte JSON préféré pour modifier le fichier `asset-model-payload.json` pour les éléments suivants :

   a. Saisissez un nom (`assetModelName`) pour le modèle de ressource, tel que **`Wind Turbine`** ou **`Wind Turbine Model`**. Ce nom doit être unique pour tous les modèles d'actifs et modèles de composants de votre compte Région AWS.

   b. (Facultatif) Entrez un ID externe (`assetModelExternalId`) pour le modèle d'actif. Il s'agit d'un identifiant défini par l'utilisateur. Pour plus d'informations, consultez Référencement d'objets avec des identifiants externes dans le Guide de l'utilisateur AWS IoT SiteWise .

   c. (Facultatif) Saisissez une description (`assetModelDescription`) pour le modèle de ressource ou supprimez la paire clé-valeur `assetModelDescription`.

d. (Facultatif) Définissez les propriétés de ressources (`assetModelProperties`) pour le modèle. Pour plus d'informations, consultez Définition des propriétés des données.

e. (Facultatif) Définissez les hiérarchies de ressources (`assetModelHierarchies`) pour le modèle. Pour plus d'informations, consultez Définition de hiérarchies de modèles d'actifs.

f. (Facultatif) Définissez les alarmes pour le modèle. Les alarmes surveillent d'autres propriétés afin que vous puissiez identifier les équipements ou les processus nécessitant une attention particulière. Chaque définition d'alarme est un modèle composite (`assetModelCompositeModels`) qui normalise l'ensemble de propriétés utilisées par l'alarme. Pour plus d'informations, consultez Surveillance des données à l'aide d'alarmes et Définition des alarmes sur les modèles d'actifs.

g. (Facultatif) Ajoutez des balises (`tags`) pour le modèle de ressource. Pour plus d'informations, consultez Marquer vos ressources AWS IoT SiteWise.

3. Exécutez la commande suivante pour créer un modèle de ressource à partir de la définition du fichier JSON.

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

L'opération renvoie une réponse qui contient l'élément `assetModelId` auquel vous faites référence lors de la création d'une ressource. La réponse contient également l'état du modèle (`assetModelStatus.state`), qui est initialement `CREATING`. L'état du modèle de ressource correspond à `CREATING` jusqu'à ce que les modifications se propagent.

> **Note**
>
> Le processus de création de modèles de ressources peut prendre jusqu'à quelques minutes pour les modèles complexes. Pour vérifier l'état actuel de votre modèle d'actif, utilisez l'opération DescribeAssetModèle en spécifiant le`assetModelId`. Une fois que le statut du modèle de ressource est `ACTIVE`, vous pouvez l'utiliser pour créer des ressources. Pour plus d'informations, consultez État des ressources et des modèles.

4. (Facultatif) Créez des modèles composites personnalisés pour votre modèle d'actif. Avec les modèles composites personnalisés, vous pouvez regrouper les propriétés au sein du modèle ou inclure un sous-assemblage en faisant référence à un modèle de composant. Pour plus d'informations, consultez Création de modèles composites personnalisés (composants).

Exemples de modèles de ressources

Cette section contient des exemples de définitions de modèles d'actifs que vous pouvez utiliser pour créer des modèles d'actifs avec les AWS IoT SiteWise SDK AWS CLI et. Ces modèles d'actifs représentent une éolienne et un parc éolien. Les actifs des éoliennes ingèrent les données brutes des capteurs et calculent des valeurs telles que la puissance et la vitesse moyenne du vent. Les actifs du parc éolien calculent des valeurs telles que la puissance totale de toutes les éoliennes du parc éolien.

Rubriques

- Modèle de ressource d'éolienne
- Modèle de ressource de parc éolien

Modèle de ressource d'éolienne

Le modèle de ressource suivant représente une éolienne dans un parc éolien. L'éolienne ingère les données des capteurs pour calculer des valeurs telles que la puissance et la vitesse moyenne du vent.

> **Note**
>
> Cet exemple de modèle ressemble au modèle d'éolienne de la AWS IoT SiteWise démo. Pour plus d'informations, consultez Utilisation de la AWS IoT SiteWise démo.

```
{
  "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": []
}
```

Modèle de ressource de parc éolien

Le modèle de ressource suivant représente un parc éolien qui comprend plusieurs éoliennes. Ce modèle d'actif définit une hiérarchie par rapport au modèle d'éolienne. Cela permet au parc éolien de calculer des valeurs (telles que la puissance moyenne) à partir des données de toutes les éoliennes du parc éolien.

> **Note**
>
> Cet exemple de modèle ressemble au modèle de parc éolien présenté dans la AWS IoT SiteWise démo. Pour plus d'informations, consultez Utilisation de la AWS IoT SiteWise démo.

Ce modèle de ressource dépend du Modèle de ressource d'éolienne. Remplacez les valeurs `propertyId` et `childAssetModelId` par celles d'un modèle de ressource d'éolienne existant.

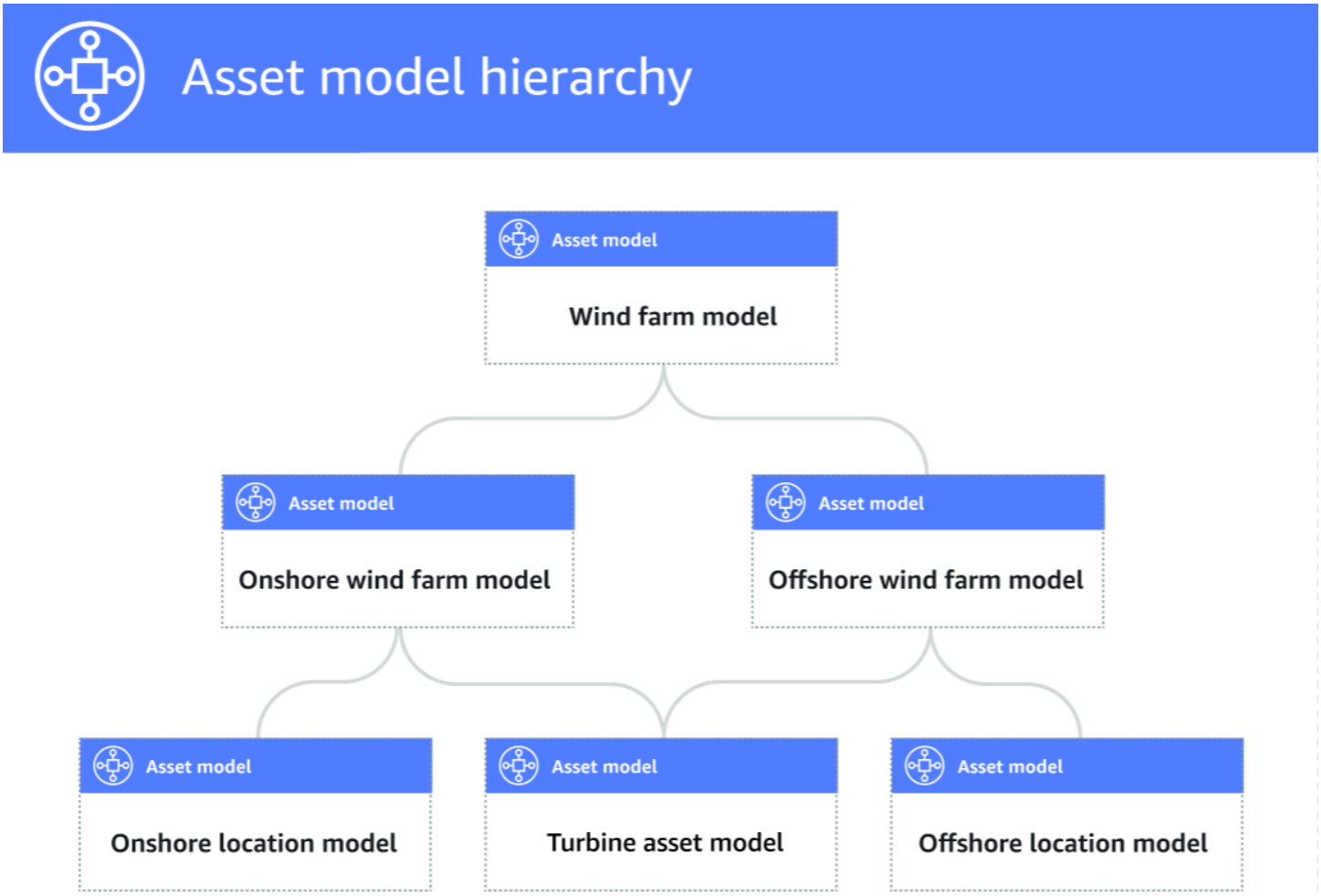
```
{
  "assetModelName": "Wind Farm Asset Model",
  "assetModelDescription": "Represents a wind farm.",
  "assetModelProperties": [
    {
      "name": "Code",
      "dataType": "INTEGER",
      "type": {
        "attribute": {
          "defaultValue": "300"
        }
      }
    },
    {
      "name": "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"
    }
  ]
}
```

Définition de hiérarchies de modèles d'actifs

Vous pouvez définir des hiérarchies de modèles d'actifs afin de créer des associations logiques entre les modèles d'actifs de votre exploitation industrielle. Par exemple, vous pouvez définir un parc éolien composé de parcs éoliens terrestres et offshore. Un parc éolien terrestre comprend une turbine et un emplacement à terre. Un parc éolien en mer contient une turbine et un emplacement en mer.



Lorsque vous associez un modèle d'actif enfant à un modèle d'actif parent par le biais d'une hiérarchie, les métriques du modèle d'actif parent peuvent entrer des données à partir des métriques du modèle d'actif enfant. Vous pouvez utiliser les hiérarchies et les métriques des modèles d'actifs pour calculer des statistiques qui fournissent un aperçu de votre activité ou d'un sous-ensemble de celle-ci. Pour plus d'informations, consultez Agrégation de données provenant de propriétés et d'autres actifs (métriques).

Chaque hiérarchie définit une relation entre un modèle d'actif parent et un modèle d'actif enfant. Dans un modèle d'actif parent, vous pouvez définir plusieurs hiérarchies pour le même modèle d'actif enfant. Par exemple, si vous avez deux types d'éoliennes différents dans vos parcs éoliens, où toutes les éoliennes sont représentées par le même modèle d'actif, vous pouvez définir une hiérarchie pour chaque type. Vous pouvez ensuite définir des mesures dans le modèle de parc éolien afin de calculer des statistiques indépendantes et combinées pour chaque type d'éolienne.

Un modèle d'actif parent peut être associé à plusieurs modèles d'actifs enfants. Par exemple, si vous avez un parc éolien terrestre et un parc éolien offshore représentés par deux modèles d'actifs différents, vous pouvez associer ces modèles d'actifs au même modèle d'actif de parc éolien parent.

Un modèle d'actif enfant peut également être associé à plusieurs modèles d'actifs parents. Par exemple, si vous avez deux types de parcs éoliens différents, où toutes les éoliennes sont représentées par le même modèle d'actif, vous pouvez associer le modèle d'actif d'éolienne à différents modèles d'actifs de parcs éoliens.

> **Note**
>
> Lorsque vous définissez une hiérarchie de modèles d'actifs, le modèle d'actif enfant doit être `ACTIVE` ou avoir une `ACTIVE` version précédente. Pour plus d'informations, consultez État des ressources et des modèles.

Après avoir défini des modèles de ressources hiérarchiques et créé des ressources, vous pouvez associer les ressources pour terminer la relation parent-enfant. Pour plus d'informations, consultez Création de ressources et Association et dissociation de ressources.

Rubriques

- Définition de hiérarchies de modèles d'actifs (console)
- Définition des hiérarchies d'actifs ()AWS CLI

Définition de hiérarchies de modèles d'actifs (console)

Lorsque vous définissez une hiérarchie pour un modèle d'actif dans la AWS IoT SiteWise console, vous spécifiez les paramètres suivants :

- Nom de la hiérarchie : nom de la hiérarchie, par exemple**`Wind Turbines`**.
- Modèle hiérarchique : modèle d'actif enfant.
- ID externe de hiérarchie (facultatif) : il s'agit d'un identifiant défini par l'utilisateur. Pour plus d'informations, consultez Référencement d'objets avec des identifiants externes dans le Guide de l'utilisateur AWS IoT SiteWise .

Pour plus d'informations, consultez Création d'un modèle de ressource (console).

Définition des hiérarchies d'actifs ()AWS CLI

Lorsque vous définissez une hiérarchie pour un modèle d'actif à l'aide de l' AWS IoT SiteWise API, vous spécifiez les paramètres suivants :

- `name`— Le nom de la hiérarchie, par exemple**`Wind Turbines`**.
- `childAssetModelId`— L'ID ou l'ID externe du modèle d'actif enfant pour la hiérarchie. Vous pouvez utiliser l'opération ListAssetModèles pour trouver l'ID d'un modèle d'actif existant.

Example Exemple de définition de hiérarchie

L'exemple suivant illustre une hiérarchie de modèles d'actifs qui représente la relation entre un parc éolien et les éoliennes. Cet objet est un exemple de AssetModelhiérarchie. Pour plus d'informations, consultez Création d'un modèle d'actifs (AWS CLI).

```
{
  ...
  "assetModelHierarchies": [
    {
      "name": "Wind Turbines",
      "childAssetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE"
    },
  ]
}
```

Création de modèles de composants

Utilisez des modèles de AWS IoT SiteWise composants pour définir des sous-assemblages auxquels vous pouvez faire référence à partir de modèles de ressources ou d'autres modèles de composants. De cette façon, vous pouvez réutiliser la définition du composant dans plusieurs autres modèles, ou plusieurs fois dans le même modèle.

Le processus de définition d'un modèle de composant est très similaire à celui d'un modèle d'actif. Tout comme un modèle d'actif, un modèle de composant possède un nom, une description et des propriétés d'actif. Toutefois, les modèles de composants ne peuvent pas inclure de définitions de hiérarchie des actifs, car les modèles de composants eux-mêmes ne peuvent pas être utilisés pour créer directement des actifs. Les modèles de composants ne peuvent pas non plus définir d'alarmes.

Par exemple, vous pouvez définir un composant pour un servomoteur avec des propriétés de température du moteur, de température du codeur et de résistance d'isolement. Vous pouvez ensuite

définir un modèle d'actif pour les équipements contenant des servomoteurs, tels qu'une machine à commande numérique.

> **Note**
>
> - Nous vous recommandons de modéliser votre opération en commençant par les nœuds de niveau inférieur. Par exemple, créez le composant de votre servomoteur avant de créer le modèle d'actif de votre machine CNC. Les modèles d'actifs contiennent des références à des modèles de composants existants.
> - Vous ne pouvez pas créer un actif directement à partir d'un modèle de composant. Pour créer un actif qui utilise votre composant, vous devez créer un modèle d'actif pour votre actif. Ensuite, vous créez un modèle composite personnalisé qui fait référence à votre composant. Pour plus d'informations sur la création de modèles d'actifs, voir Création de modèles de ressources Pour plus d'informations sur la création de modèles composites personnalisés, voirCréation de modèles composites personnalisés (composants).

Les sections suivantes décrivent comment utiliser l' AWS IoT SiteWise API pour créer des modèles de composants.

Rubriques

- Création d'un modèle de composant (AWS CLI)
- Exemple de modèle de composant

Création d'un modèle de composant (AWS CLI)

Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour créer un modèle de composant.

Utilisez l'opération CreateAssetModel pour créer un modèle de composant doté de propriétés. Cette opération attend une charge utile dont la structure est la suivante :

```
{
  "assetModelType": "COMPONENT_MODEL",
  "assetModelName": "String",
  "assetModelDescription": "String",
  "assetModelProperties": Array of AssetModelProperty,
```

```
}
```

Pour créer un modèle de composant (AWS CLI)

1. Créez un fichier appelé, `component-model-payload.json` puis copiez l'objet JSON suivant dans le fichier :

   ```
   {
     "assetModelType": "COMPONENT_MODEL",
     "assetModelName": "",
     "assetModelDescription": "",
     "assetModelProperties": [

     ]
   }
   ```

2. Utilisez votre éditeur de texte JSON préféré pour modifier le fichier `component-model-payload.json` pour les éléments suivants :

   a. Entrez un nom (`assetModelName`) pour le modèle de composant, tel que **`Servo Motor`** ou**`Servo Motor Model`**. Ce nom doit être unique pour tous les modèles d'actifs et modèles de composants de votre compte Région AWS.

   b. (Facultatif) Entrez un ID externe (`assetModelExternalId`) pour le modèle de composant. Il s'agit d'un identifiant défini par l'utilisateur. Pour plus d'informations, consultez Référencement d'objets avec des identifiants externes dans le Guide de l'utilisateur AWS IoT SiteWise .

   c. (Facultatif) Saisissez une description (`assetModelDescription`) pour le modèle de ressource ou supprimez la paire clé-valeur `assetModelDescription`.

   d. (Facultatif) Définissez les propriétés des actifs (`assetModelProperties`) pour le modèle de composant. Pour plus d'informations, consultez Définition des propriétés des données.

   e. (Facultatif) Ajoutez des balises (`tags`) pour le modèle de ressource. Pour plus d'informations, consultez Marquer vos ressources AWS IoT SiteWise.

3. Exécutez la commande suivante pour créer un modèle de composant à partir de la définition du fichier JSON.

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

L'opération renvoie une réponse contenant ce à quoi vous `assetModelId` faites référence lorsque vous ajoutez une référence à votre modèle de composant dans un modèle d'actif ou un autre modèle de composant. La réponse contient également l'état du modèle (`assetModelStatus.state`), qui est initialement `CREATING`. L'état du modèle de composant est maintenu `CREATING` jusqu'à ce que les modifications se propagent.

> **Note**
>
> Le processus de création de modèles de composants peut prendre jusqu'à quelques minutes pour les modèles complexes. Pour vérifier l'état actuel de votre modèle de composant, utilisez l'opération DescribeAssetModel en spécifiant le`assetModelId`. Une fois que le statut du modèle de composant est `ACTIVE` défini, vous pouvez ajouter des références à votre modèle de composant dans des modèles d'actifs ou d'autres modèles de composants. Pour plus d'informations, consultez État des ressources et des modèles.

4. (Facultatif) Créez des modèles composites personnalisés pour votre modèle de composant. Avec les modèles composites personnalisés, vous pouvez regrouper les propriétés au sein du modèle ou inclure un sous-assemblage en faisant référence à un autre modèle de composant. Pour plus d'informations, consultez Création de modèles composites personnalisés (composants).

Exemple de modèle de composant

Cette section contient un exemple de définition de modèle de composant que vous pouvez utiliser pour créer un modèle de composant avec les AWS IoT SiteWise SDK AWS CLI et. Ce modèle de composant représente un servomoteur qui peut être utilisé dans un autre équipement, tel qu'une machine à commande numérique.

Rubriques

- Modèle de composant du servomoteur

Modèle de composant du servomoteur

Le modèle de composant suivant représente un servomoteur qui peut être utilisé dans des équipements tels que des machines à commande numérique. Le servomoteur fournit diverses mesures, telles que les températures et la résistance électrique. Ces mesures sont disponibles sous

forme de propriétés sur des actifs créés à partir de modèles d'actifs faisant référence au modèle de composant du servomoteur.

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

Définition des propriétés des données

Les propriétés des actifs sont les structures de chaque actif qui contiennent des données sur les actifs. Les propriétés des ressources peuvent être l'un des types suivants :

- Attributs : propriétés généralement statiques d'un actif, telles que le fabricant de l'appareil ou la région géographique. Pour plus d'informations, consultez Définition de données statiques (attributs).
- Mesures — Les flux de données brutes des capteurs de l'appareil d'un actif, tels que les valeurs de vitesse de rotation horodatées ou les valeurs de température horodatées en degrés Celsius. Une mesure est définie par un alias de flux de données. Pour plus d'informations, consultez Définition des flux de données provenant des équipements (mesures).
- Transformations : valeurs de série chronologique transformées d'un actif, telles que les valeurs de température horodatées en degrés Fahrenheit. Une transformation est définie par une expression

et les variables à consommer avec cette expression. Pour plus d'informations, consultez Transformation des données (transformations).

- Métriques : données d'un actif agrégées sur un intervalle de temps spécifié, tel que la température moyenne horaire. Une métrique est définie par un intervalle de temps, une expression et les variables à consommer avec cette expression. Les expressions métriques peuvent saisir les propriétés métriques des actifs associés, afin que vous puissiez calculer des mesures représentant votre activité ou un sous-ensemble de celle-ci. Pour plus d'informations, consultez Agrégation de données provenant de propriétés et d'autres actifs (métriques).

Pour plus d'informations, consultez Création de modèles de ressources.

Pour obtenir un exemple d'utilisation des mesures, des transformations et des métriques pour calculer l'efficacité globale de l'équipement (OEE), veuillez consulter Calcul de l'OEE dans AWS IoT SiteWise.

Rubriques

- Définition de données statiques (attributs)
- Définition des flux de données provenant des équipements (mesures)
- Transformation des données (transformations)
- Agrégation de données provenant de propriétés et d'autres actifs (métriques)
- Utilisation d'expressions de formule

Définition de données statiques (attributs)

Les attributs des actifs représentent des informations généralement statiques, telles que le fabricant de l'appareil ou l'emplacement géographique. Chaque ressource que vous créez à partir d'un modèle de ressource contient les attributs de ce modèle.

Rubriques

- Définition des attributs (console)
- Définition des attributs (AWS CLI)

Définition des attributs (console)

Lorsque vous définissez un attribut pour un modèle de ressource dans la AWS IoT SiteWise console, vous spécifiez les paramètres suivants :

- Nom : nom de la propriété.
- Valeur par défaut — (Facultatif) La valeur par défaut de cet attribut. Les ressources créées à partir du modèle ont cette valeur pour l'attribut. Pour de plus amples informations sur la façon de remplacer la valeur par défaut dans une ressource créée à partir d'un modèle, veuillez consulter Mise à jour des valeurs d'attribut.
- Type de données : type de données de la propriété, qui est l'un des suivants :
  - String — Chaîne de 1024 octets maximum.
  - Entier — Un entier signé de 32 bits dont la plage est comprise entre [-2 147 483 648, 2 147 483 647].
  - Double : nombre à virgule flottante avec une plage [-10^100, 10^100] et une double précision IEEE 754.
  - Boolean — **`true`** ou. `false`
- ID externe — (Facultatif) Il s'agit d'un identifiant défini par l'utilisateur. Pour plus d'informations, consultez Référencement d'objets avec des identifiants externes dans le Guide de l'utilisateur AWS IoT SiteWise .

Pour plus d'informations, consultez Création d'un modèle de ressource (console).

Définition des attributs (AWS CLI)

Lorsque vous définissez un attribut pour un modèle d'actif avec l' AWS IoT SiteWise API, vous spécifiez les paramètres suivants :

- `name`— Le nom de la propriété.
- `defaultValue`— (Facultatif) La valeur par défaut de cet attribut. Les ressources créées à partir du modèle ont cette valeur pour l'attribut. Pour de plus amples informations sur la façon de remplacer la valeur par défaut dans une ressource créée à partir d'un modèle, veuillez consulter Mise à jour des valeurs d'attribut.
- `dataType`— Le type de données de la propriété, qui est l'un des suivants :
  - `STRING`— Chaîne de 1024 octets maximum.
  - `INTEGER`— Un entier signé de 32 bits dont la plage est comprise entre [-2 147 483 648, 2 147 483 647].
  - `DOUBLE`— Un nombre à virgule flottante avec une plage [-10^100, 10^100] et une double précision IEEE 754.
  - `BOOLEAN`— `true` ou`false`.

- `externalId`— (Facultatif) Il s'agit d'un identifiant défini par l'utilisateur. Pour plus d'informations, consultez Référencement d'objets avec des identifiants externes dans le Guide de l'utilisateur AWS IoT SiteWise .

Example Exemple de définition d'attribut

L'exemple suivant illustre un attribut qui représente le numéro de modèle d'une ressource avec une valeur par défaut. Cet objet est un exemple de AssetModelpropriété contenant un attribut. Vous pouvez spécifier cet objet dans le cadre de la charge utile de la demande de CreateAssetmodèle pour créer une propriété d'attribut. Pour plus d'informations, consultez Création d'un modèle d'actifs (AWS CLI).

```
{
...
"assetModelProperties": [
{
  "name": "Model number",
  "dataType": "STRING",
  "type": {
    "attribute": {
      "defaultValue": "BLT123"
    }
  }
}
],
...
}
```

Définition des flux de données provenant des équipements (mesures)

Une mesure représente le flux de données brutes du capteur d'un appareil, tel que les valeurs de température horodatées ou les valeurs de rotations par minute (RPM) horodatées.

Rubriques

- Définition des mesures (console)
- Définition des mesures (AWS CLI)

Définition des mesures (console)

Lorsque vous définissez une mesure pour un modèle d'actif dans la AWS IoT SiteWise console, vous spécifiez les paramètres suivants :

- Nom : nom de la propriété.
- Unité — (Facultatif) L'unité scientifique de la propriété, telle que mm ou Celsius.
- Type de données : type de données de la propriété, qui est l'un des suivants :
  - String — Chaîne de 1024 octets maximum.
  - Entier — Un entier signé de 32 bits dont la plage est comprise entre [-2 147 483 648, 2 147 483 647].
  - Double : nombre à virgule flottante avec une plage [-10^100, 10^100] et une double précision IEEE 754.
  - Boolean — **`true`** ou. `false`
- ID externe — (Facultatif) Il s'agit d'un identifiant défini par l'utilisateur. Pour plus d'informations, consultez Référencement d'objets avec des identifiants externes dans le Guide de l'utilisateur AWS IoT SiteWise .

Pour plus d'informations, consultez Création d'un modèle de ressource (console).

Définition des mesures (AWS CLI)

Lorsque vous définissez une mesure pour un modèle d'actif à l'aide de l' AWS IoT SiteWise API, vous spécifiez les paramètres suivants :

- `name`— Le nom de la propriété.
- `dataType`— Le type de données de la propriété, qui est l'un des suivants :
  - `STRING`— Chaîne de 1024 octets maximum.
  - `INTEGER`— Un entier signé de 32 bits dont la plage est comprise entre [-2 147 483 648, 2 147 483 647].
  - `DOUBLE`— Un nombre à virgule flottante avec une plage [-10^100, 10^100] et une double précision IEEE 754.
  - `BOOLEAN`— `true` ou`false`.
- `unit`— (Facultatif) L'unité scientifique de la propriété, telle que mm ou Celsius.

- `externalId`— (Facultatif) Il s'agit d'un identifiant défini par l'utilisateur. Pour plus d'informations, consultez Référencement d'objets avec des identifiants externes dans le Guide de l'utilisateur AWS IoT SiteWise .

Example Exemple de définition de mesure

L'exemple suivant illustre une mesure qui représente les lectures du capteur de température d'une ressource. Cet objet est un exemple de AssetModelpropriété contenant une mesure. Vous pouvez spécifier cet objet dans le cadre de la charge utile de la demande de CreateAssetmodèle pour créer une propriété de mesure. Pour plus d'informations, consultez Création d'un modèle d'actifs (AWS CLI).

La structure de mesure est une structure vide lorsque vous définissez un modèle d'actif, car vous configurez ultérieurement chaque actif pour utiliser des flux de données d'appareils uniques. Pour plus d'informations sur la façon de connecter la propriété de mesure d'un actif au flux de données du capteur d'un appareil, consultezMappage des flux de données industrielles avec des propriétés de ressources.

```
{
      ...
      "assetModelProperties": [
      {
          "name": "Temperature C",
          "dataType": "DOUBLE",
          "type": {
              "measurement": {}
          },
          "unit": "Celsius"
      }
  ],
      ...
}
```

Transformation des données (transformations)

Les transformations sont des expressions mathématiques qui mappent les points de données des propriétés des actifs d'un formulaire à l'autre. Une expression de transformation comprend des variables de propriété d'actif, des littéraux, des opérateurs et des fonctions. Les points de données transformés entretiennent une one-to-one relation avec les points de données d'entrée. AWS IoT

SiteWise calcule un nouveau point de données transformé chaque fois que l'une des propriétés d'entrée reçoit un nouveau point de données.

Par exemple, si votre ressource a un flux de mesure de température nommé `Temperature_C` avec des unités en Celsius, vous pouvez convertir chaque point de données en Fahrenheit avec la formule `Temperature_F = 9/5 * Temperature_C + 32`. Chaque fois qu'un point de données est AWS IoT SiteWise reçu dans le flux de `Temperature_C` mesure, la `Temperature_F` valeur correspondante est calculée en quelques secondes et disponible en tant que `Temperature_F` propriété.

Si votre transformation contient plusieurs variables, le point de données qui arrive le plus tôt lance immédiatement le calcul. Prenons l'exemple d'un fabricant de pièces utilisant une transformation pour contrôler la qualité de ses produits. En utilisant une norme différente basée sur le type de pièce, le fabricant utilise les mesures suivantes pour représenter le processus :

- `Part_Number`- Chaîne identifiant le type de pièce.
- `Good_Count`- Un entier qui augmente d'un si la pièce répond à la norme.
- `Bad_Count`- Un entier qui augmente d'un si la pièce ne répond pas à la norme.

Le fabricant crée également une transformation`Quality_Monitor`, qui équivaut à `if(eq(Part_Number, "BLT123") and (Bad_Count / (Good_Count + Bad_Count) > 0.1), "Caution", "Normal")`.

Cette transformation surveille le pourcentage de pièces défectueuses produites pour un type de pièce spécifique. Si le numéro de pièce est BLT123 et que le pourcentage de pièces défectueuses dépasse 10 % (0,1), la transformation est renvoyée. `"Caution"` Dans le cas contraire, la transformation est renvoyée`"Normal"`.

> **Note**
>
> - Si `Part_Number` elle reçoit un nouveau point de données avant les autres mesures, la `Quality_Monitor` transformation utilise la nouvelle `Part_Number` valeur et les dernières `Bad_Count` valeurs `Good_Count` et. Pour éviter les erreurs, effectuez une réinitialisation `Good_Count` et `Bad_Count` avant le prochain cycle de fabrication.
> - Utilisez des métriques si vous souhaitez évaluer les expressions uniquement lorsque toutes les variables ont reçu de nouveaux points de données.

Rubriques

- Définition des transformations (console)
- Définition des transformations (AWS CLI)

Définition des transformations (console)

Lorsque vous définissez une transformation pour un modèle d'actif dans la AWS IoT SiteWise console, vous spécifiez les paramètres suivants :

- Nom : nom de la propriété.
- Unité — (Facultatif) L'unité scientifique de la propriété, telle que mm ou Celsius.
- Type de données : type de données de la transformation, qui peut être double ou chaîne.
- ID externe — (Facultatif) Il s'agit d'un identifiant défini par l'utilisateur. Pour plus d'informations, consultez Référencement d'objets avec des identifiants externes dans le Guide de l'utilisateur AWS IoT SiteWise .
- Formule — L'expression de transformation. Les expressions de transformation ne peuvent pas utiliser de fonctions d'agrégation ou de fonctions temporelles. Pour ouvrir la fonction de saisie automatique, commencez à taper ou appuyez sur la flèche vers le bas. Pour plus d'informations, consultez Utilisation d'expressions de formule.

> **Important**
>
> Les transformations peuvent saisir des propriétés de type entier, double, booléen ou chaîne. Les booléens sont convertis en `0` (faux) et `1` (vrai).
> Les transformations doivent saisir une ou plusieurs propriétés qui ne sont pas des attributs et un certain nombre de propriétés d'attribut. AWS IoT SiteWise calcule un nouveau point de données transformé chaque fois que la propriété d'entrée qui n'est pas un attribut reçoit un nouveau point de données. Les nouvelles valeurs d'attribut ne lancent pas les mises à jour de transformation. Le même taux de demande pour les opérations de l'API de données relatives aux propriétés des actifs s'applique aux résultats des calculs de transformation.
> Les expressions de formule ne peuvent générer que des valeurs doubles ou des valeurs de chaîne. Les expressions imbriquées peuvent générer d'autres types de données, tels que des chaînes, mais la formule dans son ensemble doit être évaluée à un nombre ou à une chaîne. Vous pouvez utiliser la fonction jp pour convertir une chaîne en nombre. La valeur

booléenne doit être 1 (vrai) ou 0 (faux). Pour plus d'informations, consultez Valeurs non définies, infinies et en dépassement.

Pour plus d'informations, consultez Création d'un modèle de ressource (console).

Définition des transformations (AWS CLI)

Lorsque vous définissez une transformation pour un modèle d'actif à l'aide de l' AWS IoT SiteWise API, vous spécifiez les paramètres suivants :

- `name`— Le nom de la propriété.
- `unit`— (Facultatif) L'unité scientifique de la propriété, telle que mm ou Celsius.
- `dataType`— Le type de données de la transformation, qui doit être `DOUBLE` ou`STRING`.
- `externalId`— (Facultatif) Il s'agit d'un identifiant défini par l'utilisateur. Pour plus d'informations, consultez Référencement d'objets avec des identifiants externes dans le Guide de l'utilisateur AWS IoT SiteWise .
- `expression`— L'expression de transformation. Les expressions de transformation ne peuvent pas utiliser de fonctions d'agrégation ou de fonctions temporelles. Pour plus d'informations, consultez Utilisation d'expressions de formule.
- `variables`— La liste des variables qui définit les autres propriétés de votre actif à utiliser dans l'expression. Chaque structure de variable contient un nom simple à utiliser dans l'expression et une structure `value` qui identifie la propriété à lier à cette variable. La structure `value` contient les informations suivantes :
  - `propertyId`— L'ID de la propriété à partir de laquelle les valeurs doivent être saisies. Vous pouvez utiliser le nom de la propriété au lieu de son ID.

> **Important**
>
> Les transformations peuvent saisir des propriétés de type entier, double, booléen ou chaîne. Les booléens sont convertis en `0` (faux) et `1` (vrai).
> Les transformations doivent saisir une ou plusieurs propriétés qui ne sont pas des attributs et un certain nombre de propriétés d'attribut. AWS IoT SiteWise calcule un nouveau point de données transformé chaque fois que la propriété d'entrée qui n'est pas un attribut reçoit un nouveau point de données. Les nouvelles valeurs d'attribut ne lancent pas les mises à jour de transformation. Le même taux de demande pour les opérations de l'API de données relatives aux propriétés des actifs s'applique aux résultats des calculs de transformation.

Les expressions de formule ne peuvent générer que des valeurs doubles ou des valeurs de chaîne. Les expressions imbriquées peuvent générer d'autres types de données, tels que des chaînes, mais la formule dans son ensemble doit être évaluée à un nombre ou à une chaîne. Vous pouvez utiliser la fonction jp pour convertir une chaîne en nombre. La valeur booléenne doit être 1 (vrai) ou 0 (faux). Pour plus d'informations, consultez Valeurs non définies, infinies et en dépassement.

Example définition de transformation

L'exemple suivant illustre une propriété de transformation qui convertit les données de mesure de température d'une ressource de Celsius en Fahrenheit. Cet objet est un exemple de AssetModelpropriété contenant une transformation. Vous pouvez spécifier cet objet dans le cadre de la charge utile de la demande de CreateAssetmodèle pour créer une propriété de transformation. Pour plus d'informations, consultez Création d'un modèle d'actifs (AWS CLI).

```
{
...
"assetModelProperties": [
...
{
  "name": "Temperature F",
  "dataType": "DOUBLE",
  "type": {
    "transform": {
      "expression": "9/5 * temp_c + 32",
      "variables": [
        {
          "name": "temp_c",
          "value": {
            "propertyId": "Temperature C"
          }
        }
      ]
    }
  },
  "unit": "Fahrenheit"
}
],
...
}
```

Example définition de transformation contenant trois variables

L'exemple suivant illustre une propriété de transformation qui renvoie un message d'avertissement (`"Caution"`) si plus de 10 % des pièces du BLT123 ne répondent pas à la norme. Dans le cas contraire, il renvoie un message d'information (`"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"
                }
            }
        ]
    }
}
}
...
}
```

Agrégation de données provenant de propriétés et d'autres actifs (métriques)

Les métriques sont des expressions mathématiques qui utilisent des fonctions d'agrégation pour traiter tous les points de données en entrée et en sortie un seul point de données par intervalle de temps spécifié. Par exemple, une métrique peut calculer la température horaire moyenne à partir d'un flux de données de température.

Les métriques peuvent entrer des données à partir des métriques des ressources associées, de sorte que vous pouvez calculer des statistiques qui fournissent un aperçu de votre opération ou d'un sous-ensemble de votre opération. Par exemple, une métrique peut calculer la température horaire moyenne pour toutes les éoliennes d'un parc éolien. Pour de plus amples informations sur la définition des associations entre les ressources, veuillez consulter Définition de hiérarchies de modèles d'actifs.

Les métriques peuvent également saisir des données provenant d'autres propriétés sans agréger les données sur chaque intervalle de temps. Si vous spécifiez un attribut dans une formule, AWS IoT SiteWise utilise la dernière valeur de cet attribut lors du calcul de la formule. Si vous spécifiez une métrique dans une formule, AWS IoT SiteWise utilise la dernière valeur de l'intervalle de temps pendant lequel la formule est calculée. Cela signifie que vous pouvez définir des indicateurs tels que `OEE = Availability * Quality * Performance` `Availability`, `Quality`, où et quels `Performance` sont tous les autres indicateurs du même modèle d'actif.

AWS IoT SiteWise calcule également automatiquement un ensemble de mesures d'agrégation de base pour toutes les propriétés des actifs. Pour réduire les coûts de calcul, vous pouvez utiliser ces agrégats au lieu de définir des métriques personnalisées pour les calculs de base. Pour plus d'informations, consultez Interrogation des agrégats de propriétés d'actif.

Rubriques

- Définition des métriques (console)
- Définition des métriques (AWS CLI)

Définition des métriques (console)

Lorsque vous définissez une métrique pour un modèle d'actif dans la AWS IoT SiteWise console, vous spécifiez les paramètres suivants :

- Nom : nom de la propriété.
- Type de données : type de données de la transformation, qui peut être double ou chaîne.

- ID externe — (Facultatif) Il s'agit d'un identifiant défini par l'utilisateur. Pour plus d'informations, consultez Référencement d'objets avec des identifiants externes dans le Guide de l'utilisateur AWS IoT SiteWise .
- Formule — L'expression métrique. Les expressions métriques peuvent utiliser des fonctions d'agrégation pour saisir des données à partir d'une propriété pour tous les actifs associés dans une hiérarchie. Commencez à taper ou appuyez sur la flèche vers le bas pour ouvrir la fonction de saisie automatique. Pour plus d'informations, consultez Utilisation d'expressions de formule.

  > **Important**
  >
  > Les métriques ne peuvent être que des propriétés de type entier, double, booléen ou chaîne. Les booléens sont convertis en `0` (faux) et `1` (vrai).
  > Si vous définissez des variables d'entrée de métrique dans l'expression d'une métrique, ces entrées doivent avoir le même intervalle de temps que la métrique de sortie.
  > Les expressions de formule ne peuvent générer que des valeurs doubles ou des valeurs de chaîne. Les expressions imbriquées peuvent générer d'autres types de données, tels que des chaînes, mais la formule dans son ensemble doit être évaluée à un nombre ou à une chaîne. Vous pouvez utiliser la fonction jp pour convertir une chaîne en nombre. La valeur booléenne doit être 1 (vrai) ou 0 (faux). Pour plus d'informations, consultez Valeurs non définies, infinies et en dépassement.

- Intervalle de temps : intervalle de temps métrique. AWS IoT SiteWise prend en charge les intervalles temporels suivants, où chaque intervalle commence à la fin du précédent :
  - 1 minute à 1 minute, calculée à la fin de chaque minute (00h00, 00h01, 00h02, etc.).
  - 5 minutes — 5 minutes, calculées à la fin de toutes les cinq minutes à partir de l'heure (00h00, 00h05, 00h10, etc.).
  - 15 minutes — 15 minutes, calculées à la fin de toutes les quinze minutes à partir de l'heure (00h00, 00h15, 00h30, etc.).
  - 1 heure — 1 heure (60 minutes), calculée à la fin de chaque heure en UTC (00:00 AM, 01:00:00 AM, 02:00:00 AM, etc.).
  - 1 jour — 1 jour (24 heures), calculé à la fin de chaque journée en UTC (00h00 le lundi, 00h00 le mardi, etc.).
  - 1 semaine — 1 semaine (7 jours), calculée à la fin de chaque dimanche en UTC (tous les lundis à 00h00).

  - Intervalle personnalisé : vous pouvez saisir n'importe quel intervalle de temps compris entre une minute et une semaine.
- Date de décalage — (Facultatif) Date de référence à partir de laquelle agréger les données.
- Temps de décalage — (Facultatif) Heure de référence à partir de laquelle agréger les données. L'heure de décalage doit être comprise entre 00:00:00 et 23:59:59.
- Fuseau horaire du décalage — (Facultatif) Fuseau horaire du décalage. S'il n'est pas spécifié, le fuseau horaire décalé par défaut est le temps universel coordonné (UTC).

Fuseaux horaires pris en charge

  - (UTC+ 00:00) Heure universelle coordonnée
  - (UTC+ 01:00) Heure centrale européenne
  - (UTC+ 02:00) Europe de l'Est
  - (UTC03+:00) Heure de l'Afrique de l'Est
  - (UTC+ 04:00) Heure du Proche-Orient
  - (UTC+ 05:00) Heure de Lahore au Pakistan
  - (UTC+ 05:30) Heure normale de l'Inde
  - (UTC+ 06:00) Heure normale du Bangladesh
  - (UTC+ 07:00) Heure normale du Vietnam
  -
  - (UTC+ 09:00) Heure normale du Japon
  - (UTC+ 09:30) Heure centrale de l'Australie
  - (UTC+ 10:00) Heure de l'Est de l'Australie
  - (UTC+ 11:00) Heure normale de Salomon
  - (UTC+ 12:00) Heure normale de Nouvelle-Zélande
  - (UTC- 11:00) Heure des îles Midway
  - (UTC- 10:00) Heure normale d'Hawaï
  - (UTC- 09:00) Heure normale de l'Alaska
  - (UTC- 08:00) Heure normale du Pacifique
  - (UTC- 07:00) Heure normale de Phoenix
  - (UTC- 06:00) Heure normale du Centre
  - (UTC- 05:00) Heure normale de l'Est

- (UTC- 04:00) Heure de Porto Rico et des îles Vierges américaines
- (UTC- 03:00) Heure normale d'Argentine
- (UTC- 02:00) Heure de Géorgie du Sud
- (UTC- 01:00) Heure d'Afrique centrale

Example intervalle de temps personnalisé avec décalage (console)

L'exemple suivant vous montre comment définir un intervalle de 12 heures avec un décalage le 20 février 2021 à 18 h 30 30 (PST).

Pour définir un intervalle personnalisé avec un décalage

1. Pour Intervalle de temps, choisissez Intervalle personnalisé.
2. Pour Intervalle de temps, effectuez l'une des opérations suivantes :
   - Entrez**`12`**, puis choisissez les heures.
   - Entrez**`720`**, puis choisissez minutes.
   - Entrez**`43200`**, puis choisissez secondes.

   > ⚠ Important
   >
   > L'intervalle de temps doit être un entier, quelle que soit l'unité.

3. Pour Date de décalage, choisissez 2021/02/20.
4. Pour Heure de décalage, entrez**`18:30:30`**.
5. Pour le fuseau horaire décalé, choisissez (UTC- 08:00) Heure normale du Pacifique.

Si vous créez la métrique le 1er juillet 2021, avant ou à 18 h 30 30 (PST), vous obtenez le premier résultat d'agrégation le 1er juillet 2021 à 18 h 30 30 (PST). Le deuxième résultat d'agrégation est le 2 juillet 2021 à 06h30 (PST), et ainsi de suite.

Définition des métriques (AWS CLI)

Lorsque vous définissez une métrique pour un modèle d'actif avec l' AWS IoT SiteWise API, vous spécifiez les paramètres suivants :

- `name`— Le nom de la propriété.
- `dataType`— Le type de données de la métrique, qui peut être `DOUBLE` ou`STRING`.
- `externalId`— (Facultatif) Il s'agit d'un identifiant défini par l'utilisateur. Pour plus d'informations, consultez Référencement d'objets avec des identifiants externes dans le Guide de l'utilisateur AWS IoT SiteWise .
- `expression`— L'expression métrique. Les expressions métriques peuvent utiliser des fonctions d'agrégation pour saisir des données à partir d'une propriété pour tous les actifs associés dans une hiérarchie. Pour plus d'informations, consultez Utilisation d'expressions de formule.
- `window`— L'intervalle de temps et le décalage correspondant à la fenêtre de fluctuation de la métrique, où chaque intervalle commence à la fin du précédent :
  - `interval`— L'intervalle de temps pendant lequel la fenêtre clignote. L'intervalle de temps doit être compris entre une minute et une semaine.
  - `offsets`— Le décalage dû à la fenêtre qui piétine.

  Pour plus d'informations, consultez TumblingWindowla référence de AWS IoT SiteWise l'API.

  Example intervalle de temps personnalisé avec un décalage (AWS CLI)

  L'exemple suivant vous montre comment définir un intervalle de 12 heures avec un décalage le 20 février 2021 à 18h30 (PST).

  ```
  {
      "window": {
          "tumbling": {
              "interval": "12h",
              "offset": " 2021-07-23T18:30:30-08"
          }
      }
  }
  ```

  Si vous créez la métrique le 1er juillet 2021, avant ou à 18 h 30 30 (PST), vous obtenez le premier résultat d'agrégation le 1er juillet 2021 à 18 h 30 30 (PST). Le deuxième résultat d'agrégation est le 2 juillet 2021 à 06h30 (PST), et ainsi de suite.
- `variables`— La liste des variables qui définit les autres propriétés de votre actif ou de vos actifs enfants à utiliser dans l'expression. Chaque structure de variable contient un nom simple à

utiliser dans l'expression et une structure `value` qui identifie la propriété à lier à cette variable. La structure `value` contient les informations suivantes :

- `propertyId`— L'ID de la propriété à partir de laquelle les valeurs doivent être extraites. Vous pouvez utiliser le nom de la propriété au lieu de son ID si la propriété est définie dans le modèle actuel (plutôt que définie dans un modèle à partir d'une hiérarchie).
- `hierarchyId`— (Facultatif) L'ID de la hiérarchie à partir de laquelle interroger les actifs enfants de la propriété. Vous pouvez utiliser le nom de la définition de hiérarchie au lieu de son ID. Si vous omettez cette valeur, AWS IoT SiteWise recherche la propriété dans le modèle actuel.

> **Important**
>
> Les métriques ne peuvent être que des propriétés de type entier, double, booléen ou chaîne. Les booléens sont convertis en `0` (faux) et `1` (vrai).
> Si vous définissez des variables d'entrée de métrique dans l'expression d'une métrique, ces entrées doivent avoir le même intervalle de temps que la métrique de sortie.
> Les expressions de formule ne peuvent générer que des valeurs doubles ou des valeurs de chaîne. Les expressions imbriquées peuvent générer d'autres types de données, tels que des chaînes, mais la formule dans son ensemble doit être évaluée à un nombre ou à une chaîne. Vous pouvez utiliser la fonction jp pour convertir une chaîne en nombre. La valeur booléenne doit être 1 (vrai) ou 0 (faux). Pour plus d'informations, consultez Valeurs non définies, infinies et en dépassement.

- `unit`— (Facultatif) L'unité scientifique de la propriété, telle que mm ou Celsius.

Example Exemple de définition de métrique

L'exemple suivant illustre une propriété de métrique qui agrège les données de mesure de la température d'une ressource pour calculer la température horaire maximale en Fahrenheit. Cet objet est un exemple de AssetModelpropriété contenant une métrique. Vous pouvez spécifier cet objet dans le cadre de la charge utile de la demande de CreateAssetmodèle pour créer une propriété métrique. Pour plus d'informations, consultez Création d'un modèle d'actifs (AWS CLI).

```
{
      ...
      "assetModelProperties": [
      ...
      {
```

```
        "name": "Max temperature",
        "dataType": "DOUBLE",
        "type": {
          "metric": {
            "expression": "max(temp_f)",
            "variables": [
              {
                "name": "temp_f",
                "value": {
                  "propertyId": "Temperature F"
                }
              }
            ],
            "window": {
              "tumbling": {
                "interval": "1h"
              }
            }
          }
        },
        "unit": "Fahrenheit"
      }
    ],
    ...
}
```

Example Exemple de définition de métrique qui saisit les données des actifs associés

L'exemple suivant illustre une propriété métrique qui agrège les données de puissance moyenne de plusieurs éoliennes pour calculer la puissance moyenne totale d'un parc éolien. Cet objet est un exemple de AssetModelpropriété contenant une métrique. Vous pouvez spécifier cet objet dans le cadre de la charge utile de la demande de CreateAssetmodèle pour créer une propriété métrique.

```
{
      ...
      "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"
      }
    ],
    ...
}
```

Utilisation d'expressions de formule

Avec les expressions de formule, vous pouvez définir les fonctions mathématiques permettant de transformer et d'agréger vos données industrielles brutes afin d'obtenir des informations sur votre opération. Les expressions de formule combinent des littéraux, des opérateurs, des fonctions et des variables pour traiter les données. Pour plus d'informations sur la façon de définir les propriétés des actifs qui utilisent des expressions de formule, reportez-vous Transformation des données (transformations) aux sections etAgrégation de données provenant de propriétés et d'autres actifs (métriques). Les transformations et les métriques sont des propriétés de formule.

Rubriques

- Utilisation de variables dans des expressions de formule
- Utilisation de littéraux dans les expressions de formule
- Utilisation d'opérateurs dans les expressions de formule
- Utilisation de constantes dans les expressions de formule
- Utilisation de fonctions dans des expressions de formule
- Tutoriels d'expression de formules

Utilisation de variables dans des expressions de formule

Les variables représentent les propriétés des AWS IoT SiteWise actifs dans les expressions de formule. Utilisez des variables pour saisir des valeurs provenant d'autres propriétés d'actifs dans vos expressions, afin de pouvoir traiter les données issues de propriétés constantes (attributs), de flux de données brutes (mesures) et d'autres propriétés de formule.

Les variables peuvent représenter les propriétés des actifs à partir du même modèle d'actif ou à partir de modèles d'actifs enfants associés. Seules les formules métriques peuvent saisir des variables à partir de modèles d'actifs enfants.

Vous identifiez les variables sous différents noms dans la console et dans l'API.

- AWS IoT SiteWise console — Utilisez les noms des propriétés des actifs comme variables dans vos expressions.
- AWS IoT SiteWise API (AWS CLI, AWS SDK) — Définissez les variables avec la ExpressionVariablestructure, qui nécessite un nom de variable et une référence à une propriété d'actif. Le nom de la variable peut contenir des lettres minuscules, des chiffres et des traits de soulignement. Utilisez ensuite des noms de variables pour référencer les propriétés des actifs dans vos expressions.

Les noms de variables distinguent les majuscules et minuscules.

Pour plus d'informations, consultez les sections Définition des transformations et Définition des métriques.

Utilisation de variables pour référencer des propriétés

La valeur d'une variable définit la propriété à laquelle elle fait référence. AWS IoT SiteWise propose différentes manières de le faire.

- Par identifiant de propriété : vous pouvez spécifier l'identifiant unique (UUID) de la propriété pour l'identifier.
- Par nom : si la propriété utilise le même modèle d'actif, vous pouvez spécifier son nom dans le champ ID de propriété.
- Par chemin : la valeur d'une variable peut faire référence à une propriété par son chemin. Pour plus d'informations, consultez Utilisation de chemins pour référencer les propriétés de modèles composites personnalisés.

> **Note**
>
> Les variables ne sont pas prises en charge par AWS IoT SiteWise la console. Ils sont utilisés par AWS IoT SiteWise l'API, y compris le AWS Command Line Interface AWS CLI) et AWS les SDK.

Une variable que vous recevez dans une réponse AWS IoT SiteWise inclut des informations complètes sur la valeur, notamment l'ID et le chemin.

Toutefois, lorsque vous transmettez une variable à AWS IoT SiteWise (par exemple, lors d'un appel « créer » ou « mettre à jour »), il vous suffit de spécifier l'une de ces variables. Par exemple, si vous spécifiez le chemin, vous n'avez pas besoin de fournir l'ID.

Utilisation de littéraux dans les expressions de formule

Vous pouvez définir des nombres et des littéraux de chaîne dans les expressions de formule.

- Chiffres

  Utilisez les nombres et la notation scientifique pour définir des nombres entiers et des doubles. Vous pouvez utiliser la notation E pour exprimer des nombres en notation scientifique.

  Exemples : `12.0`,`.9`,`-23.1`,`7.89e3`, `3.4E-5`

- Chaînes

  Utilisez les caractères `'` (guillemets) et `''` (guillemets doubles) pour définir les chaînes. Le type de devis pour le début et la fin doit correspondre. Pour éviter un guillemet correspondant à celui que vous utilisez pour déclarer une chaîne, incluez ce guillemet deux fois. Il s'agit du seul caractère d'échappement dans AWS IoT SiteWise les chaînes.

  Exemples : `'active'`, `"inactive"`, `'{"temp": 52}'`, `"{""temp"": ""high""}"`

Utilisation d'opérateurs dans les expressions de formule

Vous pouvez utiliser les opérateurs courants suivants dans les expressions de formule.

Opérateur	Description
`+`	Si les deux opérandes sont des nombres, cet opérateur ajoute les opérandes gauche et droit. Si l'un des opérandes est une chaîne, cet opérateur concatène les opérandes gauche et droit sous forme de chaînes. Par exemple, l'expression est `1 + 2 + " is three"` évaluée à. `"3 is three"` La chaîne concaténée peut comporter jusqu'à 1024 caractères. Si la chaîne dépasse 1024 caractères, elle AWS IoT SiteWise ne produit aucun point de données pour ce calcul.
`-`	Il soustrait l'opérande droit de l'opérande gauche. Vous ne pouvez utiliser cet opérateur qu'avec des opérandes numériques.
`/`	Il divise l'opérande gauche par l'opérande droit. Vous ne pouvez utiliser cet opérateur qu'avec des opérandes numériques.
`*`	Il multiplie les opérandes gauche et droit. Vous ne pouvez utiliser cet opérateur qu'avec des opérandes numériques.
`^`	Il élève l'opérande gauche à la puissance de l'opérande droit (élévation de la puissance). Vous ne pouvez utiliser cet opérateur qu'avec des opérandes numériques.
`%`	Il renvoie le reste résultant de la division de l'opérande gauche par l'opérande droit.

Opérateur	Description
	Le résultat a le même signe que l'opérande gauche. Ce comportement est différent de celui de l'opération modulo. Vous ne pouvez utiliser cet opérateur qu'avec des opérandes numériques.
`x < y`	Renvoie 1 si la valeur `x` est inférieure à`y`, sinon`0`.
`x > y`	Renvoie 1 si la valeur `x` est supérieure à`y`, sinon`0`.
`x <= y`	Renvoie 1 si la valeur `x` est inférieure ou égale à`y`, sinon`0`.
`x >= y`	Renvoie 1 si la valeur `x` est supérieure ou égale à`y`, sinon`0`.
`x == y`	Renvoie 1 si `x` c'est égal à`y`, sinon`0`.
`x != y`	Renvoie 1 si `x` ce n'est pas égal à`y`, sinon`0`.
`!x`	Renvoie 1 si la valeur `x` est évaluée à `0` (faux), sinon`0`. `x`est évalué à faux si : • `x`est un opérande numérique évalué à. `0` • `x`est évalué à une chaîne vide. • `x`est évalué à un tableau vide. • `x`est évalué à`None`.

Opérateur	Description
`x and y`	Renvoie `0` si la valeur `x` est évaluée à `0` (faux). Sinon, renvoie le résultat évalué de`y`. `x`ou `y` est évalué à faux si : • `x`ou `y` est un opérande numérique et il est évalué à. `0` • `x`ou `y` est évalué à une chaîne vide. • `x`ou `y` est évalué selon un tableau vide. • `x`ou `y` est évalué à`None`.
`x or y`	Renvoie 1 si la valeur `x` est évaluée à 1 (vrai). Sinon, renvoie le résultat évalué de`y`. `x`ou `y` est évalué à faux si : • `x`ou `y` est un opérande numérique et il est évalué à. `0` • `x`ou `y` est évalué à une chaîne vide. • `x`ou `y` est évalué selon un tableau vide. • `x`ou `y` est évalué à`None`.
`not x`	Renvoie 1 si la valeur `x` est évaluée à `0` (faux), sinon`0`. `x`est évalué à faux si : • `x`est un opérande numérique évalué à. `0` • `x`est évalué à une chaîne vide. • `x`est évalué à un tableau vide. • `x`est évalué à`None`.

Opérateur	Description

`[]`
 	
`s[index]`
	Renvoie le caractère à un index `index` de la chaînes. Ceci est équivalent à la syntaxe d'index en Python.
	
	Example Exemples
	
	• `"Hello!"[1]` renvoie `e`.
	• `"Hello!"[-2]` renvoie `o`.

Opérateur	Description

`[]`
 	
`s[start:end:step]`
	Renvoie une tranche de la chaînes. Ceci est équivalent à la syntaxe des tranches en Python. Cet opérateur possède les arguments suivants :
	
	• `start`— (Facultatif) Indice de début inclus de la tranche. La valeur par défaut est `0`.
	• `end`— (Facultatif) Indice final exclusif de la tranche. La valeur par défaut est la longueur de la chaîne.
	• `step`— (Facultatif) Le nombre à incrément er pour chaque étape de la tranche. Par exemple, vous pouvez spécifier 2 de renvoyer une tranche avec tous les autres caractères ou `-1` d'inverser la tranche. La valeur par défaut est 1.
	
	Vous pouvez omettre l'`step`argument pour utiliser sa valeur par défaut. Par exemple, `s[1:4:1]` équivaut à `s[1:4]`.
	
	Les arguments doivent être des entiers ou la constante none. Si vous le spécifiez`none`, AWS IoT SiteWise utilise la valeur par défaut pour cet argument.
	
	Example Exemples
	
	• `"Hello!"[1:4]` renvoie `"ell"`.
	• `"Hello!"[:2]` renvoie `"He"`.
	• `"Hello!"[3:]` renvoie `"lo!"`.
	• `"Hello!"[:-4]` renvoie `"He"`.
	• `"Hello!"[::2]` renvoie `"Hlo"`.
	• `"Hello!"[::-1]` renvoie `"!olleH"`.

Utilisation de constantes dans les expressions de formule

Vous pouvez utiliser les constantes mathématiques courantes suivantes dans vos expressions. Toutes les constantes ne distinguent pas les majuscules et minuscules.

> **Note**
>
> Si vous définissez une variable portant le même nom qu'une constante, la variable remplace la constante.

Constant	Description
`pi`	Le nombre pi (π) : `3.141592653589793`
`e`	Le chiffre e : `2.718281828459045`
`true`	C'est l'équivalent du chiffre 1. Dans AWS IoT SiteWise, les booléens sont convertis en équivalents numériques.
`false`	Équivalent au chiffre 0. Dans AWS IoT SiteWise, les booléens sont convertis en équivalents numériques.
`none`	C'est équivalent à aucune valeur. Vous pouvez utiliser cette constante pour ne rien afficher à la suite d'une expression conditionnelle.

Utilisation de fonctions dans des expressions de formule

Vous pouvez utiliser les fonctions suivantes pour agir sur les données de vos expressions de formule.

Les transformations et les métriques prennent en charge différentes fonctions. Le tableau suivant indique les types de fonctions compatibles avec chaque type de propriété de formule.

> **Note**
>
> Vous pouvez inclure un maximum de 10 fonctions dans une expression de formule.

Type de fonction	Transformations	Métriques
Utilisation de fonctions courantes dans les expressions de formule	Oui	Oui
Utilisation de fonctions de comparaison dans des expressions de formule	Oui	Oui
Utilisation de fonctions conditionnelles dans les expressions de formule	Oui	Oui
Utilisation de fonctions de chaîne dans des expressions de formule	Oui	Oui
Utilisation de fonctions d'agrégation dans des expressions de formule	Non	Oui
Utilisation de fonctions temporelles dans les expressions de formules	Oui	Oui

Type de fonction	Transformations	Métriques
Utilisation des fonctions de date et d'heure dans les expressions de formule	 Oui	 Oui

Syntaxe des fonctions

Vous pouvez utiliser la syntaxe suivante pour créer des fonctions :

Syntaxe régulière

Avec la syntaxe normale, le nom de la fonction est suivi de parenthèses contenant zéro argument ou plus.

function_name(*argument1, argument2, argument3, ...*). Par exemple, les fonctions dont la syntaxe est normale peuvent ressembler à `log(x)` et`contains(s, substring)`.

Syntaxe uniforme des appels de fonction (UFCS)

L'UFCS vous permet d'appeler des fonctions en utilisant la syntaxe des appels de méthode dans la programmation orientée objet. Avec UFCS, le premier argument est suivi par point (`.`), puis le nom de la fonction et les autres arguments (le cas échéant) entre parenthèses.

argument1.*function_name*(*argument2, argument3, ...*). Par exemple, les fonctions avec UFCS peuvent ressembler à `x.log()` et`s.contains(substring)`.

Vous pouvez également utiliser l'UFCS pour enchaîner les fonctions suivantes. AWS IoT SiteWise utilise le résultat de l'évaluation de la fonction en cours comme premier argument de la fonction suivante.

Par exemple, vous pouvez utiliser à la `message.jp('$.status').lower().contains('fail')` place `decontains(lower(jp(message, '$.status')),'fail')`.

Pour plus d'informations, consultez le site Web du langage de programmation D.

> **Note**
>
> Vous pouvez utiliser l'UFCS pour toutes les AWS IoT SiteWise fonctions.
> AWS IoT SiteWise les fonctions ne distinguent pas les majuscules et minuscules. Par exemple, vous pouvez utiliser `lower(s)` et de `Lower(s)` manière interchangeable.

Utilisation de fonctions courantes dans les expressions de formule

Dans les transformations et les métriques, vous pouvez utiliser les fonctions suivantes pour calculer les fonctions mathématiques courantes dans les transformations et les métriques.

Fonction	Description
`abs(x)`	Renvoie la valeur absolue de `x`.
`acos(x)`	Renvoie l'arc cosinus de `x`.
`asin(x)`	Renvoie l'arc sinus de `x`.
`atan(x)`	Renvoie l'arc tangent de `x`.
`cbrt(x)`	Renvoie la racine cubique de `x`.
`ceil(x)`	Renvoie l'entier le plus proche supérieur à `x`.
`cos(x)`	Renvoie le cosinus de `x`.
`cosh(x)`	Renvoie le cosinus hyperbolique de `x`.
`cot(x)`	Renvoie la cotangente de. `x`
`exp(x)`	Renvoie e à la puissance de `x`.
`expm1(x)`	Renvoie `exp(x) - 1`. Utilisez cette fonction pour calculer avec plus de précision `exp(x) - 1` les petites valeurs de`x`.
`floor(x)`	Renvoie l'entier le plus proche inférieur à `x`.

Fonction	Description
`log(x)`	Renvoie l'élément $\log_e$ (base e) de x.
`log10(x)`	Renvoie l'élément $\log_{10}$ (base 10) de x.
`log1p(x)`	Renvoie `log(1 + x)`. Utilisez cette fonction pour calculer avec plus de précision `log(1 + x)` les petites valeurs dex.
`log2(x)`	Renvoie l'élément $\log_2$ (base 2) de x.
`pow(x, y)`	Renvoie x à la puissance de y. Cela équivaut àx `^` y.
`signum(x)`	Renvoie le signe de x (`-1` pour les entrées négatives, `0` pour les entrées nulles et `+1` pour les entrées positives).
`sin(x)`	Renvoie le sinus de x.
`sinh(x)`	Renvoie le sinus hyperbolique de x.
`sqrt(x)`	Renvoie la racine carrée de x.
`tan(x)`	Renvoie la tangente de x.
`tanh(x)`	Renvoie la tangente hyperbolique de x.

Utilisation de fonctions de comparaison dans des expressions de formule

Dans les transformations et les métriques, vous pouvez utiliser les fonctions de comparaison suivantes pour comparer deux valeurs et obtenir un résultat 1 (vrai) ou `0` (faux). AWS IoT SiteWise compare les chaînes par ordre lexicographique.

Fonction	Description
`gt(x, y)`	Renvoie 1 si x est supérieur à y, sinon `0` (`x > y`).

Fonction	Description
	Cette fonction ne renvoie pas de valeur s'il s'xyagit de types incompatibles, tels qu'un nombre et une chaîne.
`gte(x, y)`	Renvoie 1 si `x` est supérieur ou égal à `y`, sinon `0` (`x ≥ y`). AWS IoT SiteWise considère que les arguments sont égaux s'ils se situent dans une tolérance relative de`1E-9`. Cela se comporte de la même manière que la fonction isclose en Python. Cette fonction ne renvoie pas de valeur s'il s'xyagit de types incompatibles, tels qu'un nombre et une chaîne.
`eq(x, y)`	Renvoie 1 si `x` est égal à `y`, sinon `0` (`x == y`). AWS IoT SiteWise considère que les arguments sont égaux s'ils se situent dans une tolérance relative de`1E-9`. Cela se comporte de la même manière que la fonction isclose en Python. Cette fonction ne renvoie pas de valeur s'il s'xyagit de types incompatibles, tels qu'un nombre et une chaîne.
`lt(x, y)`	Renvoie 1 si `x` est inférieur à `y`, sinon `0` (`x < y`). Cette fonction ne renvoie pas de valeur s'il s'xyagit de types incompatibles, tels qu'un nombre et une chaîne.

Fonction	Description
`lte(x, y)`	Renvoie 1 si x est inférieur ou égal à y, sinon `0` (x ≤ y). AWS IoT SiteWise considère que les arguments sont égaux s'ils se situent dans une tolérance relative de`1E-9`. Cela se comporte de la même manière que la fonction isclose en Python. Cette fonction ne renvoie pas de valeur s'il s'`xy`agit de types incompatibles, tels qu'un nombre et une chaîne.
`isnan(x)`	Renvoie 1 si x c'est égal à`NaN`, sinon`0`. Cette fonction ne renvoie pas de valeur s'il s'`x`agit d'une chaîne.

Utilisation de fonctions conditionnelles dans les expressions de formule

Dans les transformations et les métriques, vous pouvez utiliser la fonction suivante pour vérifier une condition et renvoyer différents résultats, que la condition soit vraie ou fausse.

Fonction	Description
`if(condition, result_if_true, result_if_false)`	Évalue `condition` et renvoie `result_if_true` si la condition est vraie ou `result_if_false` si la condition est évaluée à. `false` `condition` doit être un chiffre. Cette fonction considère `0` une chaîne vide comme `false` et tout le reste (y compris`NaN`) comme`true`. Les booléens sont convertis en `0` (faux) et `1` (vrai). Vous pouvez renvoyer la constante none à partir de cette fonction pour supprimer la sortie

Fonction	Description
	pour une condition particulière. Cela signifie que vous pouvez filtrer les points de données qui ne répondent pas à une condition. Pour plus d'informations, consultez Filtrer les points de données. Example Exemples • `if(0, x, y)`renvoie la variable`y`. • `if(5, x, y)`renvoie la variable`x`. • `if(gt(temp, 300), x, y)` renvoie la variable `x` si celle-ci `temp` est supérieure à`300`. • `if(gt(temp, 300), temp, none)`renvoie la variable `temp` si elle est supérieure ou égale à`300`, ou `none` (aucune valeur) si elle `temp` est inférieure à`300`. Nous vous recommandons d'utiliser l'UFCS pour les fonctions conditionnelles imbriquées dans lesquelles un ou plusieurs arguments sont des fonctions conditionnelles. Vous pouvez l'utiliser `if(condition, result_if_true)` pour évaluer une condition et `elif(condition, result_if_true, result_if_false)` pour évaluer des conditions supplémentaires. Par exemple, vous pouvez utiliser à la `if(condition1, result1_if_true).elif(condition2, result2_if_true, result2_if_false)` place de`if(condition1, result1_if_true, if(condition2, result2_if_true, result2_if_false))` .

Fonction	Description
	Vous pouvez également enchaîner des fonctions conditionnelles intermédiaires supplémentaires. Par exemple, vous pouvez utiliser plusieurs `if` instructions `if(condition1, result1_if_true).elif(condition2, result2_if_true).elif(condition3, result3_if_true, result3_if_false)` au lieu de les imbriquer, telles que `if(condition1, result1_if_true, if(condition2, result2_if_true, if(condition3, result3_if_true result3_if_false)))` . **Important** Vous devez l'utiliser `elif(condition, result_if_true, result_if_false)` avec l'UFCS.

Utilisation de fonctions de chaîne dans des expressions de formule

Dans les transformations et les métriques, vous pouvez utiliser les fonctions suivantes pour agir sur des chaînes. Pour plus d'informations, consultez Utilisation de chaînes dans les formules.

Important

Les expressions de formule ne peuvent générer que des valeurs doubles ou des valeurs de chaîne. Les expressions imbriquées peuvent générer d'autres types de données, tels que des chaînes, mais la formule dans son ensemble doit être évaluée à un nombre ou à une chaîne. Vous pouvez utiliser la fonction jp pour convertir une chaîne en nombre. La valeur booléenne doit être 1 (vrai) ou 0 (faux). Pour plus d'informations, consultez Valeurs non définies, infinies et en dépassement.

Fonction	Description
`len(s)`	Renvoie la longueur de la chaînes.
`find(s, substring)`	Renvoie l'index de la chaîne `substring` dans la chaînes.
`contains(s, substring)`	Renvoie 1 si la chaîne `s` contient la chaîne`substring` , sinon`0`.
`upper(s)`	Renvoie la chaîne `s` en majuscules.
`lower(s)`	Renvoie la chaîne `s` en minuscules.
`jp(s, json_path)`	Évalue la chaîne `s` avec l'JsonPathexpression `json_path` et renvoie le résultat. Utilisez cette fonction pour effectuer les opérations suivantes : • Extrayez une valeur, un tableau ou un objet d'une structure JSON sérialisée. • Convertit une chaîne en nombre. Par exemple, la formule est `jp('111', '$')` renvoyée 111 sous forme de nombre. Pour extraire une valeur de chaîne d'une structure JSON et la renvoyer sous forme de nombre, vous devez utiliser plusieurs `jp` fonctions imbriquées. La `jp` fonction externe extrait la chaîne de la structure JSON et la `jp` fonction interne convertit la chaîne en nombre. La chaîne `json_path` doit contenir une chaîne littérale. Cela signifie qu'il ne `json_path` peut pas s'agir d'une expression évaluée en chaîne.

Fonction	Description
	Example Exemples • `jp('{"status":"active","value":15}', '$.value')` renvoie 15. • `jp('{"measurement":{"reading":25,"confidence":0.95}}', '$.measurement.reading')` renvoie 25. • `jp('[2,8,23]', '$[2]')` renvoie 23. • `jp('{"values":[3,6,7]}', '$.values[1]')` renvoie 6. • `jp('111', '$')` renvoie 111. • `jp(jp('{"measurement":{"reading":25,"confidence":"0.95"}}', '$.measurement.confidence'), '$')` renvoie `0.95`.
`join(s0, s1, s2, s3, ...)`	Renvoie une chaîne concaténée avec un délimiteur. Cette fonction utilise la première chaîne d'entrée comme délimiteur et réunit les chaînes d'entrée restantes. Cela se comporte de la même manière que la fonction join (CharSequence delimiter, CharSequence... elements) en Java. Example Exemples • `join("-", "aa", "bb", "cc")`retours `aa-bb-cc`

Fonction	Description
`format(expression: "format")` ou `format("format", expression)`	Renvoie une chaîne au format spécifié. Cette fonction donne `expression` une valeur, puis renvoie la valeur dans le format spécifié. Cela se comporte de la même manière que la fonction format (String format, Object... args) en Java. Pour plus d'informations sur les formats pris en charge, consultez la section Conversio ns sous Class Formatter dans la plate-forme Java, spécification de l'API Standard Edition 7. Example Exemples • `format(100+1: "d")` renvoie une chaîne,`101`. • `format("The result is %d", 100+1)`renvoie une chaîne,`The result is 101`.

Fonction	Description
`f'expression'`	Renvoie une chaîne concaténée. Avec cette fonction formatée, vous pouvez utiliser une expression simple pour concaténer et formater des chaînes. Ces fonctions peuvent contenir des expressions imbriquées. Vous pouvez utiliser `{}` (accolades) pour interpoler des expressions. Cela se comporte de la même manière que les littéraux de chaîne formatés en Python. Example Exemples • `f'abc{1+2: "f"}d'` renvoie `abc3.000000d` . Pour évaluer cet exemple d'expression, procédez comme suit : 1. `format(1+2: "f")` renvoie un nombre à virgule flottante,`3.000000`. 2. `join('', "abc", 1+2, 'd')`renvoie une chaîne,`abc3.000000d` . Vous pouvez également écrire l'expression de la manière suivante : `join('', "abc", format(1+2: "f"), 'd')`

Utilisation de fonctions d'agrégation dans des expressions de formule

Dans les métriques uniquement, vous pouvez utiliser les fonctions suivantes pour agréger les valeurs d'entrée sur chaque intervalle de temps et calculer une valeur de sortie unique. Les fonctions d'agrégation peuvent agréger les données issues de ressources associées.

Les arguments des fonctions d'agrégation peuvent être des variables, des littéraux numériques, des fonctions temporelles, des expressions imbriquées ou des fonctions d'agrégation. La formule `max(latest(x), latest(y), latest(z))` utilise une fonction d'agrégation comme argument et renvoie la plus grande valeur actuelle des z propriétés `xy`, et.

Vous pouvez utiliser des expressions imbriquées dans les fonctions d'agrégation. Lorsque vous utilisez des expressions imbriquées, les règles suivantes s'appliquent :

- Chaque argument ne peut comporter qu'une seule variable.

  Example

  Par exemple, `avg(x*(x-1))` et `sum(x/2 )/avg(y^2 )` sont pris en charge.

  Par exemple, `min(x/y)` n'est pas pris en charge.
- Chaque argument peut comporter des expressions imbriquées à plusieurs niveaux.

  Example

  Par exemple, `sum(avg(x^2 )/2)` est pris en charge.
- Les différents arguments peuvent avoir des variables différentes.

  Example

  Par exemple, `sum(x/2, y*2)` est pris en charge.

> **Note**
>
> - Si vos expressions contiennent des mesures, AWS IoT SiteWise utilise les dernières valeurs de l'intervalle de temps actuel pour que les mesures calculent les agrégats.
> - Si vos expressions contiennent des attributs, AWS IoT SiteWise utilise les dernières valeurs des attributs pour calculer les agrégats.

Fonction	Description
`avg(`x_0`, ..., `x_n`)`	Renvoie la moyenne des valeurs des variables données sur l'intervalle de temps actuel. Cette fonction produit un point de données uniquement si les variables données ont au moins un point de données sur l'intervalle de temps actuel.

Fonction	Description
`sum(`x_0`, ..., `x_n`)`	Renvoie la somme des valeurs de variables données sur l'intervalle de temps actuel. Cette fonction produit un point de données uniquement si les variables données ont au moins un point de données sur l'intervalle de temps actuel.
`min(`x_0`, ..., `x_n`)`	Renvoie la valeur minimale des valeurs des variables données sur l'intervalle de temps actuel. Cette fonction produit un point de données uniquement si les variables données ont au moins un point de données sur l'intervalle de temps actuel.
`max(`x_0`, ..., `x_n`)`	Renvoie la valeur maximale des valeurs de variables données sur l'intervalle de temps actuel. Cette fonction produit un point de données uniquement si les variables données ont au moins un point de données sur l'intervalle de temps actuel.
`count(`x_0`, ..., `x_n`)`	Renvoie le nombre total de points de données pour les variables données sur l'intervalle de temps actuel. Pour de plus amples informations sur la comptabilisation du nombre de points de données qui répondent à une condition, veuillez consulter Comptage des points de données correspondant à une condition. Cette fonction calcule un point de données pour chaque intervalle de temps.

Fonction	Description
`stdev(x0, ..., xn)`	Renvoie l'écart type des valeurs des variables données sur l'intervalle de temps actuel. Cette fonction produit un point de données uniquement si les variables données ont au moins un point de données sur l'intervalle de temps actuel.

Utilisation de fonctions temporelles dans les expressions de formules

Utilisez des fonctions temporelles pour renvoyer des valeurs basées sur les horodatages des points de données.

Utilisation de fonctions temporelles dans les métriques

Dans les métriques uniquement, vous pouvez utiliser les fonctions suivantes qui renvoient des valeurs basées sur l'horodatage des points de données.

Les arguments des fonctions temporelles doivent être des propriétés du modèle d'actif local ou des expressions imbriquées. Cela signifie que vous ne pouvez pas utiliser les propriétés des modèles d'actifs enfants dans les fonctions temporelles.

Vous pouvez utiliser des expressions imbriquées dans les fonctions temporelles. Lorsque vous utilisez des expressions imbriquées, les règles suivantes s'appliquent :

- Chaque argument ne peut comporter qu'une seule variable.

  Par exemple, `latest( t*9/5 + 32 )` est pris en charge.
- Les arguments ne peuvent pas être des fonctions d'agrégation.

  Par exemple, `first( sum(x) )` n'est pas pris en charge.

Fonction	Description
`first(x)`	Renvoie la valeur de la variable donnée avec l'horodatage le plus ancien sur l'intervalle de temps actuel.
`last(x)`	Renvoie la valeur de la variable donnée avec l'horodatage le plus récent sur l'intervalle de temps actuel.
`earliest(x)`	Renvoie la dernière valeur de la variable donnée avant le début de l'intervalle de temps actuel. Cette fonction calcule un point de données pour chaque intervalle de temps, si la propriété d'entrée a au moins un point de données dans son historique. Consultez time-range-defintion pour plus de détails.
`latest(x)`	Renvoie la dernière valeur de la variable donnée avec le dernier horodatage avant la fin de l'intervalle de temps actuel. Cette fonction calcule un point de données pour chaque intervalle de temps, si la propriété d'entrée a au moins un point de données dans son historique. Consultez time-range-defintion pour plus de détails.
`statetime(x)`	Renvoie la durée, en secondes, pendant laquelle les variables données sont positives sur l'intervalle de temps actuel. Vous pouvez utiliser les fonctions de comparaison pour créer une propriété de transformation pour la `statetime` fonction à utiliser.

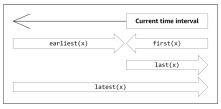
Fonction	Description
	Par exemple, si vous avez une propriété `Idle` qui est `0` ou `1`, vous pouvez calculer le temps d'inactivité par intervalle de temps avec l'expression suivante : `IdleTime = statetime(Idle)` . Pour plus d'informations, consultez l'exemple de scénario d'heure d'état. Cette fonction ne prend pas en charge les propriétés de métriques en tant que variables d'entrée. Cette fonction calcule un point de données pour chaque intervalle de temps, si la propriété d'entrée a au moins un point de données dans son historique.

Fonction	Description
`TimeWeightedAvg(x, [interpolation])`	Renvoie la moyenne des données d'entrée pondérées par les intervalles de temps entre les points. Voir Paramètres des fonctions pondérées dans le temps pour plus de détails sur les calculs et les intervalles. L'argument facultatif `interpolaton` doit être une constante de chaîne : • `locf`— Il s'agit de la valeur par défaut. Le calcul utilise l'algorithme de calcul du dernier report observé pour les intervalles entre les points de données. Dans cette approche, le point de données est calculé comme la dernière valeur observée jusqu'au prochain horodatage du point de données d'entrée. La valeur après un point de données valide est extrapolée sous forme de valeur jusqu'à l'horodatage du point de données suivant. • `linear`— Le calcul utilise l'algorithme d'interpolation linéaire pour les intervalles entre les points de données. La valeur entre deux bons points de données est extrapolée sous forme d'interpolation linéaire entre les valeurs de ces points de données. La valeur entre les bons et les mauvais points de données ou la valeur après le dernier bon point de données sera extrapolée en tant que bon point de données.

Fonction	Description
`TimeWeightedStDev(x, [algo])`	Renvoie l'écart type des données d'entrée pondéré avec les intervalles de temps entre les points. Voir Paramètres des fonctions pondérées dans le temps pour plus de détails sur les calculs et les intervalles. Le calcul utilise l'algorithme de calcul du dernier report observé pour les intervalles entre les points de données. Dans cette approche, le point de données est calculé comme la dernière valeur observée jusqu'au prochain horodatage du point de données d'entrée. Le poids est calculé sous la forme d'un intervall e de temps en secondes entre les points de données ou les limites des fenêtres. L'argument facultatif `algo` doit être une constante de chaîne : • `f`— Il s'agit de la valeur par défaut. Il renvoie une variance d'échantillon pondérée non biaisée avec des poids de fréquence, TimeWeight calculée en secondes. Cet algorithme est généralement supposé en fonction de l'écart type et est connu sous le nom de correction de Bessel de l'écart type pour les échantillons pondérés. • p— Renvoie la variance d'échantillon pondérée biaisée, également connue sous le nom de variance de population. Les formules suivantes sont utilisées pour le calcul où :

Fonction	Description
	• S_p = écart type de la population • S_f = écart type de fréquence • X_i = données entrantes • ω_i = poids égal à l'intervalle de temps en secondes • μ* = moyenne pondérée des données entrantes Équation pour l'écart type de la population : $$S_p^2 = \frac{\sum_{i=1}^{N} \omega_i (x_i - \mu^*)^2}{\sum_{i=1}^{N} \omega_i}$$ Équation pour l'écart type de fréquence : $$S_f^2 = \frac{\sum_{i=1}^{N} \omega_i (x_i - \mu^*)^2}{\sum_{i=1}^{N} \omega_i - 1}$$

Le schéma suivant montre comment AWS IoT SiteWise les fonctions temporelles`first`, `last` `earliest``latest`, et sont calculées par rapport à l'intervalle de temps actuel.



> **Note**
>
> - L'intervalle de temps pour`first(x)`, `last(x)` est (début de la fenêtre actuelle, fin de la fenêtre actuelle].
> - L'intervalle de temps pour `latest(x)` est [début du temps, fin de la fenêtre actuelle].
> - La plage de temps pour `earliest(x)` est (début de l'heure, fin de la fenêtre précédente).

Paramètres des fonctions pondérés dans le temps

Les fonctions pondérées dans le temps calculées pour la fenêtre d'agrégation prennent en compte les éléments suivants :

- Points de données à l'intérieur de la fenêtre
- Intervalles de temps entre les points de données
- Dernier point de données avant la fenêtre
- Premier point de données après la fenêtre (pour certains algorithmes)

Termes :

- Point de données incorrect : tout point de données dont la qualité n'est pas bonne ou dont la valeur n'est pas numérique. Ceci n'est pas pris en compte dans le calcul des résultats d'une fenêtre.
- Intervalle incorrect — Intervalle après un point de données incorrect. L'intervalle avant le premier point de données connu est également considéré comme un mauvais intervalle.
- Bon point de données — Tout point de données présentant une bonne qualité et une bonne valeur numérique.

> **Note**
>
> - AWS IoT SiteWise ne consomme des données `GOOD` de qualité que lorsqu'il calcule les transformations et les métriques. Il ignore les points `UNCERTAIN` de `BAD` données.
> - L'intervalle avant le premier point de données connu est considéré comme un mauvais intervalle. Pour plus d'informations, consultez the section called "Tutoriels d'expression de formules".

L'intervalle après le dernier point de données connu se poursuit indéfiniment, affectant toutes les fenêtres suivantes. Lorsqu'un nouveau point de données arrive, la fonction recalcule l'intervalle.

Conformément aux règles ci-dessus, le résultat agrégé des fenêtres est calculé et limité aux limites des fenêtres. Par défaut, la fonction envoie le résultat de la fenêtre uniquement si l'ensemble de la fenêtre correspond à un bon intervalle.

Si l'intervalle de validité de la fenêtre est inférieur à la longueur de la fenêtre, la fonction n'envoie pas la fenêtre.

Lorsque les points de données affectant le résultat de la fenêtre changent, la fonction recalcule la fenêtre, même si les points de données se trouvent en dehors de la fenêtre.

Si la propriété d'entrée comporte au moins un point de données dans son historique et qu'un calcul a été lancé, la fonction calcule les fonctions d'agrégation pondérées dans le temps pour chaque intervalle de temps.

Example Exemple de scénario statetime

Prenons un exemple où vous avez une ressource avec les propriétés suivantes :

- `Idle`— Une mesure qui est `0` ou`1`. Lorsque la valeur est `1`, la machine est inactive.
- `Idle Time`— Mesure qui utilise la formule `statetime(Idle)` pour calculer la durée en secondes pendant laquelle la machine est inactive, par intervalle d'une minute.

La propriété `Idle` possède les points de données suivants.

Horodatage	2:00:00 PM	2:00:30 PM	2:01:15 PM	2:02:45 PM	2:04:00 PM
Idle	0	1	1	0	0

AWS IoT SiteWise calcule la `Idle Time` propriété toutes les minutes à partir des valeurs de`Idle`. Une fois ce calcul terminé, la propriété `Idle Time` possède les points de données suivants.

Horodatage	2:00:00 PM	2:01:00 PM	2:02:00 PM	2:03:00 PM	2:04:00 PM
Idle Time	N/A	30	60	45	0

AWS IoT SiteWise effectue les calculs suivants `Idle Time` à la fin de chaque minute.

- À 2:00 PM (pour 1:59 PM à 2:00 PM)
  - Il n'y a pas de données pour `Idle` avant 2:00 PM, donc aucun point de données n'est calculé.
- À 2:01 PM (pour 2:00 PM à 2:01 PM)
  - À 2:00:00 PM, la machine est active (`Idle` est égal à `0`).

  - À 2:00:30 PM, la machine es inactive (`Idle` est égal à 1).
  - `Idle` ne change plus avant la fin de l'intervalle à 2:01:00 PM, `Idle Time`est donc égal à 30 secondes.
- À 2:02 PM (pour 2:01 PM à 2:02 PM)
  - À 2:01:00 PM, la machine est inactive (conformément au dernier point de données à 2:00:30 PM).
  - À 2:01:15 PM, la machine est toujours inactive.
  - `Idle` ne change plus non plus avant la fin de l'intervalle à 2:02:00 PM, `Idle Time` est donc égal à 60 secondes.
- À 2:03 PM (pour 2:02 PM à 2:03 PM)
  - À 2:02:00 PM, la machine est inactive (conformément au dernier point de données à 2:01:15 PM).
  - À 2:02:45 PM, la machine est active.
  - `Idle` ne change plus non plus avant la fin de l'intervalle à 2:03:00 PM, `Idle Time` est donc égal à 45 secondes.
- À 2:04 PM (pour 2:03 PM à 2:04 PM)
  - À 2:03:00 PM, la machine est active (conformément au dernier point de données à 2:02:45 PM).
  - `Idle` ne change plus non plus avant la fin de l'intervalle à 2:04:00 PM, `Idle Time` est donc égal à 0 seconde.

Example Exemple TimeWeightedAvg et TimeWeightedStDev scénario

Les tableaux suivants fournissent des exemples d'entrées et de sorties pour ces métriques de fenêtre d'une minute :`Avg(x)`, `TimeWeightedAvg(x)`, `TimeWeightedAvg(x, "linear")`, `stDev(x)`, `timeWeightedStDev(x)`, `timeWeightedStDev(x, 'p')`.

Exemple de saisie pour une fenêtre agrégée d'une minute :

> **Note**
>
> Ces points de données sont tous `GOOD` de qualité.

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

Résultats agrégés en sortie :

> **Note**
>
> Aucun — Résultat non produit pour cette fenêtre.

Heure	`Avg(x)`	`TimeWeighted Avg(x)`	`TimeWeighted Avg(X, "linear")`	`stDev(X)`	`timeWeighted StDev(x)`	`timeWeighted StDev(x, 'p')`
3:00:00	4	Aucun	Aucun	0	Aucun	Aucun
3:01:00	2	4	3	0	0	0
3:02:00	14	9	13	6	5,430610041581775	5,385164807134504
3:03:00	11	13	12,875	8,54400374531753	7,724054437220943	7,659416862050705

Heure	**Avg(x)**	**TimeWeighted Avg(x)**	**TimeWeighted Avg(X, "linear")**	**stDev(X)**	**timeWeighted StDev(x)**	**timeWeighted StDev(x, 'p')**
3:04:00	0 USD	10	2,5	0	10,084389 681792215	10
3:05:00	Aucun	0	0	Aucun	0	0

Utilisation de fonctions temporelles dans les transformations

Dans les transformations uniquement, vous pouvez utiliser la `pretrigger()` fonction pour récupérer la valeur de GOOD qualité d'une variable avant la mise à jour de propriété qui a lancé le calcul de transformation en cours.

Prenons l'exemple d'un fabricant AWS IoT SiteWise qui surveille l'état d'une machine. Le fabricant utilise les mesures et transformations suivantes pour représenter le processus :

- Une mesure`current_state`, qui peut être 0 ou 1.
  - Si la machine est en état de nettoyage, `current_state` égal à 1.
  - Si la machine est en cours de fabrication, `current_state` est égal à 0.
- Une transformation`cleaning_state_duration`, ça équivaut à`if(pretrigger(current_state) == 1, timestamp(current_state) - timestamp(pretrigger(current_state)), none)`. Cette transformation renvoie la durée pendant laquelle la machine est restée en état de nettoyage en secondes, au format Unix Epoch. Pour plus d'informations, consultez Utilisation de fonctions conditionnelles dans les expressions de formule et la fonction timestamp ().

Si la machine reste en état de nettoyage plus longtemps que prévu, le fabricant peut examiner la machine.

Vous pouvez également utiliser la `pretrigger()` fonction dans des transformations multivariées. Par exemple, vous avez deux mesures nommées `x` et`y`, et une transformation`z`, égale à`x + y + pretrigger(y)`. Le tableau suivant indique les valeurs pour `x`y, et `z` entre 9 h 00 et 9 h 15.

> **Note**
>
> - Cet exemple suppose que les valeurs des mesures arrivent par ordre chronologique. Par exemple, la valeur de `x` pour 9 h 00 arrive avant la valeur de `x` pour 9 h 05.
> - Si les points de données de 9 h 05 arrivent avant les points de données de 9 h 00, cela `z` n'est pas calculé à 9 h 05.
> - Si la valeur de `x` pour 9 h 05 arrive avant la valeur de `x` pour 9 h 00 et que les valeurs de `y` arrivent chronologiquement, `z` est égale `22 = 20 + 1 + 1` à 9 h 05.

	9 H 00	9 H 05	9 H 10	9 H 15
x	10	20		30
y	1	2	3	
`z = x + y + pretrigger(y)`	yne reçoit aucun point de données avant 9h00. Par conséquent, z n'est pas calculé à 9 h 00.	23 = 20 + 2 + 1 `pretrigger(y)` est égal à 1.	25 = 20 + 3 + 2 xne reçoit pas de nouveau point de données. `pretrigger(y)` est égal à 2.	36 = 30 + 3 + 3 yne reçoit pas de nouveau point de données. Par conséquent, `pretrigger(y)` est égal à 3 à 9 h 15.

Utilisation des fonctions de date et d'heure dans les expressions de formule

Dans les transformations et les métriques, vous pouvez utiliser les fonctions de date et d'heure de la manière suivante :

- Récupérez l'horodatage actuel d'un point de données en UTC ou dans le fuseau horaire local.
- Construisez des horodatages avec des arguments tels que `yearmonth`, et. `day_of_month`
- Extrayez une période telle qu'une année ou un mois avec l'`unix_time`argument.

Fonction	Description
`now()`	Renvoie la date et l'heure actuelles, en secondes, au format Unix Epoch.
`timestamp()`	• Lors des transformations, la fonction renvoie l'horodatage, en secondes, du message d'entrée au format Unix Epoch. Dans les transformations uniquement, vous pouvez effectuer l'une des opérations suivantes : • Fournissez une variable comme argument à la fonction. La `timestamp ( variable-name )` fonction renvoie l'horodatage, en secondes, de la dernière valeur de `GOOD` qualité pour la variable spécifiée au format Unix Epoch. Par exemple, si votre actif possède une propriété de transformation nommée `Temperature_F` qui utilise la `9/5 * Temperature_C` formule pour convertir chaque point de données de température de degrés Celsius en degrés Fahrenhei t, vous pouvez utiliser cette `timestamp (Temperature_F)` fonction pour obtenir l'horodatage de la dernière valeur de `GOOD` qualité de la propriété. `Temperature_F` • Utilisez la `pretrigger()` fonction comme argument de la fonction. La `timestamp(pretrigger( variable-name ))` fonction renvoie l'horodatage, en secondes, de la valeur de `GOOD` qualité pour la variable spécifiée avant la mise à jour de la propriété qui a initié le calcul

Fonction	Description
	de transformation actuel au format Unix Epoch. Pour plus d'informations, consultez Utilisation de fonctions temporelles dans les transformations. • En métriques, la fonction renvoie l'horodat age récupéré à la fin de la fenêtre en cours, en secondes, au format Unix Epoch.

Fonction	Description
`mktime(time_zone, year, month, day_of_month, hour, minute, second)`	Renvoie le temps d'entrée en secondes, au format Unix Epoch. Les conditions suivantes s'appliquent à l'utilisation de cette fonction : • L'argument de fuseau horaire doit être une chaîne entre guillemets (`'UTC'`). S'il n'est pas spécifié, le fuseau horaire par défaut est UTC. L'argument du fuseau horaire peut être le premier ou le dernier argument. • L'année, le mois, le jour du mois, l'heure, la minute et le deuxième argument doivent être en ordre. • Les arguments relatifs à l'année, au mois et à la date sont obligatoires. Les limites suivantes s'appliquent à l'utilisation de cette fonction : • `year`- Les valeurs valides sont comprises entre 1970 et 2250. • `month`- Les valeurs valides sont comprises entre 1 et 12. • `day-of-month` - Les valeurs valides sont comprises entre 1 et 31. • `hour`- Les valeurs valides sont comprises entre 0 et 23. • `minute`- Les valeurs valides sont comprises entre 0 et 59.

Fonction	Description
	• `second`- Les valeurs valides sont comprises entre 0 et 60. Il peut s'agir d'un nombre à virgule flottante. Exemples : • `mktime(2020, 2, 29)` • `mktime('UTC+3', 2021, 12, 31, 22)` • `mktime(2022, 10, 13, 2, 55, 13.68, 'PST')`

Fonction	Description
`localtime(unix_time, time_zone)`	Renvoie l'année, le jour du mois, le jour de la semaine, le jour de l'année, l'heure, la minute ou la seconde du fuseau horaire spécifié par rapport à l'heure Unix. Les conditions suivantes s'appliquent à l'utilisation de cette fonction : • L'argument de fuseau horaire doit être une chaîne entre guillemets (`'UTC'`). S'il n'est pas spécifié, le fuseau horaire par défaut est UTC. • L'argument Unix time est le temps en secondes, au format Unix Epoch. La plage valide est comprise entre 1 et 31556889864403199. Il peut s'agir d'un nombre à virgule flottante. Exemple de réponse : `2007-12-03T10:15:30+01:00[Europe/Paris]` `localtime(unix_time, time_zone)` n'est pas une fonction autonome. Les `sec()` fonctions `year()` `mon()``mday`,`wday()`,`yday()`, `hour()``minute()`,, et prennent `localtime(unix_time, time_zone)` comme argument.  Exemples :  • `year(localtime('GMT', 1605898608.8113723))` • `now().localtime().year()`

Fonction	Description
	• `timestamp().localtime('PST' ).year()` • `localtime(1605289736, 'Europe/L ondon').year()`
`year(localtime(unix_time, time_zone)`	Renvoie l'année à partir de`localtime (unix_time, time_zone)` .
`mon(localtime(unix_time, time_zone))`	Renvoie le mois de`localtime(unix_tim e, time_zone)` .
`mday(localtime(unix_time, time_zone))`	Renvoie le jour du mois à partir de`localtime (unix_time, time_zone)` .
`wday(localtime(unix_time, time_zone))`	Renvoie le jour de la semaine à partir de`localtime(unix_time, time_zone ) .`
`yday(localtime(unix_time, time_zone))`	Renvoie le jour de l'année à partir de`localtime(unix_time, time_zone ) .`
`hour(localtime(unix_time, time_zone))`	Renvoie l'heure de`localtime(unix_tim e, time_zone)` .
`minute(localtime(unix_time, time_zone))`	Renvoie la minute de`localtime(unix_tim e, time_zone)` .
`sec(localtime(unix_time, time_zone))`	Renvoie le second de`localtime(unix_tim e, time_zone)` .

Formats de fuseau horaire pris en charge

Vous pouvez spécifier l'argument du fuseau horaire de différentes manières :

- Décalage de fuseau horaire - Spécifiez `'Z'` un UTC ou un décalage (`'+2'`ou`'-5'`).

- Identifiants de décalage : combinez une abréviation de fuseau horaire et un décalage. Par exemple : `'GMT+2'` et `'UTC-01:00'`. L'abréviation du fuseau horaire ne doit contenir que trois lettres.
- Identifiants basés sur la région : par exemple, `'Etc/GMT+12'` et`'Pacific/Pago_Pago'`.

Abréviations de fuseaux horaires prises en charge

Les fonctions de date et d'heure prennent en charge les abréviations de fuseau horaire à trois lettres suivantes :

- EST - 05:00
- HST - 10:00
- MARDI - 07:00
- ACT - Australie/Darwin
- AET - Australie/Sydney
- AGT - America/Argentine/Buenos_Aires
- ART - Africa/Le Caire
- AST - Amérique/Anchorage
- BET - America/Sao_Paulo
- BST - Asia/Dhaka
- CAT - Afrique/Harare
- CET - Europe/Paris
- CNT - America/St_Johns
- CST - America/Chicago
- CTT - Asia/Shanghai
- EAT - Africa/Addis_Abeba
- IET - America/Indiana/Indianapolis
- IST - Asia/Kolkata
- JST - Asia/Tokyo
- MIT - Pacific/Apia
- NET - Asia/Yerevan

- NST - Pacific/Auckland
- PLT - Asia/Karachi
- PRT - America/Puerto_Rico
- PST - America/Los_Angeles
- SST - Pacific/Guadalcanal
- VST - Asia/Ho_Chi_Minh

Identifiants basés sur les régions pris en charge

Les fonctions de date et d'heure prennent en charge les identifiants régionaux suivants, organisés en fonction de leur relation avec UTC+ 00:00 :

- ETC/GMT+12 (UTC- 12h00)
- Pacific/Pago_Pago (UTC- 11:00)
- Pacifique/Samoa (UTC- 11:00)
- Pacifique/Niue (UTC- 11:00)
- États-Unis/Samoa (UTC- 11:00)
- ETC/GMT+11 (UTC- 11:00)
- Pacifique/Midway (UTC- 11:00)
- Pacifique/Honolulu (UTC- 10:00)
- Pacifique/Rarotonga (UTC- 10:00)
- Pacifique/Tahiti (UTC- 10:00)
- Pacifique/Johnston (UTC- 10:00)
- États-Unis/Hawaï (UTC- 10:00)
- Système V/HST10 (UTC- 10:00)
- ETC/GMT+10 (UTC- 10:00)
- Pacifique/Marquises (UTC- 09:30)
- ETC/GMT+9 (UTC- 09:00)
- Pacifique/Gambier (UTC- 09:00)
- Amérique/Atka (UTC- 09:00)

- Système V/YST9 (UTC- 09:00)
- Amérique/Adak (UTC- 09:00)
- Etats-Unis/Aléoutiennes (UTC- 09:00)
- ETC/GMT+8 (UTC- 08:00)
- États-Unis/Alaska (UTC- 08:00)
- Amérique/Juneau (UTC- 08:00)
- Amérique/Metlakatla (UTC- 08:00)
- Amérique/Yakutat (UTC- 08:00)
- Pacifique/Pitcairn (UTC- 08:00)
- Amérique/Sitka (UTC- 08:00)
- Amérique/Anchorage (UTC- 08:00)
- Système V/PST8 (UTC- 08:00)
- Amérique/Nome (UTC- 08:00)
- Système V/YST9YDT (UTC- 08:00)
- Canada/Yukon (UTC- 07:00)
- US/Pacific-New (UTC- 07:00)
- ETC/GMT+7 (UTC- 07:00)
- Etats-Unis/Arizona (UTC- 07:00)
- Amérique/Dawson_Creek (UTC- 07:00)
- Canada/Pacifique (UTC- 07:00)
- PST8PDT (UTC- 07:00)
- Système V/MST7 (UTC- 07:00)
- Amérique/Dawson (UTC- 07:00)
- Mexique/ BajaNorte (UTC- 07:00)
- Amérique/Tijuana (UTC- 07:00)
- Amérique/Creston (UTC- 07:00)
- America/Hermosillo (UTC- 07:00)
- Amérique/Santa_Isabel (UTC- 07:00)
- Amérique/Vancouver (UTC- 07:00)

- America/Ensenada (UTC- 07:00)
- Amérique/Phoenix (UTC- 07:00)
- Amérique/Whitehorse (UTC- 07:00)
- America/Fort_Nelson (UTC- 07:00)
- SystemV/PST8PDT (UTC- 07:00)
- Amérique/Los_Angeles (UTC- 07:00)
- États-Unis/Pacifique (UTC- 07:00)
- America/El Salvador (UTC- 06:00)
- Amérique/Guatemala (UTC- 06:00)
- Amérique/Belize (UTC- 06:00)
- Amérique/Managua (UTC- 06:00)
- America/Tegucigalpa (UTC- 06:00)
- ETC/GMT+6 (UTC- 06:00)
- Pacifique/Pâques (UTC- 06:00)
- Mexique/ BajaSur (UTC- 06:00)
- America/Regina (UTC- 06:00)
- Amérique/Denver (UTC- 06:00)
- Pacifique/Galapagos (UTC- 06:00)
- Amérique/Yellowknife (UTC- 06:00)
- America/Swift_Current (UTC- 06:00)
- Amérique/Inuvik (UTC- 06:00)
- Amérique/Mazatlan (UTC- 06:00)
- Amérique/Boise (UTC- 06:00)
- Amérique/Costa_Rica (UTC- 06:00)
- MST7MDT (UTC- 06:00)
- Système V/CST6 (UTC- 06:00)
- Amérique/Chihuahua (UTC- 06:00)
- Amérique/Ojinaga (UTC- 06:00)
- Chili/ EasterIsland (UTC- 06:00)

- Etats-Unis/Montagne (UTC- 06:00)
- Amérique/Edmonton (UTC- 06:00)
- Canada/Montagne (UTC- 06:00)
- Amérique/Cambridge_Bay (UTC- 06:00)
- Navajo (UTC- 06:00)
- SystemV/MST7MDT (UTC- 06:00)
- Canada/Saskatchewan (UTC- 06:00)
- Amérique/Shiprock (UTC- 06:00)
- Amérique/Panama (UTC- 05:00)
- Amérique/Chicago (UTC- 05:00)
- America/Eirunepe (UTC- 05:00)
- ETC/GMT+5 (UTC- 05:00)
- Mexique/Général (UTC- 05:00)
- America/Porto_Acre (UTC- 05:00)
- Amérique/Guayaquil (UTC- 05:00)
- America/Rankin_Inlet (UTC- 05:00)
- US/Central (UTC- 05:00)
- Amérique/Rainy_River (UTC- 05:00)
- Amérique/Indiana/Knox (UTC- 05:00)
- Amérique/Dakota du Nord/Beulah (UTC- 05:00)
- Amérique/Monterrey (UTC- 05:00)
- Amérique/Jamaïque (UTC- 05:00)
- Amérique/Atikokan (UTC- 05:00)
- America/Coral_Harbour (UTC- 05:00)
- Amérique/Dakota du Nord/Centre (UTC- 05:00)
- Amérique/Cayman (UTC- 05:00)
- Amérique/Indiana/Tell_City (UTC- 05:00)
- America/Mexico_City (UTC- 05:00)
- Amérique/Matamoros (UTC- 05:00)

- CST6CDT (UTC- 05:00)
- America/Knox_IN (UTC- 05:00)
- Amérique/Bogota (UTC- 05:00)
- Amérique/Menominee (UTC- 05:00)
- America/Resolute (UTC- 05:00)
- Système V/EST5 (UTC- 05:00)
- Canada/Centre (UTC- 05:00)
- Brésil/Acre (UTC- 05:00)
- Amérique/Cancun (UTC- 05:00)
- Amérique/Lima (UTC- 05:00)
- Amérique/Bahia_Banderas (UTC- 05:00)
- US/Indiana-Starke (UTC- 05:00)
- America/Rio_Branco (UTC- 05:00)
- SystemV/CST6CDT (UTC- 05:00)
- Jamaïque (UTC- 05:00)
- Amérique/Mérida (UTC- 05:00)
- Amérique/Dakota du Nord/New_Salem (UTC- 05:00)
- Amérique/Winnipeg (UTC- 05:00)
- Amérique/Cuiaba (UTC- 04:00)
- Amérique/Marigot (UTC- 04:00)
- Amérique/Indiana/Petersburg (UTC- 04:00)
- Chili/Continental (UTC- 04:00)
- America/Grand_Turk (UTC- 04:00)
- Cuba (UTC- 04:00)
- ETC/GMT+4 (UTC- 04:00)
- Amérique/Manaus (UTC- 04:00)
- Amérique/Fort_Wayne (UTC- 04:00)
- America/St_Thomas (UTC- 04:00)
- Amérique/Anguilla (UTC- 04:00)

- Amérique/La Havane (UTC- 04:00)
- États-Unis/Michigan (UTC- 04:00)
- Amérique/Barbade (UTC- 04:00)
- Amérique/Louisville (UTC- 04:00)
- Amérique/Curaçao (UTC- 04:00)
- Amérique/Guyana (UTC- 04:00)
- Amérique/Martinique (UTC- 04:00)
- Amérique/Porto_Rico (UTC- 04:00)
- Amérique/Port_of_Spain (UTC- 04:00)
- Système V/AST4 (UTC- 04:00)
- Amérique/Indiana/Vevay (UTC- 04:00)
- Amérique/Indiana/Vincennes (UTC- 04:00)
- America/Kralendijk (UTC- 04:00)
- Amérique/Antigua (UTC- 04:00)
- Amérique/Indianapolis (UTC- 04:00)
- Amérique/Iqaluit (UTC- 04:00)
- America/St_Vincent (UTC- 04:00)
- Amérique/Kentucky/Louisville (UTC- 04:00)
- Amérique/Dominique (UTC- 04:00)
- America/Asuncion (UTC- 04:00)
- 5 EST (UTC- 04:00)
- Amérique/Nassau (UTC- 04:00)
- Amérique/Kentucky/Monticello (UTC- 04:00)
- Brésil/Ouest (UTC- 04:00)
- Amérique/Aruba (UTC- 04:00)
- Amérique/Indiana/Indianapolis (UTC- 04:00)
- Amérique/Santiago (UTC- 04:00)
- America/La_Paz (UTC- 04:00)
- America/Thunder_Bay (UTC- 04:00)

- Amérique/Indiana/Marengo (UTC- 04:00)
- Amérique/Blanc-Sablon (UTC- 04:00)
- America/Santo_Domingo (UTC- 04:00)
- Etats-Unis/Est (UTC- 04:00)
- Canada/Est (UTC- 04:00)
- Amérique/Port-au-Prince (UTC- 04:00)
- America/Saint-Barthélemy (UTC- 04:00)
- Amérique/Nipigon (UTC- 04:00)
- Etats-Unis/Est de l'Indiana (UTC- 04:00)
- Amérique/Sainte-Lucie (UTC- 04:00)
- Amérique/Montserrat (UTC- 04:00)
- America/Lower_Princes (UTC- 04:00)
- Amérique/Détroit (UTC- 04:00)
- Amérique/Tortola (UTC- 04:00)
- America/Porto_Velho (UTC- 04:00)
- America/Campo_Grande (UTC- 04:00)
- America/Virgin (UTC- 04:00)
- America/Pangnirtung (UTC- 04:00)
- Amérique/Montréal (UTC- 04:00)
- Amérique/Indiana/Winamac (UTC- 04:00)
- Amérique/Boa_Vista (UTC- 04:00)
- Amérique/Grenade (UTC- 04:00)
- Amérique/New_York (UTC- 04:00)
- America/St_Kitts (UTC- 04:00)
- Amérique/Caracas (UTC- 04:00)
- Amérique/Guadeloupe (UTC- 04:00)
- Amérique/Toronto (UTC- 04:00)
- SystemV/EST5EDT (UTC- 04:00)
- Amérique/Argentine/Catamarca (UTC- 03:00)

- Canada/Atlantique (UTC- 03:00)
- Amérique/Argentine/Cordoba (UTC- 03:00)
- Amérique/Araguaina (UTC- 03:00)
- Amérique/Argentine/Salta (UTC- 03:00)
- ETC/GMT+3 (UTC- 03:00)
- Amérique/Montevideo (UTC- 03:00)
- Brésil/Est (UTC- 03:00)
- Amérique/Argentine/Mendoza (UTC- 03:00)
- Amérique/Argentine/Rio_Gallegos (UTC- 03:00)
- Amérique/Catamarca (UTC- 03:00)
- Amérique/Cordoba (UTC- 03:00)
- America/Sao_Paulo (UTC- 03:00)
- Amérique/Argentine/Jujuy (UTC- 03:00)
- Amérique/Cayenne (UTC- 03:00)
- Amérique/Recife (UTC- 03:00)
- America/Buenos_Aires (UTC- 03:00)
- Amérique/Paramaribo (UTC- 03:00)
- Amérique/Moncton (UTC- 03:00)
- America/Mendoza (UTC- 03:00)
- Amérique/Santarém (UTC- 03:00)
- Atlantique/Bermudes (UTC- 03:00)
- Amérique/Maceio (UTC- 03:00)
- Atlantic/Stanley (UTC- 03:00)
- Amérique/Halifax (UTC- 03:00)
- Antarctique/Rothera (UTC- 03:00)
- Amérique/Argentine/San_Luis (UTC- 03:00)
- Amérique/Argentine/Ushuaïa (UTC- 03:00)
- Antarctique/Palmer (UTC- 03:00)
- America/Punta_Arenas (UTC- 03:00)

- Amérique/Glace_Bay (UTC- 03:00)
- America/Fortaleza (UTC- 03:00)
- Amérique/Thule (UTC- 03:00)
- Amérique/Argentine/La_Rioja (UTC- 03:00)
- Amérique/Belém (UTC- 03:00)
- America/Jujuy (UTC- 03:00)
- Amérique/Bahia (UTC- 03:00)
- Amérique/Goose_Bay (UTC- 03:00)
- Amérique/Argentine/San_Juan (UTC- 03:00)
- Amérique/Argentine/ ComodRivadavia (UTC- 03:00)
- Amérique/Argentine/Tucuman (UTC- 03:00)
- America/Rosario (UTC- 03:00)
- SystemV/AST4ADT (UTC- 03:00)
- Amérique/Argentine/Buenos_Aires (UTC- 03:00)
- America/St_Johns (UTC- 02:30)
- Canada/Terre-Neuve (UTC- 02:30)
- Amérique/Miquelon (UTC- 02:00)
- ETC/GMT+2 (UTC- 02:00)
- Amérique/Godthab (UTC- 02:00)
- America/Noronha (UTC- 02:00)
- Brésil/ DeNoronha (UTC- 02:00)
- Atlantique/Géorgie du Sud (UTC- 02:00)
- Etc/GMT+1 (UTC- 01:00)
- Atlantique/Cap-Vert (UTC- 01:00)
- Pacifique/Kiritimati (UTC+ 14:00)
- Etc/GMT-14 (UTC+ 14:00)
- Pacifique/Fakaofo (UTC+ 13:00)
- Pacifique/Enderbury (UTC+ 13:00)
- Pacifique/Apia (UTC+ 13:00)

- Pacifique/Tongatapu (UTC+ 13:00)
- Etc/GMT-13 (UTC+ 13:00)
- NZ-CHAT (UTC+ 12:45)
- Pacifique/Chatham (UTC+ 12:45)
- Pacifique/Kwajalein (UTC+ 12:00)
- Antarctique/ McMurdo (UTC+ 12:00)
- Pacifique/Wallis (UTC+ 12:00)
- Pacifique/Fidji (UTC+ 12:00)
- Pacifique/Funafuti (UTC+ 12:00)
- Pacifique/Nauru (UTC+ 12:00)
- Kwajalein (UTC+ 12:00)
- NOUVELLE-ZÉLANDE (UTC+ 12:00)
- Pacific/Wake (UTC+ 12:00)
- Antarctique/Pôle Sud (UTC+ 12:00)
- Pacifique/Tarawa (UTC+ 12:00)
- Pacifique/Auckland (UTC+ 12:00)
- Asie/Kamchatka (UTC+ 12:00)
- etc/GMT-12 (UTC+ 12:00)
- Asie/Anadyr (UTC+ 12:00)
- Pacifique/Majuro (UTC+ 12:00)
- Pacifique/Ponape (UTC+ 11:00)
- Pacifique/Bougainville (UTC+ 11:00)
- Antarctique/Macquarie (UTC+ 11:00)
- Pacifique/Pohnpei (UTC+ 11:00)
- Pacifique/Efate (UTC+ 11:00)
- Pacifique/Norfolk (UTC+ 11:00)
- Asie/Magadan (UTC+ 11:00)
- Pacifique/Kosrae (UTC+ 11:00)
- Asie/Sakhaline (UTC+ 11:00)

- Pacifique/Nouméa (UTC+ 11:00)
- Etc/GMT-11 (UTC+ 11:00)
- Asie/Srednekolymsk (UTC+ 11:00)
- Pacifique/Guadalcanal (UTC+ 11:00)
- Australie/Lord_Howe (UTC+ 10:30)
- Australie/LHI (UTC+ 10:30)
- Australie/Hobart (UTC+ 10:00)
- Pacifique/Yap (UTC+ 10:00)
- Australie/Tasmanie (UTC+ 10:00)
- Pacifique/Port_Moresby (UTC+ 10:00)
- Australie/ACT (UTC+ 10:00)
- Australie/Victoria (UTC+ 10:00)
- Pacifique/Chuuk (UTC+ 10:00)
- Australie/Queensland (UTC+ 10:00)
- Australie/Canberra (UTC+ 10:00)
- Australie/Currie (UTC+ 10:00)
- Pacifique/Guam (UTC+ 10:00)
- Pacifique/Truk (UTC+ 10:00)
- Australie/NSW (UTC+ 10:00)
- Asie/Vladivostok (UTC+ 10:00)
- Pacifique/Saipan (UTC+ 10:00)
- Antarctique/Dumontdurville (UTC+ 10:00)
- Australie/Sydney (UTC+ 10:00)
- Australie/Brisbane (UTC+ 10:00)
- Etc/GMT-10 (UTC+ 10:00)
- Asie/Ust-Nera (UTC+ 10:00)
- Australie/Melbourne (UTC+ 10:00)
- Australie/Lindeman (UTC+ 10:00)
- Australie/Nord (UTC+ 09:30)

- Australie/Yancowinna (UTC+ 09:30)
- Australie/Adélaïde (UTC+ 09:30)
- Australie/Broken_Hill (UTC+ 09:30)
- Australie/Sud (UTC+ 09:30)
- Australie/Darwin (UTC+ 09:30)
- Etc/GMT-9 (UTC+ 09:00)
- Pacifique/Palaos (UTC+ 09:00)
- Asie/Chita (UTC+ 09:00)
- Asie/Dili (UTC+ 09:00)
- Asie/Jayapura (UTC+ 09:00)
- Asie/Yakutsk (UTC+ 09:00)
- Asie/Pyongyang (UTC+ 09:00)
- MERCREDI (UTC+ 09:00)
- Asie/Séoul (UTC+ 09:00)
- Asie/Khandyga (UTC+ 09:00)
- Japon (UTC+ 09:00)
- Asie/Tokyo (UTC+ 09:00)
- Australie/Eucla (UTC+ 08:45)
- Asie/Kuching (UTC+ 08:00)
- Asie/Chungking (UTC+ 08:00)
- Etc/GMT-8 (UTC+ 08:00)
- Australie/Perth (UTC+ 08:00)
- Asie/Macao (UTC+ 08:00)
- Asie/Macao (UTC+ 08:00)
- Asie/Choibalsan (UTC+ 08:00)
- Asie/Shanghai (UTC+ 08:00)
- Antarctique/Casey (UTC+ 08:00)
- Asie/Ulan_Bator (UTC+ 08:00)
- Asie/Chongqing (UTC+ 08:00)

- Asie/Oulan-Bator (UTC+ 08:00)
- Asie/Taipei (UTC+ 08:00)
- Asie/Manille (UTC+ 08:00)
- PRC (UTC+ 08:00)
- Asie/Ujung_Pandang (UTC+ 08:00)
- Asie/Harbin (UTC+ 08:00)
- Singapour (UTC+ 08:00)
- Asie/Brunei (UTC+ 08:00)
- Australie/Ouest (UTC+ 08:00)
- Asie/Hong_Kong (UTC+ 08:00)
- Asie/Makassar (UTC+ 08:00)
- Hong Kong (UTC+ 08:00)
- Asie/Kuala_Lumpur (UTC+ 08:00)
- Asie/Irkutsk (UTC+ 08:00)
- Asie/Singapour (UTC+ 08:00)
- Asie/Pontianak (UTC+ 07:00)
- Etc/GMT-7 (UTC+ 07:00)
- Asie/Phnom_Penh (UTC+ 07:00)
- Asie/Novossibirsk (UTC+ 07:00)
- Antarctique/Davis (UTC+ 07:00)
- Asie/Tomsk (UTC+ 07:00)
- Asie/Jakarta (UTC+ 07:00)
- Asie/Barnaoul (UTC+ 07:00)
- Indien/Noël (UTC+ 07:00)
- Asie/Ho_Chi_Minh (UTC+ 07:00)
- Asie/Hovd (UTC+ 07:00)
- Asie/Bangkok (UTC+ 07:00)
- Asie/Vientiane (UTC+ 07:00)
- Asie/Novokuznetsk (UTC+ 07:00)

- Asie/Krasnoïarsk (UTC+ 07:00)
- Asie/Saigon (UTC+ 07:00)
- Asie/Yangon (UTC+ 06:30)
- Asie/Rangoon (UTC+ 06:30)
- Indien/Cocos (UTC+ 06:30)
- Asie/Kachgar (UTC+ 06:00)
- Etc/GMT-6 (UTC+ 06:00)
- Asie/Almaty (UTC+ 06:00)
- Asie/Dacca (UTC+ 06:00)
- Asie/Omsk (UTC+ 06:00)
- Asie/Dhaka (UTC+ 06:00)
- Indien/Chagos (UTC+ 06:00)
- Asie/Qyzylorda (UTC+ 06:00)
- Asie/Bichkek (UTC+ 06:00)
- Antarctique/Vostok (UTC+ 06:00)
- Asie/Urumqi (UTC+ 06:00)
- Asie/Thimbu (UTC+ 06:00)
- Asie/Thimphou (UTC+ 06:00)
- Asie/Katmandou (UTC+ 05:45)
- Asie/Katmandou (UTC+ 05:45)
- Asie/Kolkata (UTC+ 05:30)
- Asie/Colombo (UTC+ 05:30)
- Asie/Calcutta (UTC+ 05:30)
- Asie/Aqtau (UTC+ 05:00)
- Etc/GMT-5 (UTC+ 05:00)
- Asie/Samarkand (UTC+ 05:00)
- Asie/Karachi (UTC+ 05:00)
- Asie/Ekaterinbourg (UTC+ 05:00)
- Asie/Douchanbé (UTC+ 05:00)

- Indien/Maldives (UTC+ 05:00)
- Asie/Oral (UTC+ 05:00)
- Asie/Tachkent (UTC+ 05:00)
- Antarctique/Mawson (UTC+ 05:00)
- Asie/Aqtobe (UTC+ 05:00)
- Asie/Ashkhabad (UTC+ 05:00)
- Asie/Ashgabat (UTC+ 05:00)
- Asie/Atyrau (UTC+ 05:00)
- Indien/Kerguelen (UTC+ 05:00)
- Iran (UTC+ 04:30)
- Asie/Téhéran (UTC+ 04:30)
- Asie/Kaboul (UTC+ 04:30)
- Asie/Yerevan (UTC+ 04:00)
- Etc/GMT-4 (UTC+ 04:00)
- Etc/GMT-4 (UTC+ 04:00)
- Asie/Dubaï (UTC+ 04:00)
- Indien/Réunion (UTC+ 04:00)
- Europe/Saratov (UTC+ 04:00)
- Europe/Samara (UTC+ 04:00)
- Indien/Mahé (UTC+ 04:00)
- Asie/Bakou (UTC+ 04:00)
- Asie/Muscat (UTC+ 04:00)
- Europe/Volgograd (UTC+ 04:00)
- Europe/Astrakhan (UTC+ 04:00)
- Asie/Tbilissi (UTC+ 04:00)
- Europe/Oulianovsk (UTC+ 04:00)
- Asie/Aden (UTC+ 03:00)
- Afrique/Nairobi (UTC+ 03:00)
- Europe/Istanbul (UTC+ 03:00)

- Etc/GMT-3 (UTC+ 03:00)
- Europe/Zaporijia (UTC+ 03:00)
- Israël (UTC+ 03:00)
- Indien/Comores (UTC+ 03:00)
- Antarctique/Syowa (UTC+ 03:00)
- Afrique/Mogadiscio (UTC+ 03:00)
- Europe/Bucarest (UTC+ 03:00)
- Afrique/Asmera (UTC+ 03:00)
- Europe/Mariehamn (UTC+ 03:00)
- Asie/Istanbul (UTC+ 03:00)
- Europe/Tiraspol (UTC+ 03:00)
- Europe/Moscou (UTC+ 03:00)
- Europe/Chișinău (UTC+ 03:00)
- Europe/Helsinki (UTC+ 03:00)
- Asie/Beyrouth (UTC+ 03:00)
- Asie/Tel_Aviv (UTC+ 03:00)
- Afrique/Djibouti (UTC+ 03:00)
- Europe/Simferopol (UTC+ 03:00)
- Europe/Sofia (UTC+ 03:00)
- Asie/Gaza (UTC+ 03:00)
- Afrique/Asmara (UTC+ 03:00)
- Europe/Riga (UTC+ 03:00)
- Asie/Bagdad (UTC+ 03:00)
- Asie/Damas (UTC+ 03:00)
- AFRIQUE/Dar_es_Salaam (UTC+ 03:00)
- Afrique/Addis_Abeba (UTC+ 03:00)
- Europe/Oujgorod (UTC+ 03:00)
- Asie/Jerusalem (UTC+ 03:00)
- Asie/Riyadh (UTC+ 03:00)

- Asie/Koweït (UTC+ 03:00)
- Europe/Kirov (UTC+ 03:00)
- Afrique/Kampala (UTC+ 03:00)
- Europe/Minsk (UTC+ 03:00)
- Asie/Qatar (UTC+ 03:00)
- Europe/Kiev (UTC+ 03:00)
- Asie/Bahreïn (UTC+ 03:00)
- Europe/Vilnius (UTC+ 03:00)
- Indien/Antananarivo (UTC+ 03:00)
- Indien/Mayotte (UTC+ 03:00)
- Europe/Tallinn (UTC+ 03:00)
- Turquie (UTC+ 03:00)
- Afrique/Juba (UTC+ 03:00)
- Asie/Nicosie (UTC+ 03:00)
- Asie/Famagouste (UTC+ 03:00)
- SAMEDI (UTC+ 03:00)
- RENCONTRE (UTC+ 03:00)
- Asie/Hébron (UTC+ 03:00)
- Asie/Amman (UTC+ 03:00)
- Europe/Nicosie (UTC+ 03:00)
- Europe/Athènes (UTC+ 03:00)
- Afrique/Le Caire (UTC+ 02:00)
- Afrique/Mbabane (UTC+ 02:00)
- Europe/Bruxelles (UTC+ 02:00)
- Europe/Varsovie (UTC+ 02:00)
- HEURE DE PARIS (UTC+ 02:00)
- Europe/Luxembourg (UTC+ 02:00)
- Etc/GMT-2 (UTC+ 02:00)
- Libye (UTC+ 02:00)

- Afrique/Kigali (UTC+ 02:00)
- Afrique/Tripoli (UTC+ 02:00)
- Europe/Kaliningrad (UTC+ 02:00)
- Afrique/Windhoek (UTC+ 02:00)
- Europe/Malte (UTC+ 02:00)
- Europe/Büsingen (UTC+ 02:00)
-
- Europe/Skopje (UTC+ 02:00)
- Europe/Sarajevo (UTC+ 02:00)
- Europe/Rome (UTC+ 02:00)
- Europe/Zürich (UTC+ 02:00)
- Europe/Gibraltar (UTC+ 02:00)
- Afrique/Lubumbashi (UTC+ 02:00)
- Europe/Vaduz (UTC+ 02:00)
- Europe/Ljubljana (UTC+ 02:00)
- Europe/Berlin (UTC+ 02:00)
- Europe/Stockholm (UTC+ 02:00)
- Europe/Budapest (UTC+ 02:00)
- Europe/Zagreb (UTC+ 02:00)
- Europe/Paris (UTC+ 02:00)
- Afrique/Ceuta (UTC+ 02:00)
- Europe/Praha (UTC+ 02:00)
- Antarctique/Troll (UTC+ 02:00)
- Afrique/Gaborone (UTC+ 02:00)
- Europe/Copenhague (UTC+ 02:00)
- Europe/Vienne (UTC+ 02:00)
- Europe/Tirana (UTC+ 02:00)
- MET (UTC+ 02:00)
- Europe/Amsterdam (UTC+ 02:00)

- Afrique/Maputo (UTC+ 02:00)
- Europe/Saint-Marin (UTC+ 02:00)
- Pologne (UTC+ 02:00)
- Europe/Andorre (UTC+ 02:00)
- Europe/Oslo (UTC+ 02:00)
- Europe/Podgorica (UTC+ 02:00)
- Afrique/Bujumbura (UTC+ 02:00)
- Atlantic/Jan_Mayen (UTC+ 02:00)
- Afrique/Maseru (UTC+ 02:00)
- Europe/Madrid (UTC+ 02:00)
- Afrique/Blantyre (UTC+ 02:00)
- Afrique/Lusaka (UTC+ 02:00)
- Afrique/Harare (UTC+ 02:00)
- Afrique/Khartoum (UTC+ 02:00)
- Afrique/Johannesburg (UTC+ 02:00)
- Europe/Belgrade (UTC+ 02:00)
- Europe/Bratislava (UTC+ 02:00)
- Arctic/Longyearbyen (UTC+ 02:00)
- Égypte (UTC+ 02:00)
- Europe/Vatican (UTC+ 02:00)
- Europe/Monaco (UTC+ 02:00)
- Europe/Londres (UTC+ 01:00)
- Etc/GMT-1 (UTC+ 01:00)
- Europe/Jersey (UTC+ 01:00)
- Europe/Guernesey (UTC+ 01:00)
- Europe/Isle_of_Man (UTC+ 01:00)
- Afrique/Tunis (UTC+ 01:00)
- Afrique/Malabo (UTC+ 01:00)
- GB-Eire (UTC+ 01:00)

- Afrique/Lagos (UTC+ 01:00)
- Afrique/Alger (UTC+ 01:00)
- GB (UTC+ 01:00)
- Portugal (UTC+ 01:00)
- Afrique/Sao_Tome (UTC+ 01:00)
- Afrique/Ndjamena (UTC+ 01:00)
- Atlantique/Féroé (UTC+ 01:00)
- Irlande (UTC+ 01:00)
- Atlantique/Féroé (UTC+ 01:00)
- Europe/Dublin (UTC+ 01:00)
- Afrique/Libreville (UTC+ 01:00)
- Afrique/El_Aaiun (UTC+ 01:00)
- Afrique/El_Aaiun (UTC+ 01:00)
- Afrique/Douala (UTC+ 01:00)
- Afrique/Brazzaville (UTC+ 01:00)
- Afrique/Porto-Novo (UTC+ 01:00)
- Atlantique/Madère (UTC+ 01:00)
- Europe/Lisbonne (UTC+ 01:00)
- Atlantique/Canaries (UTC+ 01:00)
- Afrique/Casablanca (UTC+ 01:00)
- Europe/Belfast (UTC+ 01:00)
- Afrique/Luanda (UTC+ 01:00)
- Afrique/Kinshasa (UTC+ 01:00)
- Afrique/Bangui (UTC+ 01:00)
- HUMIDE (UTC+ 01:00)
- Afrique/Niamey (UTC+ 01:00)
- GMT (UTC+ 00:00)
- Etc/GMT-0 (UTC+ 00:00)
- Atlantic/Sainte-Hélène (UTC+ 00:00)

- Etc/GMT+0 (UTC+ 00:00)
- Afrique/Banjul (UTC+ 00:00)
- Etc/GMT (UTC+ 00:00)
- Afrique/Freetown (UTC+ 00:00)
- Afrique/Bamako (UTC+ 00:00)
- Afrique/Conakry (UTC+ 00:00)
- Universel (UTC+ 00:00)
- Afrique/Nouakchott (UTC+ 00:00)
- UTC (UTC+ 00:00)
- Etc/Universal (UTC+ 00:00)
- Atlantique/Açores (UTC+ 00:00)
- Afrique/Abidjan (UTC+ 00:00)
- Afrique/Accra (UTC+ 00:00)
- Etc/UCT (UTC+ 00:00)
- GMT0 (UTC+ 00:00)
- Zoulou (UTC+ 00:00) Zoulou (UTC+ 00:00)
- Afrique/Ouagadougou (UTC+ 00:00)
- Atlantique/Reykjavik (UTC+ 00:00)
- Etc/Zoulou (UTC+ 00:00)
- Islande (UTC+ 00:00)
- Afrique/Lomé (UTC+ 00:00)
- Greenwich (UTC+ 00:00)
- Etc/GMT0 (UTC+ 00:00)
- America/Danmarkshavn (UTC+ 00:00)
- Afrique/Dakar (UTC+ 00:00)
- Afrique/Bissau (UTC+ 00:00)
- Etc/Greenwich (UTC+ 00:00)
- Afrique/Tombouctou (UTC+ 00:00)
- UTC (UTC+ 00:00)

- Afrique/Monrovia (UTC+ 00:00)
- Etc/UTC (UTC+ 00:00)

Tutoriels d'expression de formules

Vous pouvez suivre ces didacticiels pour utiliser des expressions de formule dans AWS IoT SiteWise.

Rubriques

- Utilisation de chaînes dans les formules
- Filtrer les points de données
- Comptage des points de données correspondant à une condition
- Données tardives dans les formules
- Qualité des données dans les formules
- Valeurs non définies, infinies et en dépassement

Utilisation de chaînes dans les formules

Vous pouvez opérer sur des chaînes dans vos expressions de formule. Vous pouvez également saisir des chaînes à partir de variables qui font référence à des propriétés d'attribut et de mesure.

> **Important**
>
> Les expressions de formule ne peuvent générer que des valeurs doubles ou des valeurs de chaîne. Les expressions imbriquées peuvent générer d'autres types de données, tels que des chaînes, mais la formule dans son ensemble doit être évaluée à un nombre ou à une chaîne. Vous pouvez utiliser la fonction jp pour convertir une chaîne en nombre. La valeur booléenne doit être 1 (vrai) ou 0 (faux). Pour plus d'informations, consultez Valeurs non définies, infinies et en dépassement.

AWS IoT SiteWise fournit les fonctionnalités d'expression de formule suivantes que vous pouvez utiliser pour agir sur des chaînes :

- Littéraux de chaîne
- L'opérateur d'index (`s[index]`)

- L'opérateur de tranche (`s[start:end:step]`)
- Fonctions de comparaison, que vous pouvez utiliser pour comparer des chaînes par ordre lexicographique
- Fonctions de chaîne, qui incluent la `jp` fonction capable d'analyser des objets JSON sérialisés et de convertir des chaînes en nombres

Filtrer les points de données

Vous pouvez utiliser la fonction if pour filtrer les points de données qui ne répondent pas à une condition. La `if` fonction évalue une condition et renvoie des valeurs `true` et des `false` résultats différents. Vous pouvez utiliser la constante none comme sortie pour un cas de `if` fonction afin de supprimer le point de données correspondant à ce cas.

Pour filtrer les points de données qui correspondent à une condition

- Créez une transformation qui utilise la `if` fonction pour définir une condition qui vérifie si une condition est remplie et renvoie none la `result_if_false` valeur `result_if_true` ou.

Example Exemple : filtrer les points de données où l'eau ne bout pas

Imaginons un scénario dans lequel vous avez une mesure qui fournit la température (en degrés Celsius) de l'eau dans une machine. `temp_c` Vous pouvez définir la transformation suivante pour filtrer les points de données où l'eau n'est pas en ébullition :

- Transformation : `boiling_temps = if(gte(temp_c, 100), temp_c, none)` — Renvoie la température si elle est supérieure ou égale à 100 degrés Celsius, sinon elle ne renvoie aucun point de données.

Comptage des points de données correspondant à une condition

Vous pouvez utiliser les fonctions de comparaison et sum () pour compter le nombre de points de données pour lesquels une condition est vraie.

Pour compter les points de données qui correspondent à une condition

1. Créez une transformation qui utilise une fonction de comparaison pour définir une condition de filtre sur une autre propriété.
2. Créez une métrique qui additionne les points de données lorsque cette condition est remplie.

Example Exemple : Compter le nombre de points de données où l'eau bout

Imaginons un scénario dans lequel vous avez une mesure qui fournit la température (en degrés Celsius) de l'eau dans une machine. `temp_c` Vous pouvez définir les propriétés de transformation et de métrique suivantes pour compter le nombre de points de données où l'eau bout :

- Transformation : `is_boiling = gte(temp_c, 100)` — Renvoie 1 si la température est supérieure ou égale à 100 degrés Celsius, sinon elle renvoie la valeur`0`.
- Métrique : `boiling_count = sum(is_boiling)` — Renvoie le nombre de points de données où l'eau est en ébullition.

Données tardives dans les formules

AWS IoT SiteWise prend en charge l'ingestion tardive de données datant de moins de 7 jours. Lorsqu'il AWS IoT SiteWise reçoit des données tardives, il recalcule les valeurs existantes pour toute métrique qui saisit les données tardives dans une fenêtre précédente. Ces nouveaux calculs entraînent des frais de traitement des données.

> **Note**
>
> Lorsqu'il AWS IoT SiteWise calcule des propriétés qui entrent des données tardives, il utilise l'expression de formule actuelle de chaque propriété.

Après avoir AWS IoT SiteWise recalculé une fenêtre passée pour une métrique, elle remplace la valeur précédente pour cette fenêtre. Si vous avez activé les notifications pour cette métrique, émet AWS IoT SiteWise également une notification de valeur de propriété. Cela signifie que vous pouvez recevoir une nouvelle notification de mise à jour de valeur de propriété pour la même propriété et le même horodatage que ceux pour lesquels vous avez déjà reçu une notification. Si vos applications ou lacs de données utilisent des notifications de valeur de propriété, vous devez mettre à jour la valeur précédente avec la nouvelle valeur afin que leurs données soient exactes.

Qualité des données dans les formules

Dans AWS IoT SiteWise, chaque point de données possède un code de qualité, qui peut être l'un des suivants :

- `GOOD`— Les données ne sont affectées par aucun problème.

- `BAD`— Les données sont affectées par un problème tel qu'une défaillance du capteur.
- `UNCERTAIN`— Les données sont affectées par un problème tel que l'imprécision du capteur.

AWS IoT SiteWise ne consomme que des données `GOOD` de qualité lorsqu'il calcule les transformations et les métriques. AWS IoT SiteWise ne produit que des données `GOOD` de qualité pour des calculs réussis. Si un calcul échoue, aucun point de données AWS IoT SiteWise n'est généré pour ce calcul. Cela peut se produire si un calcul aboutit à une valeur non définie, infinie ou en dépassement.

Pour de plus amples informations sur l'interrogation des données et les filtres par qualité de données, veuillez consulter Interrogez les données de AWS IoT SiteWise.

Valeurs non définies, infinies et en dépassement

Certaines expressions de formule (telles que `x / 0`ou`sqrt(-1)`, ou`log(0)`) calculent des valeurs non définies dans un système de nombres réels, infinies ou situées en dehors de la plage prise en charge par AWS IoT SiteWise. Lorsque l'expression d'une propriété d'actif calcule une valeur indéfinie, infinie ou de dépassement, AWS IoT SiteWise elle ne produit aucun point de données pour ce calcul.

AWS IoT SiteWise ne produit pas non plus de point de données s'il calcule une valeur non numérique à la suite d'une expression de formule. Cela signifie que si vous définissez une formule qui calcule une chaîne, un tableau ou la constante none, elle AWS IoT SiteWise ne produit aucun point de données pour ce calcul.

Example Exemples

Chacune des expressions de formule suivantes génère une valeur qui ne AWS IoT SiteWise peut pas être représentée sous forme de nombre. AWS IoT SiteWise ne produit pas de point de données lorsqu'il calcule ces expressions de formule.

- `x / 0`n'est pas défini.
- `log(0)`n'est pas défini.
- `sqrt(-1)`n'est pas défini dans un système de nombres réels.
- `"hello" + " world"`est une chaîne.
- `jp('{"values":[3,6,7]}', '$.values')`est un tableau.
- `if(gte(temp, 300), temp, none)`c'est none quand `temp` est inférieur à`300`.

Création de modèles composites personnalisés (composants)

Les modèles composites personnalisés, ou composants si vous utilisez la console, fournissent un autre niveau d'organisation pour vos modèles d'actifs et vos modèles de composants. Vous pouvez les utiliser pour structurer vos modèles en regroupant les propriétés ou en référençant d'autres modèles. Pour plus d'informations sur l'utilisation de modèles composites personnalisés, consultezModèles composites personnalisés (composants).

Vous créez un modèle composite personnalisé au sein d'un modèle d'actif ou d'un modèle de composant existant. Il existe deux types de modèles composites personnalisés. Pour regrouper les propriétés associées au sein d'un modèle, vous pouvez créer un modèle composite personnalisé en ligne. Pour référencer un modèle de composant dans votre modèle d'actif ou de composant, vous pouvez créer un modèle composite personnalisé basé sur un modèle de composant.

Les sections suivantes décrivent comment utiliser l' AWS IoT SiteWise API pour créer des modèles composites personnalisés.

Rubriques

- Création d'un composant en ligne (console)
- Création d'un modèle composite personnalisé en ligne ()AWS CLI
- Création d'un component-model-based composant (console)
- Création d'un modèle composite component-model-based personnalisé (AWS CLI)

Création d'un composant en ligne (console)

Vous pouvez utiliser la AWS IoT SiteWise console pour créer un composant en ligne qui définit ses propres propriétés.

> **Note**
>
> Comme il s'agit d'un composant intégré, ces propriétés ne s'appliquent qu'au modèle d'actif actuel et ne sont partagées nulle part ailleurs.
> Si vous devez produire un modèle réutilisable (par exemple, pour le partager entre plusieurs modèles d'actifs ou pour inclure plusieurs instances au sein d'un même modèle d'actif), vous devez plutôt créer un composant basé sur un modèle de composant. Consultez la section suivante pour plus de détails.

Pour créer un composant (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Models (Modèles).
3. Choisissez le modèle d'actif auquel vous souhaitez ajouter un composant.
4. Dans l'onglet Propriétés, sélectionnez Composants.
5. Choisissez Créer un composant.
6. Sur la page Créer un composant, procédez comme suit :

    a. Entrez un nom pour le composant, tel que **`ServoMotor`** ou**`ServoMotor Model`**. Ce nom doit être unique pour tous les composants de votre compte dans cette région.

    b. (Facultatif) Ajoutez des définitions d'attributs pour le modèle. Les attributs représentent des informations qui changent rarement. Pour plus d'informations, consultez Définition de données statiques (attributs).

    c. (Facultatif) Ajoutez des définitions de mesures pour le modèle. Les mesures représentent des flux de données provenant de votre équipement. Pour plus d'informations, consultez Définition des flux de données provenant des équipements (mesures).

    d. (Facultatif) Ajoutez des définitions de transformations pour le modèle. Les transformations sont des formules qui font correspondre les données d'un formulaire à un autre. Pour plus d'informations, consultez Transformation des données (transformations).

    e. (Facultatif) Ajoutez des définitions de métriques pour le modèle. Les métriques sont des formules qui regroupent les données sur des intervalles de temps. Les métriques peuvent saisir des données provenant des actifs associés, afin que vous puissiez calculer des valeurs représentant votre activité ou un sous-ensemble de celle-ci. Pour plus d'informations, consultez Agrégation de données provenant de propriétés et d'autres actifs (métriques).

    f. Choisissez Créer un composant.

Création d'un modèle composite personnalisé en ligne ()AWS CLI

Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour créer un modèle composite personnalisé en ligne qui définit ses propres propriétés.

Utilisez l'opération CreateAssetModelCompositeModel pour créer un modèle en ligne avec des propriétés. Cette opération attend une charge utile avec la structure suivante.

> **Note**
>
> Comme il s'agit d'un modèle composite en ligne, ces propriétés ne s'appliquent qu'au modèle d'actif actuel et ne sont partagées nulle part ailleurs. Ce qui le rend « intégré », c'est qu'il ne fournit pas de valeur pour le `composedAssetModelId` champ.
> Si vous devez produire un modèle réutilisable (par exemple, pour le partager entre plusieurs modèles d'actifs ou pour inclure plusieurs instances au sein d'un même modèle d'actif), vous devez plutôt créer un modèle composite basé sur un modèle de composants. Consultez la section suivante pour plus de détails.

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

Création d'un component-model-based composant (console)

Vous pouvez utiliser la AWS IoT SiteWise console pour créer un composant à partir d'un modèle de composant.

Pour créer un component-model-based composant (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Models (Modèles).
3. Choisissez le modèle d'actif auquel vous souhaitez ajouter un composant.
4. Dans l'onglet Propriétés, sélectionnez Composants.
5. Choisissez Créer un composant.
6. Sur la page Créer un composant, procédez comme suit :

    a. Sélectionnez le modèle de composant sur lequel vous souhaitez baser le composant.

    b. Entrez un nom pour le composant, tel que **`ServoMotor`** ou**`ServoMotor Model`**. Ce nom doit être unique pour tous les composants de votre compte dans cette région.

    c. Choisissez Créer un composant.

Création d'un modèle composite component-model-based personnalisé (AWS CLI)

Vous pouvez utiliser le AWS CLI pour créer un modèle composite component-model-based personnalisé au sein de votre modèle d'actif. Un modèle composite component-model-based personnalisé est une référence à un modèle de composant que vous avez déjà défini ailleurs.

Utilisez l'opération CreateAssetModelCompositeModel pour créer un modèle composite component-model-based personnalisé. Cette opération attend une charge utile avec la structure suivante.

> **Note**
>
> Dans cet exemple, la valeur de `composedAssetModelId` est l'ID du modèle d'actif ou l'ID externe d'un modèle de composant existant. Pour plus d'informations, consultez Référencement d'objets avec des identifiants externes dans le Guide de l'utilisateur AWS IoT SiteWise . Pour un exemple de création d'un modèle de composant, consultezCréation d'un modèle de composant (AWS CLI).

```
{
    "assetModelCompositeModelName": "CNCLathe_ServoMotorA",
    "assetModelCompositeModelType": "CUSTOM",
    "composedAssetModelId": component model ID
]
```

Comme il ne s'agit que d'une référence, un modèle composite component-model-based personnalisé ne possède aucune propriété propre, à part un nom.

Si vous souhaitez ajouter plusieurs instances du même composant à votre modèle d'actif (par exemple, une machine CNC dotée de plusieurs servomoteurs), vous pouvez ajouter plusieurs modèles composites component-model-based personnalisés portant chacun leur propre nom mais faisant tous référence au même`composedAssetModelId`.

Vous pouvez imbriquer des composants dans d'autres composants. Pour ce faire, vous pouvez ajouter un modèle component-model-based composite, comme indiqué dans cet exemple, à l'un de vos modèles de composants.

Création de ressources

Vous pouvez créer une ressource à partir d'un modèle de ressource. Vous devez disposer d'un modèle de ressource avant de pouvoir créer une ressource. Si vous n'avez pas encore créé de modèle de ressource, veuillez consulter Création de modèles de ressources.

> **Note**
>
> Vous pouvez uniquement créer des ressources à partir de modèles `ACTIVE`. Si l'état de votre modèle n'est pas `ACTIVE`, vous devrez peut-être attendre quelques minutes avant de pouvoir créer des ressources à partir de ce modèle. Pour plus d'informations, consultez État des ressources et des modèles.

Rubriques

- Création d'une ressource (console)
- Création d'un actif (AWS CLI)
- Configuration d'une nouvelle ressource

Création d'une ressource (console)

Vous pouvez utiliser la AWS IoT SiteWise console pour créer un actif.

Pour créer une ressource (console)

1. Accédez à la console AWS IoT SiteWise.

2. Dans le panneau de navigation, choisissez Ressources.
3. Choisissez Create asset (Créer une ressource).
4. Sur la page Créer une ressource, procédez comme suit :

   a. Pour Modèle, choisissez le modèle de ressource à partir duquel créer une ressource.

   > **Note**
   >
   > Si votre modèle n'est pas ACTIF, vous devez attendre qu'il soit actif ou résoudre des problèmes s'il indique ÉCHEC.

   b. Saisissez un nom pour votre ressource.

   c. (Facultatif) Ajoutez des balises pour votre ressource. Pour plus d'informations, consultez Marquer vos ressources AWS IoT SiteWise.

   d. Choisissez Create asset (Créer une ressource).

   Lorsque vous créez un actif, la AWS IoT SiteWise console accède à la page du nouvel actif. Sur cette page, vous pouvez voir l'état de la ressource, qui est initialement CRÉATION. Cette page est automatiquement mise à jour, de sorte que vous pouvez attendre la mise à jour de l'état de la ressource.

   > **Note**
   >
   > Le processus de création des ressources peut prendre jusqu'à une minute. Une fois que le statut est ACTIF, vous pouvez effectuer des opérations de mise à jour sur votre actif. Pour plus d'informations, consultez État des ressources et des modèles.

Après avoir créé une ressource, veuillez consulter Configuration d'une nouvelle ressource.

Création d'un actif (AWS CLI)

Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour créer un actif à partir d'un modèle d'actif.

Vous devez avoir un `assetModelId` pour créer une ressource. Si vous avez créé un modèle d'actif, mais que vous ne le connaissez pas`assetModelId`, utilisez l'API ListAssetModels pour afficher tous vos modèles d'actifs.

Pour créer un actif à partir d'un modèle d'actif, utilisez l'CreateAssetAPI avec les paramètres suivants :

- `assetName`— Le nom du nouvel actif. Donnez un nom à votre actif pour vous aider à l'identifier.
- `assetModelId`— L'ID de l'actif. Il s'agit de l'identifiant réel au format UUID, ou du `externalId:myExternalId` s'il en possède un. Pour plus d'informations, consultez Référencement d'objets avec des identifiants externes dans le Guide de l'utilisateur AWS IoT SiteWise .

Pour créer un actif (AWS CLI)

- Exécutez la commande suivante pour créer une ressource. Remplacez *`asset-name`* par le nom de l'actif et *`asset-model-id par l'ID`* ou l'ID externe du modèle d'actif.

```
aws iotsitewise create-asset \
  --asset-name asset-name \
  --asset-model-id asset-model-id
```

L'opération renvoie une réponse qui contient les détails de votre nouvelle ressource et son état au format suivant.

```
{
  "assetId": "String",
  "assetArn": "String",
  "assetStatus": {
    "state": "String",
    "error": {
      "code": "String",
      "message": "String"
    }
  }
}
```

L'`state` de la ressource est `CREATING` jusqu'à ce que la ressource soit créée.

> **Note**
>
> Le processus de création des ressources peut prendre jusqu'à une minute. Pour vérifier l'état de votre actif, utilisez l'DescribeAssetopération avec l'ID de votre actif comme

`assetId` paramètre. Une fois que l'actif `state` est en `ACTIVE` place, vous pouvez effectuer des opérations de mise à jour sur celui-ci. Pour plus d'informations, consultez État des ressources et des modèles.

Après avoir créé une ressource, veuillez consulter Configuration d'une nouvelle ressource.

Configuration d'une nouvelle ressource

Terminez la configuration de votre ressource avec l'une des actions facultatives suivantes :

- Mappage des flux de données industrielles avec des propriétés de ressources si votre ressource possède des propriétés de mesure.
- Mise à jour des valeurs d'attribut si la ressource comporte des valeurs d'attribut uniques.
- Association et dissociation de ressources si votre ressource est une ressource parent.

Recherche de ressources

Utilisez la fonctionnalité Console AWS IoT SiteWise de recherche pour trouver des actifs en fonction des métadonnées et des filtres de valeur des propriétés en temps réel.

Prérequis

AWS IoT SiteWise nécessite des autorisations d'intégration AWS IoT TwinMaker afin de mieux organiser et modéliser les données industrielles. Si vous avez accordé des autorisations à AWS IoT SiteWise, utilisez l'ExecuteQueryAPI. Si vous n'avez pas accordé d' AWS IoT SiteWise autorisations et que vous avez besoin d'aide pour démarrer, consultezIntégration d'AWS IoT SiteWise et de AWS IoT TwinMaker.

Recherche avancée sur Console AWS IoT SiteWise

Recherche de métadonnées

1. Accédez à la console AWS IoT SiteWise.
2. Dans le volet de navigation, sélectionnez Recherche avancée sous Ressources.
3. Sous Recherche avancée, choisissez l'option de recherche par métadonnées.

4. Renseignez les paramètres. Renseignez autant de champs que possible pour une recherche efficace.

   a. Nom de la ressource : entrez le nom complet de la ressource ou un nom partiel pour une recherche étendue.

   b. Nom de la propriété : entrez le nom complet de la propriété ou un nom partiel pour une recherche étendue.

   c. Opérateur — Choisissez un opérateur parmi :

      - **=**
      - **<**
      - **>**
      - **<=**
      - **>=**

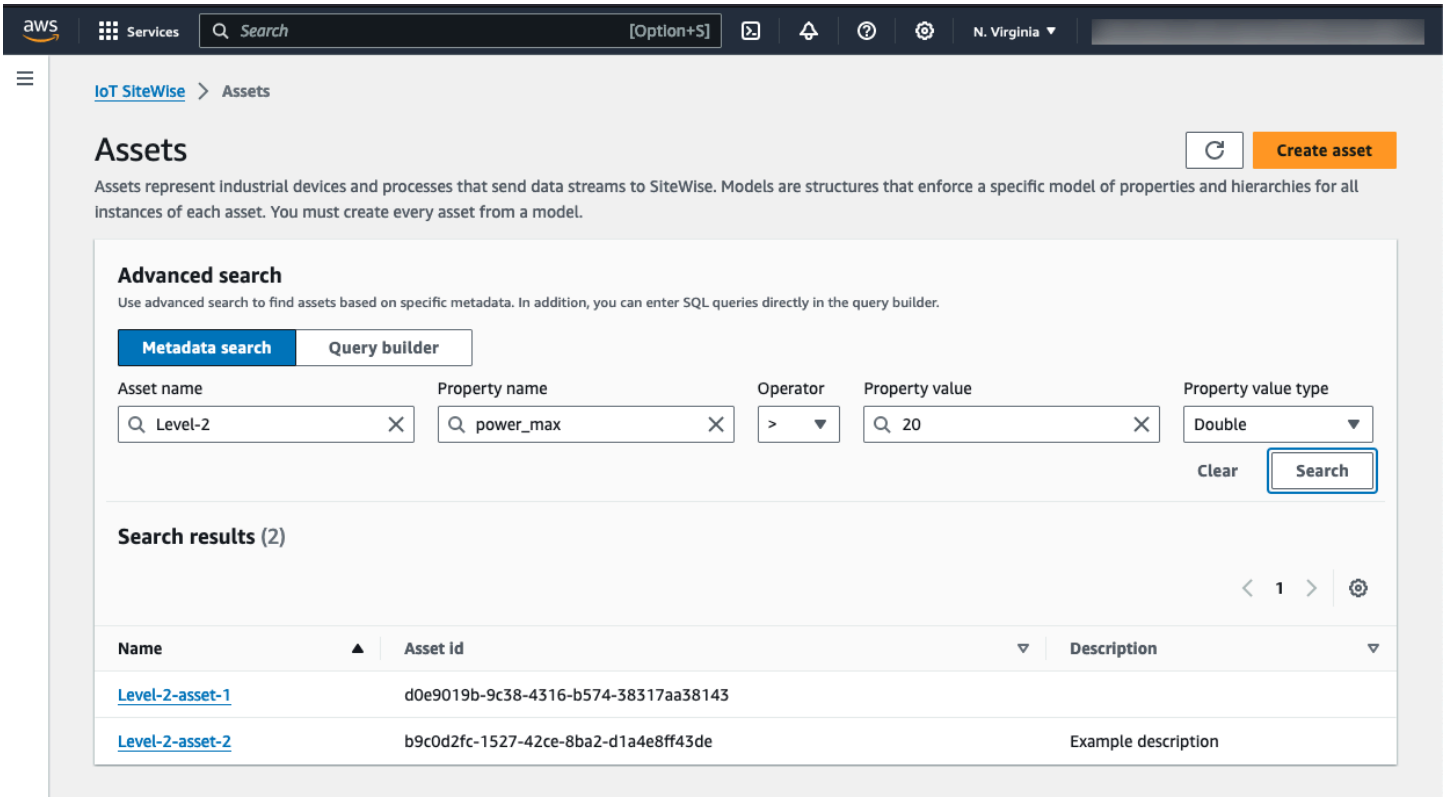
   d. Valeur de la propriété : cette valeur est comparée à la dernière valeur de la propriété.

   e. Type de valeur de propriété : type de données de la propriété. Choisissez parmi les options suivantes :

      - Double
      - Integer
      - String
      - Booléen

5. Choisissez Rechercher.

6. Dans le tableau des résultats de recherche, sélectionnez l'actif dans la colonne Nom. Cela vous amène à la page détaillée de l'actif en question.



Recherche partielle

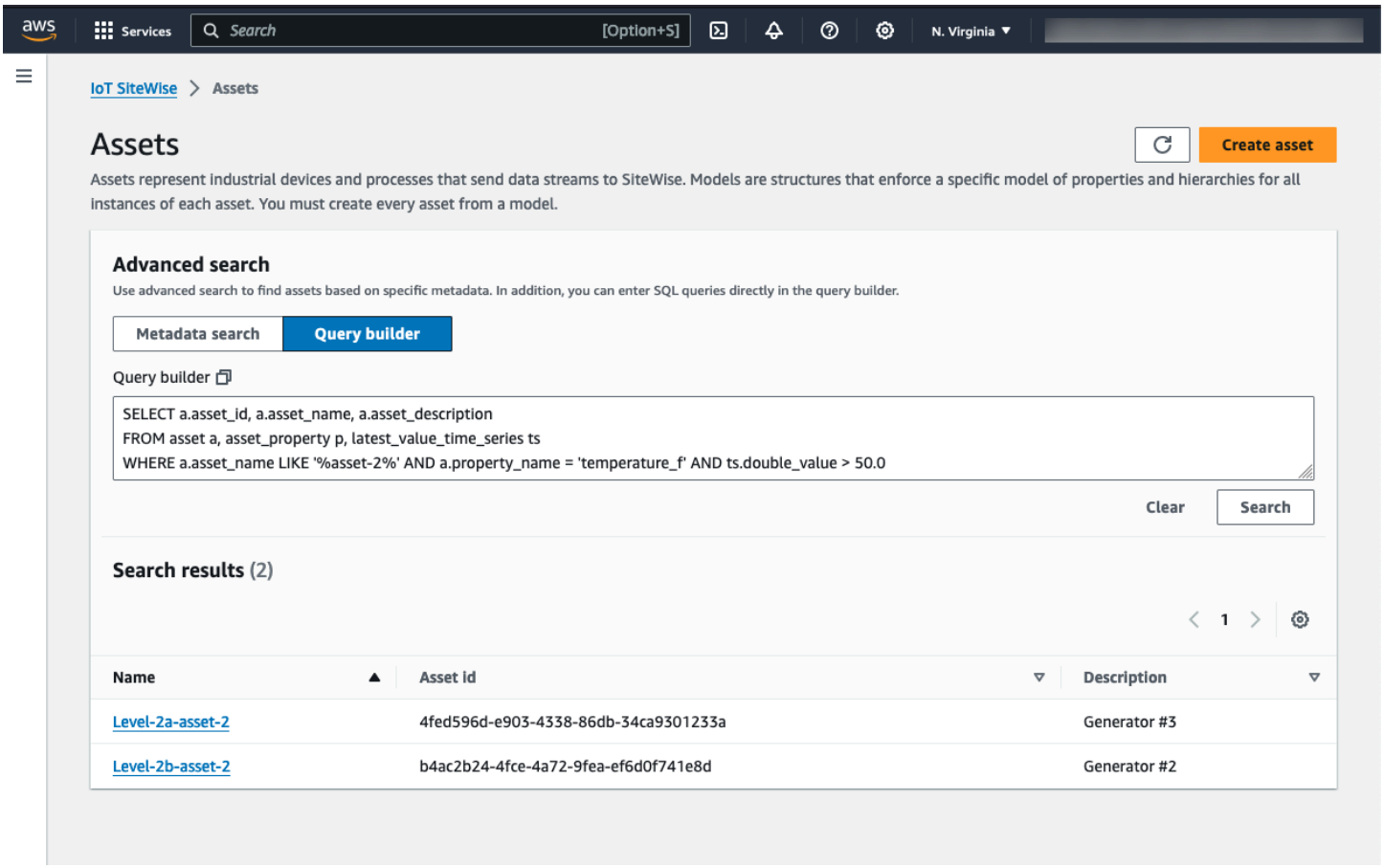
Il n'est pas nécessaire de fournir tous les paramètres pour une recherche de ressources. Voici quelques exemples de recherches partielles à l'aide de l'option de recherche de métadonnées :

- Trouvez les actifs par leur nom :
  - Entrez une valeur uniquement dans le champ Nom de l'actif.
  - Les champs Nom de la propriété et Valeur de la propriété sont vides.
- Trouvez des actifs contenant des propriétés portant un nom spécifique :
  - Entrez une valeur uniquement dans le champ Nom de la propriété.
  - Les champs Nom de l'actif et Valeur de la propriété sont vides.
- Trouvez des actifs en fonction des dernières valeurs de leurs propriétés :
  - Entrez des valeurs dans les champs Nom de la propriété et Valeur de la propriété.
  - Sélectionnez un opérateur et un type de valeur de propriété.

Recherche par générateur de requêtes

1. Accédez à Console AWS IoT SiteWise.

2. Dans le volet de navigation, sélectionnez Recherche avancée sous Ressources.
3. Sous Recherche avancée, choisissez l'option Générateur de requêtes.
4. Dans le volet Générateur de requêtes, écrivez votre requête SQL pour récupérer un `asset_name` `asset_id` et`asset_description`.
5. Choisissez Rechercher.
6. Dans le tableau des résultats de recherche, sélectionnez l'actif dans la colonne Nom. Cela vous amène à la page détaillée de l'actif en question.



Note

- La `SELECT` clause de la requête SQL doit inclure les `asset_id` champs `asset_name` et pour garantir la validité d'un actif dans la table des résultats de recherche.

- Le générateur de requêtes affiche uniquement le nom, l'identifiant de l'actif et la description dans le tableau des résultats. L'ajout de champs supplémentaires à la `SELECT` clause n'ajoute pas de colonnes supplémentaires à la table de résultats

Mappage des flux de données industrielles avec des propriétés de ressources

Vous pouvez définir un alias de propriété sur la propriété de l'actif. Cela vous aide à identifier la propriété d'un actif lorsque vous ingérez ou récupérez des données relatives à un actif. Si votre actif possède des propriétés de mesure, vous pouvez définir des alias de propriété pour mapper vos flux de données à ces propriétés de mesure.

Ce processus nécessite que vous connaissiez l'alias de votre propriété.

- Si vous ingérez des données provenant de serveurs OPC-UA à l'aide d'une source de données OPC-UA dans une passerelle SiteWise Edge, votre alias de propriété est le chemin d'accès à une variable située sous le nœud Objects, en commençant par. `/`

  Example

  Si le chemin d'accès à votre variable est`company/windfarm/3/turbine/7/temperature`, l'alias de votre propriété est`/company/windfarm/3/turbine/7/temperature`.

  Pour plus d'informations sur l'architecture d'informations OPC-UA, consultez la section Modèle d'information et mappage de l'espacement des adresses dans le manuel de référence en ligne OPC UA.

  Remarques

  - Si vous configurez un préfixe de flux de données pour votre source OPC-UA, vous devez inclure ce préfixe dans l'alias de propriété pour tous les flux de données de cette source.

    Example

    S'il s'`/RentonWA`agit d'un préfixe, l'alias précédent est`/RentonWA/company/windfarm/3/turbine/7/temperature`.

- Les alias de propriété peuvent contenir jusqu'à 1 000 octets. Les chemins de variables OPC-UA peuvent contenir jusqu'à 4 096 octets. Actuellement, AWS IoT SiteWise ne prend pas en charge l'ingestion de données à partir de variables OPC-UA avec de longs chemins.

- Si vous ingérez des données provenant de serveurs Modbus à l'aide d'une source de données Modbus TCP dans une passerelle SiteWise Edge, l'alias de votre propriété est le suivant :

  Modbus `register set tag name`

  Utilisez cette valeur pour envoyer les données de cet ensemble de registres vers une propriété d'actif.

- Si vous ingérez des données provenant d'autres sources, par exemple à l'aide de AWS IoT règles ou de l'API, vous devez définir les alias de vos propriétés. Vous pouvez définir un système d'attribution de noms d'alias de propriété applicable à la configuration de votre appareil. Par exemple, si vous ingérez des données à partir d'objets AWS IoT , vous pouvez inclure le nom de l'objet dans les alias de propriété pour identifier de manière unique les flux de données. Pour plus d'informations sur cet exemple, consultez le didacticiel sur l'ingestion de données depuis AWS IoT des objets.

Les alias de propriété doivent être uniques au sein d'une région et d'un AWS compte. AWS IoT SiteWise renvoie une erreur si vous définissez un alias de propriété sur un alias qui existe déjà sur une autre propriété d'actif.

Si plusieurs sources OPC-UA possèdent des chemins de flux de données identiques, ajoutez un préfixe aux chemins de chaque source pour former des alias uniques. Pour plus d'informations, consultez Configuration des sources de données.

> **Note**
>
> Cette section explique comment définir des alias de propriété pour les propriétés de mesure. Pour plus d'informations sur la façon de définir des alias de propriété pour les propriétés d'état des alarmes externes, consultezCartographie des flux d'état d'alarme externes.

Rubriques

- Définition d'un alias de propriété (console)

- Définition d'un alias de propriété (AWS CLI)

Définition d'un alias de propriété (console)

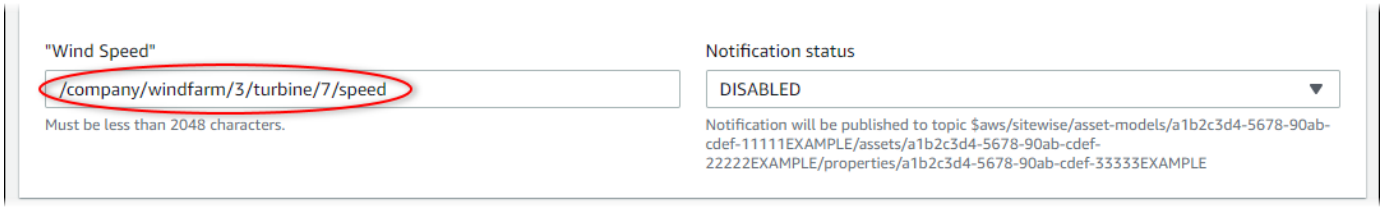
Vous pouvez utiliser la AWS IoT SiteWise console pour définir un alias pour une propriété d'actif.

Pour définir un alias de propriété (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Ressources.
3. Choisissez la ressource pour laquelle vous souhaitez définir un alias de propriété.

> **Tip**
>
> Vous pouvez cliquer sur l'icône en forme de flèche pour développer une hiérarchie de ressources afin de trouver votre ressource.

4. Choisissez Modifier.
5. Recherchez la propriété pour laquelle vous souhaitez définir un alias, puis saisissez l'alias de propriété.



6. Choisissez Enregistrer.

Définition d'un alias de propriété (AWS CLI)

Utilisez le AWS Command Line Interface (AWS CLI) pour définir un alias pour une propriété d'actif.

Vous devez connaître l'`assetId` de votre ressource et le `propertyId`de la propriété pour effectuer cette procédure. Vous pouvez également utiliser l'identifiant externe. Si vous avez créé un actif et que vous ne le connaissez pas`assetId`, utilisez l'ListAssetsAPI pour répertorier tous les actifs d'un modèle spécifique. Utilisez cette DescribeAssetopération pour afficher les propriétés de votre actif, y compris les identifiants de propriété.

Utilisez l'opération UpdateAssetPropriété pour mapper un flux de données à la propriété de votre actif. Spécifiez les paramètres suivants :

- `assetId`— L'identifiant ou l'identifiant externe de l'actif. Pour plus d'informations, consultez Référencement d'objets avec des identifiants externes dans le Guide de l'utilisateur AWS IoT SiteWise .
- `propertyId`— L'ID ou l'ID externe de la propriété de l'actif.
- `propertyAlias`— Le chemin du flux de données vers l'alias de la propriété.
- `propertyNotificationState`— État de notification de la valeur de la propriété : `ENABLED` ou`DISABLED`. Spécifiez l'état de notification existant de la propriété lorsque vous mettez à jour l'alias de propriété. Vous pouvez récupérer l'état de notification existant à l'aide de l'opération DescribeAssetPropriété.

  Si vous omettez ce paramètre, le nouvel état de notification est `DISABLED`. Pour de plus amples informations sur les notifications de propriété, veuillez consulter Interaction avec d'autres AWS services.

Pour définir un alias de propriété (AWS CLI)

1. Exécutez la commande suivante pour récupérer l'état de notification actuel de la propriété. Remplacez *`asset-id`* et *`property-id`* par les ID de la propriété de ressource.

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

   L'opération renvoie une réponse qui contient les informations de propriété de ressource au format suivant. L'état de notification de propriété est dans `assetProperty.notification.state` dans l'objet JSON.

   ```
   {
     "assetId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
     "assetName": "Wind Turbine 7",
     "assetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
     "assetProperty": {
       "id": "a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
       "name": "Wind Speed",
       "notification": {
   ```

```
      "topic": "$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/
assets/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE/properties/a1b2c3d4-5678-90ab-
cdef-33333EXAMPLE",
      "state": "ENABLED"
    },
    "dataType": "DOUBLE",
    "unit": "m/s",
    "type": {
      "measurement": {}
    }
  }
}
```

2. Exécutez la commande suivante pour définir l'alias de la propriété de ressource. Remplacez *property-alias* par l'alias de propriété et *notification-state* par l'état de notification, ou omettez `--property-notification-state` pour désactiver les notifications. Vous pouvez éventuellement mettre à jour l'unité de l'actif avec une nouvelle *unité* et`--property-unit`.

```
aws iotsitewise update-asset-property \
  --asset-id asset-id \
  --property-id property-id \
  --property-alias property-alias \
  --property-notification-state notification-state \
  --property-unit unit
```

3. Pour vérifier que l'alias a été défini, exécutez la commande suivante pour récupérer les détails de la propriété. Remplacez *asset-id* et *property-id* par les ID de la propriété de ressource.

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

L'opération renvoie une réponse qui contient les informations de propriété de ressource au format suivant. L'alias de propriété se trouve `assetProperty.alias` dans l'objet JSON et est défini sur `myAlias` dans cet exemple.

```
{
  "assetId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
  "assetName": "Wind Turbine 7",
  "assetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
  "assetProperty": {
```

```
    "alias": "myAlias",
    "id": "a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
    "name": "Wind Speed",
    "notification": {
      "topic": "$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/
assets/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE/properties/a1b2c3d4-5678-90ab-
cdef-33333EXAMPLE",
      "state": "ENABLED"
    },
    "dataType": "DOUBLE",
    "unit": "m/s",
    "type": {
      "measurement": {}
    }
  }
}
```

Mise à jour des valeurs d'attribut

Les ressources héritent des attributs de leur modèle de ressource, y compris la valeur par défaut de l'attribut. Dans certains cas, il vaudra mieux conserver l'attribut par défaut du modèle de ressource, par exemple pour une propriété de fabricant de ressource. Dans d'autres cas, il vaudra mieux actualiser l'attribut hérité, par exemple pour la latitude et la longitude spécifiques d'une ressource.

Updating an attribute value (console)

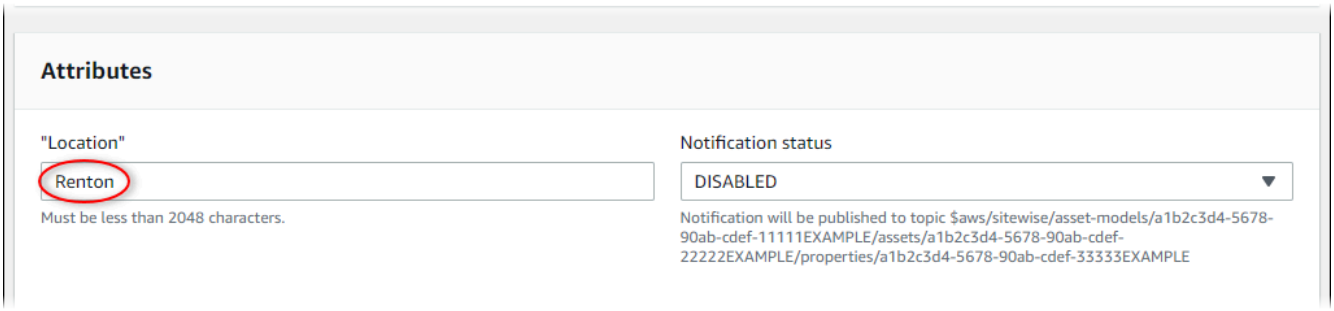
Vous pouvez utiliser la AWS IoT SiteWise console pour mettre à jour la valeur d'une propriété d'actif attributaire.

Pour mettre à jour la valeur d'un attribut (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Ressources.
3. Choisissez la ressource pour laquelle vous souhaitez mettre à jour un attribut.

> **Tip**
>
> Vous pouvez cliquer sur l'icône en forme de flèche pour développer une hiérarchie de ressources afin de trouver votre ressource.

4. Choisissez Modifier.
5. Recherchez l'attribut à mettre à jour, puis saisissez sa nouvelle valeur.



6. Choisissez Enregistrer.

Updating an attribute value (AWS CLI)

Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour mettre à jour la valeur d'un attribut.

Vous devez connaître l'`assetId` de votre ressource et le `propertyId`de la propriété pour effectuer cette procédure. Vous pouvez également utiliser l'identifiant externe. Si vous avez créé un actif et que vous ne le connaissez pas`assetId`, utilisez l'ListAssetsAPI pour répertorier tous les actifs d'un modèle spécifique. Utilisez cette DescribeAssetopération pour afficher les propriétés de votre actif, y compris les identifiants de propriété.

Utilisez l'opération BatchPutAssetPropertyValue pour attribuer des valeurs d'attribut à votre actif. Vous pouvez utiliser cette opération pour définir plusieurs attributs à la fois. La charge utile de cette opération contient une liste d'entrées, chacune contenant l'ID de ressource, l'ID de propriété et la valeur d'attribut.

Pour mettre à jour la valeur d'un attribut (AWS CLI)

1. Créez un fichier nommé `batch-put-payload.json` et copiez l'objet JSON suivant dans le fichier. Cet exemple de charge utile montre comment définir la latitude et la longitude d'une éolienne. Mettez à jour les ID, les valeurs et les horodatages pour modifier la charge utile de votre cas d'utilisation.

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

- Chaque entrée de la charge utile contient un `entryId` que vous pouvez définir sous la forme d'une chaîne unique. Si des entrées de demande échouent, chaque erreur contiendra l'`entryId` de la demande correspondante afin que vous sachiez quelles demandes réessayer.
- Pour définir une valeur d'attribut, vous pouvez inclure une structure timestamp-quality-value (TQV) dans la liste de chaque propriété `propertyValues` d'attribut. Cette structure doit contenir le nouveau `value` et le `timestamp` actuel.
  - `value`— Structure contenant l'un des champs suivants, selon le type de propriété définie :
    - `booleanValue`

- `doubleValue`
- `integerValue`
- `stringValue`

- `timestamp`— Une structure qui contient l'heure actuelle d'Unix en secondes,. `timeInSeconds` AWS IoT SiteWise rejette tous les points de données dont l'horodatage existait depuis plus de 7 jours ou moins de 5 minutes dans le futur.

Pour plus d'informations sur la préparation d'une charge utile pour BatchPutAssetPropertyValue, consultezIngestion de données à l'aide de l'API AWS IoT SiteWise.

2. Exécutez la commande suivante pour envoyer les valeurs d'attribut à AWS IoT SiteWise :

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

Association et dissociation de ressources

Si le modèle de votre ressource définit des hiérarchies de modèles de ressources enfants, vous pouvez associer des ressources enfants à votre ressource. Les ressources parents peuvent accéder aux données des ressources associées et les agréger. Pour de plus amples informations sur les modèles de ressources hiérarchiques, veuillez consulter Définition de hiérarchies de modèles d'actifs.

Rubriques

- Association et dissociation de ressources (console)
- Associer et dissocier des actifs ()AWS CLI

Association et dissociation de ressources (console)

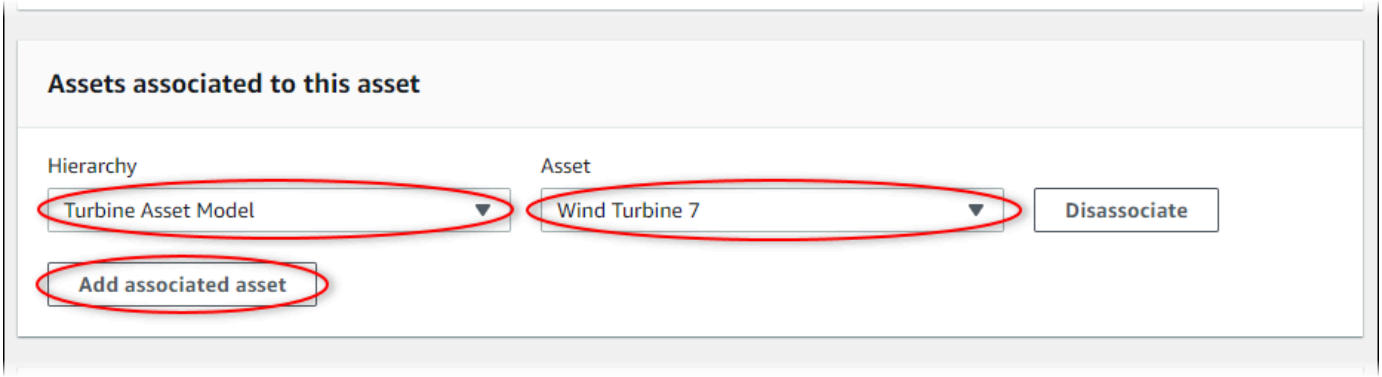
Vous pouvez utiliser la AWS IoT SiteWise console pour associer et dissocier des actifs.

Pour associer une ressource (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Ressources.
3. Choisissez la ressource parent à laquelle vous souhaitez associer une ressource enfant.

> **Tip**
>
> Vous pouvez cliquer sur l'icône en forme de flèche pour développer une hiérarchie de ressources afin de trouver votre ressource.

4. Choisissez Modifier.
5. Dans Ressources associées à cette ressource, choisissez Ajouter une ressource associée.



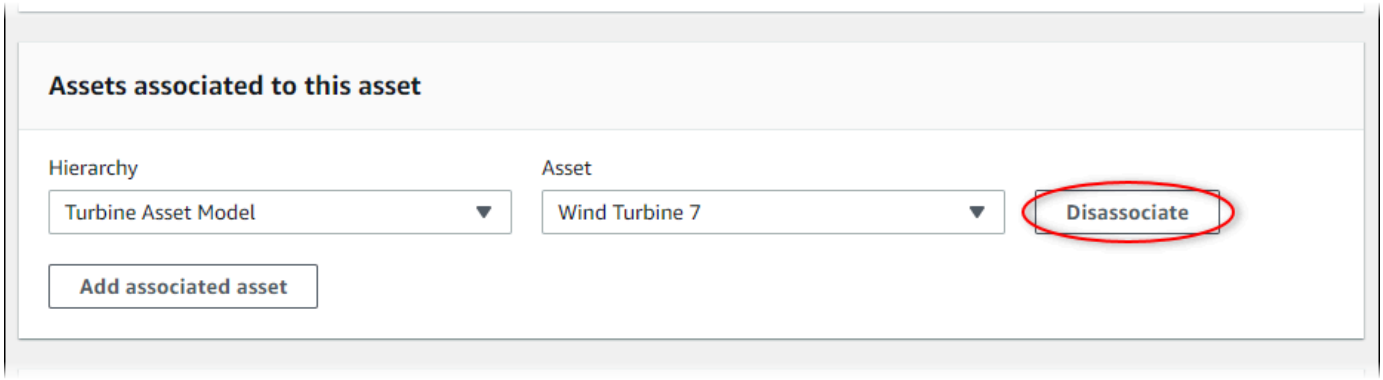
6. Pour Hiérarchie, choisissez la hiérarchie qui définit la relation entre la ressource parent et la ressource enfant.
7. Pour Ressource, choisissez la ressource enfant à associer.
8. Choisissez Enregistrer.

Pour dissocier une ressource (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Ressources.
3. Choisissez la ressource parent pour laquelle vous souhaitez dissocier une ressource enfant.

> **Tip**
>
> Vous pouvez cliquer sur l'icône en forme de flèche pour développer une hiérarchie de ressources afin de trouver votre ressource.

4. Choisissez Modifier.
5. Dans Ressources associées à cette ressource, choisissez Dissocier pour la ressource.



6. Choisissez Enregistrer.

Associer et dissocier des actifs ()AWS CLI

Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour associer et dissocier des actifs.

Pour cette procédure, vous devez connaître l'ID de la hiérarchie (`hierarchyId`) dans le modèle de ressource parent qui définit la relation avec le modèle de ressource enfant. Utilisez l'DescribeAssetopération pour trouver l'ID de hiérarchie dans la réponse.

Pour rechercher un ID de hiérarchie

- Exécutez la commande suivante pour décrire la ressource parent. Remplacez *`parent-asset-id par l'ID`* de la ressource parent ou par l'ID externe.

  ```
  aws iotsitewise describe-asset --asset-id parent-asset-id
  ```

  L'opération renvoie une réponse qui contient les détails de la ressource. La réponse contient une `assetHierarchies` liste dont la structure est la suivante :

  ```
  {
    ...
    "assetHierarchies": [
      {
        "id": "String",
        "name": "String"
      }
    ],
    ...
  ```

```
}
```

L'ID de hiérarchie est la valeur `id` d'une hiérarchie dans la liste des hiérarchies de ressources.

Une fois que vous avez l'ID de hiérarchie, vous pouvez associer ou dissocier une ressource à/de cette hiérarchie.

Pour associer un actif enfant à un actif parent, utilisez l'AssociateAssetsopération. Pour dissocier un actif enfant d'un actif parent, utilisez l'DisassociateAssetsopération. Spécifiez les paramètres suivants, qui sont les mêmes pour les deux opérations :

- `assetId`— L'ID de l'actif parent ou l'ID externe.
- `hierarchyId`— L'ID de hiérarchie ou l'ID externe de la ressource parent.
- `childAssetId`— L'identifiant ou l'identifiant externe de l'actif enfant.

Pour associer un actif (AWS CLI)

- Exécutez la commande suivante pour associer une ressource enfant à une ressource parent. *Remplacez parent-asset-id, hierarchy-id et child-asset-id par les identifiants respectifs :*

```
aws iotsitewise associate-assets \
  --asset-id parent-asset-id \
  --hierarchy-id hierarchy-id \
  --child-asset-id child-asset-id
```

Pour dissocier un actif ()AWS CLI

- Exécutez la commande suivante pour dissocier une ressource enfant d'une ressource parent. *Remplacez parent-asset-id, hierarchy-id et child-asset-id par les identifiants respectifs :*

```
aws iotsitewise disassociate-assets \
  --asset-id parent-asset-id \
  --hierarchy-id hierarchy-id \
  --child-asset-id child-asset-id
```

Mise à jour des ressources et des modèles

Vous pouvez mettre à jour vos actifs, modèles d'actifs et modèles de composants AWS IoT SiteWise pour modifier leurs noms et leurs définitions. Ces opérations de mise à jour sont asynchrones et leur propagation prend du temps. AWS IoT SiteWise Vérifiez l'état de l'actif ou du modèle avant d'apporter des modifications supplémentaires. Vous devez attendre que les modifications soient propagées avant de continuer à utiliser la ressource ou le modèle mis à jour.

Rubriques

- Mise à jour de ressources
- Mise à jour des modèles d'actifs et des modèles de composants
- Mise à jour de modèles composites personnalisés (composants)

Mise à jour de ressources

Vous pouvez utiliser la AWS IoT SiteWise console ou l'API pour mettre à jour le nom d'un actif.

Lorsque vous mettez à jour une ressource, son statut est maintenu `UPDATING` jusqu'à ce que les modifications se propagent. Pour plus d'informations, consultez État des ressources et des modèles.

Rubriques

- Mise à jour d'une ressource (console)
- Mettre à jour un actif (AWS CLI)

Mise à jour d'une ressource (console)

Vous pouvez utiliser la AWS IoT SiteWise console pour mettre à jour les détails des actifs.

Pour mettre à jour une ressource (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Ressources.
3. Choisissez la ressource à mettre à jour.

> **Tip**
>
> Vous pouvez cliquer sur l'icône en forme de flèche pour développer une hiérarchie de ressources afin de trouver votre ressource.

4. Choisissez Modifier.
5. Mettez à jour le nomde la ressource.
6. (Facultatif) Sur cette page, mettez à jour les autres informations relatives à la ressource. Pour plus d'informations, consultez les ressources suivantes :
   - Mappage des flux de données industrielles avec des propriétés de ressources
   - Mise à jour des valeurs d'attribut
   - Interaction avec d'autres AWS services
7. Choisissez Enregistrer.

Mettre à jour un actif (AWS CLI)

Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour mettre à jour le nom d'un actif.

Utilisez cette UpdateAssetopération pour mettre à jour un actif. Spécifiez les paramètres suivants :

- `assetId`— L'ID de l'actif. Il s'agit de l'identifiant réel au format UUID, ou du `externalId:myExternalId` s'il en possède un. Pour plus d'informations, consultez Référencement d'objets avec des identifiants externes dans le Guide de l'utilisateur AWS IoT SiteWise .
- `assetName`— Le nouveau nom de l'actif.

Pour mettre à jour le nom d'un actif (AWS CLI)

- Exécutez la commande suivante pour mettre à jour le nom d'une ressource. Remplacez *`asset-id`* par l'ID ou l'ID externe de l'actif. Mettez à jour le *`nom de l'actif`* avec le nouveau nom de l'actif.

```
aws iotsitewise update-asset \
  --asset-id asset-id \
  --asset-name asset-name
```

Mise à jour des modèles d'actifs et des modèles de composants

Vous pouvez utiliser la AWS IoT SiteWise console ou l'API pour mettre à jour un modèle d'actif ou un modèle de composant.

Vous ne pouvez pas modifier le type ou le type de données d'une propriété existante, ni la fenêtre d'une métrique existante. Vous ne pouvez pas non plus modifier le type du modèle d'actif en modèle de composant, ou inversement.

> **Important**
>
> - Si vous supprimez une propriété d'un modèle de ressource ou d'un modèle de composant, toutes les AWS IoT SiteWise données précédentes relatives à cette propriété sont supprimées. Pour les modèles de composants, cela concerne tous les modèles d'actifs utilisant ce modèle de composant. Veillez donc particulièrement à comprendre dans quelle mesure votre modification peut s'appliquer.
> - Si vous supprimez une définition de hiérarchie d'un modèle d'actifs, AWS IoT SiteWise dissociez tous les actifs de cette hiérarchie.

Lorsque vous mettez à jour un modèle de ressource, chaque ressource basée sur ce modèle reflète toutes les modifications que vous apportez au modèle sous-jacent. Jusqu'à ce que les modifications se propagent, l'état de chaque ressource est `UPDATING`. Attendez que l'état des ressources passe à `ACTIVE` pour pouvoir interagir avec elles. Pendant ce temps, le statut du modèle de ressource mis à jour est `PROPAGATING`.

Lorsque vous mettez à jour un modèle de composant, chaque modèle d'actif qui intègre ce modèle de composant reflète les modifications. Jusqu'à ce que les modifications du modèle de composant se propagent, chaque modèle d'actif concerné possède l'`UPDATING`état, suivi `PROPAGATING` de la mise à jour de ses actifs associés, comme décrit dans le paragraphe précédent. Vous devez attendre que ces modèles d'actifs reviennent à leur `ACTIVE` état normal avant d'interagir avec eux. Pendant ce temps, le statut du modèle de composant mis à jour sera`PROPAGATING`.

Pour plus d'informations, consultez État des ressources et des modèles.

Rubriques

- Mettre à jour un modèle d'actif ou de composant (console)

- Mettre à jour un modèle d'actif ou de composant (AWS CLI)

Mettre à jour un modèle d'actif ou de composant (console)

Vous pouvez utiliser la AWS IoT SiteWise console pour mettre à jour un modèle de ressource ou un modèle de composant.

Pour mettre à jour un modèle d'actif ou un modèle de composant (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Models (Modèles).
3. Choisissez le modèle d'actif ou le modèle de composant à mettre à jour.
4. Choisissez Modifier.
5. Sur la page Modifier le modèle, effectuez l'une des opérations suivantes :
   - Dans Informations relatives au modèle, modifiez le nom du modèle.
   - Modifiez l'une des définitions d'attribut. Vous ne pouvez pas modifier le type de données des attributs existants. Pour plus d'informations, consultez Définition de données statiques (attributs).
   - Modifiez l'une des définitions de mesure. Vous ne pouvez pas modifier le type de données des mesures existantes. Pour plus d'informations, consultez Définition des flux de données provenant des équipements (mesures).
   - Modifiez l'une des définitions de transformation. Pour plus d'informations, consultez Transformation des données (transformations).
   - Modifiez l'une des définitions de métrique. Vous ne pouvez pas modifier l'intervalle de temps des métriques existantes. Pour plus d'informations, consultez Agrégation de données provenant de propriétés et d'autres actifs (métriques).
   - (Modèles d'actifs uniquement) Modifiez l'une des définitions de hiérarchie. Vous ne pouvez pas modifier le modèle de hiérarchie des hiérarchies existantes. Pour plus d'informations, consultez Définition de hiérarchies de modèles d'actifs.
6. Choisissez Enregistrer.

Mettre à jour un modèle d'actif ou de composant (AWS CLI)

Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour mettre à jour un modèle d'actif ou un modèle de composant.

Utilisez l'API UpdateAssetModel pour mettre à jour le nom, la description et les propriétés d'un modèle d'actif ou d'un modèle de composant. Pour les modèles d'actifs uniquement, vous pouvez mettre à jour les hiérarchies. Spécifiez les paramètres suivants :

- `assetModelId`— L'ID de l'actif. Il s'agit de l'identifiant réel au format UUID, ou du `externalId:myExternalId` s'il en possède un. Pour plus d'informations, consultez Référencement d'objets avec des identifiants externes dans le Guide de l'utilisateur AWS IoT SiteWise .

Spécifiez le modèle mis à jour dans la charge utile. Pour en savoir plus sur le format attendu d'un modèle d'actif ou d'un modèle de composant, voirCréation de modèles de ressources.

> **Warning**
>
> L'API UpdateAssetModel remplace le modèle existant par le modèle que vous fournissez dans la charge utile. Pour éviter de supprimer les propriétés ou les hiérarchies de votre modèle, vous devez inclure leurs identifiants et leurs définitions dans la charge utile du modèle mise à jour. Pour savoir comment interroger la structure existante de votre modèle, consultez le fonctionnement du DescribeAssetmodèle.

> **Note**
>
> La procédure suivante ne permet de mettre à jour que les modèles composites de type`AWS/ALARM`. Si vous souhaitez mettre à jour des modèles `CUSTOM` composites, utilisez plutôt UpdateAssetModelCompositeModèle. Pour plus d'informations, consultez Mise à jour de modèles composites personnalisés (composants).

Pour mettre à jour un modèle d'actif ou un modèle de composant (AWS CLI)

1. Exécutez la commande suivante pour récupérer la définition du modèle existant. Remplacez *`asset-model-id par l'ID`* ou l'ID externe du modèle d'actif ou du modèle de composant à mettre à jour.

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

L'opération renvoie une réponse contenant les détails du modèle. La réponse présente la structure suivante.

```
{
  "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"
  }
}
```

Pour plus d'informations, reportez-vous à la section Fonctionnement du DescribeAssetmodèle.

2. Créez un fichier appelé `update-asset-model.json` et copiez la réponse de la commande précédente dans le fichier.
3. Supprimez les paires clé-valeur suivantes de l'objet JSON dans `update-asset-model.json` :

   - `assetModelId`
   - `assetModelArn`
   - `assetModelCompositeModelSummaries`
   - `assetModelCreationDate`
   - `assetModelLastUpdateDate`
   - `assetModelStatus`
   - `assetModelType`

L'opération UpdateAssetModel attend une charge utile dont la structure est la suivante :

```
{
  "assetModelName": "String",
  "assetModelDescription": "String",
  "assetModelProperties": Array of AssetModelProperty,
  "assetModelHierarchies": Array of AssetModelHierarchyDefinition,
  "assetModelCompositeModels": Array of AssetModelCompositeModel
}
```

4. Dans `update-asset-model.json`, effectuez l'une des actions suivantes :
   - Modifiez le nom du modèle de ressource (`assetModelName`).
   - Modifiez, ajoutez ou supprimez la description du modèle de ressource (`assetModelDescription`).
   - Modifiez, ajoutez ou supprimez les propriétés du modèle de ressource (`assetModelProperties`). Vous ne pouvez pas modifier le `dataType` des propriétés existantes ou le `window` des métriques existantes. Pour plus d'informations, consultez Définition des propriétés des données.
   - Modifiez, ajoutez ou supprimez les hiérarchies du modèle de ressource (`assetModelHierarchies`). Vous ne pouvez pas modifier le `childAssetModelId` des hiérarchies existantes. Pour plus d'informations, consultez Définition de hiérarchies de modèles d'actifs.
   - Modifiez, ajoutez ou supprimez l'un des modèles composites de type `AWS/ALARM` (`assetModelCompositeModels`) du modèle d'actifs. Les alarmes surveillent d'autres propriétés afin que vous puissiez identifier les équipements ou les processus nécessitant une attention particulière. Chaque définition d'alarme est un modèle composite qui normalise l'ensemble de propriétés utilisées par l'alarme. Pour plus d'informations, consultez Surveillance des données à l'aide d'alarmes et Définition des alarmes sur les modèles d'actifs.
5. Exécutez la commande suivante pour mettre à jour le modèle de ressource avec la définition stockée dans `update-asset-model.json`. Remplacez *asset-model-id par l'ID* du modèle d'actif :

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

```
  --cli-input-json file://model-payload.json
```

Mise à jour de modèles composites personnalisés (composants)

Vous pouvez utiliser l' AWS IoT SiteWise API pour mettre à jour un modèle composite personnalisé ou la AWS IoT SiteWise console pour mettre à jour les composants.

Rubriques

- Mettre à jour un composant (console)
- Mettre à jour un modèle composite personnalisé (AWS CLI)

Mettre à jour un composant (console)

Vous pouvez utiliser la AWS IoT SiteWise console pour mettre à jour un composant.

Pour mettre à jour un composant (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Models (Modèles).
3. Choisissez le modèle d'actif dans lequel se trouve le composant.
4. Dans l'onglet Propriétés, sélectionnez Composants.
5. Choisissez le composant que vous souhaitez mettre à jour.
6. Choisissez Modifier.
7. Sur la page Modifier le composant, effectuez l'une des opérations suivantes :
   - Dans Informations relatives au modèle, modifiez le nom du modèle.
   - Modifiez l'une des définitions d'attribut. Vous ne pouvez pas modifier le type de données des attributs existants. Pour plus d'informations, consultez Définition de données statiques (attributs).
   - Modifiez l'une des définitions de mesure. Vous ne pouvez pas modifier le type de données des mesures existantes. Pour plus d'informations, consultez Définition des flux de données provenant des équipements (mesures).
   - Modifiez l'une des définitions de transformation. Pour plus d'informations, consultez Transformation des données (transformations).

- Modifiez l'une des définitions de métrique. Vous ne pouvez pas modifier l'intervalle de temps des métriques existantes. Pour plus d'informations, consultez Agrégation de données provenant de propriétés et d'autres actifs (métriques).

8. Choisissez Enregistrer.

Mettre à jour un modèle composite personnalisé (AWS CLI)

Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour mettre à jour un modèle composite personnalisé.

Pour mettre à jour le nom ou la description, utilisez l'opération UpdateAssetModelCompositeModel. Pour les modèles composites personnalisés en ligne uniquement, vous pouvez également mettre à jour les propriétés. Vous ne pouvez pas mettre à jour les propriétés d'un modèle composite component-model-based personnalisé, car son modèle de composant référencé fournit les propriétés associées.

> **Important**
>
> Si vous supprimez une propriété d'un modèle composite personnalisé, toutes les données précédentes relatives à cette propriété sont AWS IoT SiteWise supprimées. Vous ne pouvez pas modifier le type ou le type de données d'une propriété existante.
> Pour remplacer une propriété de modèle composite existante par une nouvelle propriété identiquename, procédez comme suit :
>
> 1. Soumettez une `UpdateAssetModelCompositeModel` demande en supprimant l'intégralité de la propriété existante.
> 2. Soumettez une deuxième `UpdateAssetModelCompositeModel` demande qui inclut la nouvelle propriété. La nouvelle propriété de l'actif sera la même `name` que la précédente et AWS IoT SiteWise générera une nouvelle propriété unique`id`.

Pour mettre à jour un modèle composite personnalisé (AWS CLI)

1. Pour récupérer la définition du modèle composite existant, exécutez la commande suivante. Remplacez *`composite-model-id par l'ID`* ou l'ID externe du modèle composite personnalisé à mettre à jour, et *`asset-model-id`* par le modèle d'actif auquel le modèle composite personnalisé est associé. Pour plus d'informations, consultez le guide de AWS IoT SiteWise l'utilisateur.

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

Pour plus d'informations, reportez-vous à la section Fonctionnement du DescribeAssetModelCompositemodèle.

2. Créez un fichier appeléupdate-custom-composite-model.json, puis copiez la réponse de la commande précédente dans le fichier.
3. Supprimez toutes les paires clé-valeur de l'objet JSON, à update-custom-composite-model.json l'exception des champs suivants :
   - assetModelCompositeModelName
   - assetModelCompositeModelDescription(si présent)
   - assetModelCompositeModelProperties(si présent)
4. Dans update-custom-composite-model.json, effectuez l'une des actions suivantes :
   - Modifiez la valeur deassetModelCompositeModelName.
   - AjoutezassetModelCompositeModelDescription, supprimez ou modifiez sa valeur.
   - Pour les modèles composites personnalisés en ligne uniquement : modifiez, ajoutez ou supprimez l'une des propriétés du modèle d'actif dansassetModelCompositeModelProperties.

   Pour plus d'informations sur le format requis pour ce fichier, consultez la syntaxe de demande pour UpdateAssetModelCompositeModel.
5. Exécutez la commande suivante pour mettre à jour le modèle composite personnalisé avec la définition stockée dansupdate-custom-composite-model.json. Remplacez *composite-model-id par l'ID* du modèle composite et *asset-model-id par l'ID* du modèle d'actif dans lequel il se trouve.

```
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
```

Suppression des ressources et des modèles

Vous pouvez supprimer vos actifs et vos modèles une AWS IoT SiteWise fois que vous en avez terminé avec eux. Les opérations de suppression sont asynchrones et leur propagation prend du temps. AWS IoT SiteWise

Rubriques

- Suppression de ressources
- Suppression de modèles de ressource

Suppression de ressources

Vous pouvez utiliser la AWS IoT SiteWise console ou l'API pour supprimer un actif.

Avant de pouvoir supprimer une ressource, vous devez d'abord dissocier ses ressources enfants et la dissocier de sa ressource parent. Pour plus d'informations, consultez Association et dissociation de ressources. Si vous utilisez le AWS Command Line Interface (AWS CLI), vous pouvez utiliser l'opération ListAssociatedAssets pour répertorier les enfants d'un actif.

Lorsque vous supprimez une ressource, son état est `DELETING` jusqu'à ce que les modifications soient propagées. Pour plus d'informations, consultez État des ressources et des modèles. Une fois la ressource supprimée, vous ne pouvez plus l'interroger. Si vous le faites, l'API renvoie une réponse HTTP 404.

> **Important**
>
> AWS IoT SiteWise supprime toutes les données de propriété des actifs supprimés.

Rubriques

- Suppression d'une ressource (console)
- Supprimer un actif (AWS CLI)

Suppression d'une ressource (console)

Vous pouvez utiliser la AWS IoT SiteWise console pour supprimer un actif.

Pour supprimer une ressource (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Ressources.
3. Choisissez la ressource à supprimer.

> **Tip**
>
> Vous pouvez cliquer sur l'icône en forme de flèche pour développer une hiérarchie de ressources afin de trouver votre ressource.

4. Si la ressource comporte des ressources associées, supprimez chaque ressource. Vous pouvez choisir le nom d'une ressource pour accéder à sa page, où vous pouvez la supprimer.
5. Sur la page de la ressource, choisissez Supprimer.
6. Dans la boîte de dialogue Supprimer la ressource, procédez comme suit :
   a. Saisissez **`Delete`** pour confirmer la suppression.
   b. Sélectionnez Delete (Supprimer).

Supprimer un actif (AWS CLI)

Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour supprimer un actif.

Utilisez cette DeleteAssetopération pour supprimer un actif. Spécifiez le paramètre suivant :

- `assetId`— L'ID de l'actif. Il s'agit de l'identifiant réel au format UUID, ou du `externalId:myExternalId` s'il en possède un. Pour plus d'informations, consultez Référencement d'objets avec des identifiants externes dans le Guide de l'utilisateur AWS IoT SiteWise .

Pour supprimer un actif (AWS CLI)

1. Exécutez la commande suivante pour répertorier les hiérarchies de la ressource. Remplacez *`asset-id`* par l'ID ou l'ID externe de l'actif :

```
aws iotsitewise describe-asset --asset-id asset-id
```

L'opération renvoie une réponse qui contient les détails de la ressource. La réponse contient une `assetHierarchies` liste dont la structure est la suivante :

```
{
  ...
  "assetHierarchies": [
    {
      "id": "String",
      "name": "String"
    }
  ],
  ...
}
```

Pour plus d'informations, consultez l'DescribeAssetopération.

2. Pour chaque hiérarchie, exécutez la commande suivante pour répertorier les enfants de la ressource qui sont associés à cette hiérarchie. Remplacez *`asset-id`* par l'ID ou l'ID externe de l'actif et *`hierarchy-id par l'ID`* ou l'ID externe de la hiérarchie.

```
aws iotsitewise list-associated-assets \
  --asset-id asset-id \
  --hierarchy-id hierarchy-id
```

Pour plus d'informations, consultez la section Fonctionnement ListAssociateddes actifs.

3. Exécutez la commande suivante pour supprimer chaque ressource associée, puis pour supprimer la ressource. Remplacez *`asset-id`* par l'ID ou l'ID externe de l'actif.

```
aws iotsitewise delete-asset --asset-id asset-id
```

Suppression de modèles de ressource

Vous pouvez utiliser la AWS IoT SiteWise console ou l'API pour supprimer un modèle de ressource.

Avant de pouvoir supprimer un modèle d'actif, vous devez d'abord supprimer tous les actifs créés à partir du modèle d'actif.

Lorsque vous supprimez un modèle de ressource, son état est `DELETING` jusqu'à ce que les modifications soient propagées. Pour plus d'informations, consultez État des ressources et des

modèles. Une fois le modèle de ressource supprimé, vous ne pouvez plus l'interroger. Si vous le faites, l'API renvoie une réponse HTTP 404.

Rubriques

- Suppression d'un modèle de ressource (console)
- Supprimer un modèle de ressource (AWS CLI)

Suppression d'un modèle de ressource (console)

Vous pouvez utiliser la AWS IoT SiteWise console pour supprimer un modèle de ressource.

Pour supprimer un modèle de ressource (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Models (Modèles).
3. Choisissez le modèle de ressource à supprimer.
4. Si le modèle comporte des ressources, supprimez chaque ressource. Choisissez le nom d'une ressource pour accéder à sa page, où vous pouvez la supprimer. Pour plus d'informations, consultez Suppression d'une ressource (console).
5. Sur la page du modèle, choisissez Supprimer.
6. Dans la boîte de dialogue Supprimer le modèle, procédez comme suit :

    a. Saisissez **`Delete`** pour confirmer la suppression.

    b. Sélectionnez Delete (Supprimer).

Supprimer un modèle de ressource (AWS CLI)

Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour supprimer un modèle de ressource.

Utilisez l'opération DeleteAssetModel pour supprimer un modèle de ressource. Spécifiez le paramètre suivant :

- `assetModelId`— L'ID de l'actif. Il s'agit de l'identifiant réel au format UUID, ou du `externalId:myExternalId` s'il en possède un. Pour plus d'informations, consultez Référencement d'objets avec des identifiants externes dans le Guide de l'utilisateur AWS IoT SiteWise .

Pour supprimer un modèle de ressource (AWS CLI)

1. Exécutez la commande suivante pour répertorier toutes les ressources créées à partir du modèle. Remplacez *asset-model-id* par l'ID ou l'ID externe du modèle d'actif.

   ```
   aws iotsitewise list-assets --asset-model-id asset-model-id
   ```

   Pour plus d'informations, consultez l'ListAssetsopération.
2. Si la commande précédente renvoie des ressources du modèle, supprimez chaque ressource. Pour plus d'informations, consultez Supprimer un actif (AWS CLI).
3. Exécutez la commande suivante pour supprimer le modèle de ressource. Remplacez *asset-model-id par l'ID* ou l'ID externe du modèle d'actif.

   ```
   aws iotsitewise delete-asset-model --asset-model-id asset-model-id
   ```

Opérations groupées avec actifs et modèles

Pour travailler avec un grand nombre de ressources ou de modèles d'actifs, utilisez des opérations groupées pour importer et exporter des ressources en masse vers un autre emplacement. Par exemple, vous pouvez créer un fichier de données qui définit les actifs ou les modèles d'actifs dans un compartiment Amazon S3, et utiliser l'importation en masse pour les créer ou les mettre à jour AWS IoT SiteWise. Sinon, si vous avez un grand nombre de ressources ou de modèles d'actifs AWS IoT SiteWise, vous pouvez les exporter vers Amazon S3.

> **Note**
>
> Vous effectuez des opérations AWS IoT SiteWise groupées en appelant des opérations dans l' AWS IoT TwinMaker API. Vous pouvez le faire sans configurer AWS IoT TwinMaker ni créer d' AWS IoT TwinMaker espace de travail. Tout ce dont vous avez besoin, c'est d'un compartiment Amazon S3 dans lequel vous pouvez placer votre AWS IoT SiteWise contenu.

Rubriques

- Concepts clés et terminologie
- Fonctionnalités prises en charge
- Prérequis pour les opérations en masse

- Exécution d'une tâche d'importation en bloc
- Exécution d'une tâche d'exportation groupée
- Suivi de l'avancement des tâches et gestion des erreurs
- Exemples d'importation de métadonnées
- Exemples de métadonnées d'exportation
- AWS IoT SiteWise schéma de tâche de transfert de métadonnées

Concepts clés et terminologie

AWS IoT SiteWise les fonctionnalités d'importation et d'exportation en bloc reposent sur les concepts et la terminologie suivants :

- Importer : action qui consiste à déplacer des actifs ou des modèles d'actifs d'un fichier d'un compartiment Amazon S3 vers AWS IoT SiteWise.
- Exporter : action qui consiste à déplacer des actifs ou des modèles AWS IoT SiteWise d'actifs depuis un compartiment Amazon S3.
- Source : point de départ à partir duquel vous souhaitez déplacer le contenu.

  Par exemple, un compartiment Amazon S3 est une source d'importation et AWS IoT SiteWise une source d'exportation.
- Destination : emplacement souhaité vers lequel vous souhaitez déplacer votre contenu.

  Par exemple, un compartiment Amazon S3 est une destination d'exportation et AWS IoT SiteWise une destination d'importation.
- AWS IoT SiteWise Schéma : Ce schéma est utilisé pour importer et exporter des métadonnées depuis AWS IoT SiteWise.
- Ressource de haut niveau : AWS IoT SiteWise ressource que vous pouvez créer ou mettre à jour individuellement, telle qu'un actif ou un modèle d'actif.
- Sous-ressource : ressource imbriquée dans une AWS IoT SiteWise ressource de niveau supérieur. Les exemples incluent les propriétés, les hiérarchies et les modèles composites.
- Métadonnées : informations clés requises pour importer ou exporter des ressources avec succès. Les définitions des actifs et des modèles d'actifs sont des exemples de métadonnées.
- metadata TransferJob : objet créé lors de l'exécution`CreateMetadataTransferJob`.

Fonctionnalités prises en charge

Cette rubrique explique ce que vous pouvez faire lorsque vous exécutez une opération en masse. Les opérations groupées prennent en charge les fonctionnalités suivantes :

- Création de ressources de haut niveau : lorsque vous importez un actif ou un modèle d'actif qui ne définit pas d'identifiant, ou dont l'identifiant ne correspond pas à celui d'un actif existant, il est créé en tant que nouvelle ressource.
- Remplacement des ressources de haut niveau : lorsque vous importez un actif ou un modèle d'actif dont l'identifiant correspond à un actif qui existe déjà, il remplace la ressource existante.
- Création, remplacement ou suppression de sous-ressources : lorsque votre importation remplace une ressource de haut niveau telle qu'un actif ou un modèle d'actif, la nouvelle définition remplace toutes les sous-ressources, telles que les propriétés, les hiérarchies ou les modèles composites.

  Par exemple, si vous mettez à jour un modèle de ressource lors d'une importation en bloc et que la version mise à jour définit une propriété qui n'était pas présente dans l'original, une nouvelle propriété est créée. S'il définit une propriété qui existe déjà, la propriété existante sera mise à jour. Si le modèle d'actif mis à jour omet une propriété présente dans l'original, la propriété est supprimée.
- Aucune suppression de ressources de niveau supérieur : les opérations groupées ne suppriment pas un actif ou un modèle d'actif. Les opérations groupées ne font que les créer ou les mettre à jour.

Prérequis pour les opérations en masse

Cette section explique les conditions requises pour les opérations en masse, y compris les autorisations AWS Identity and Access Management (IAM) pour l'échange de ressources entre Services AWS et votre machine locale. Avant de démarrer une opération en bloc, remplissez les conditions préalables suivantes :

- Créez un compartiment Amazon S3 pour stocker les ressources. Pour plus d'informations sur l'utilisation d'Amazon S3, consultez Qu'est-ce qu'Amazon S3 ?

Autorisations IAM

Pour effectuer des opérations en masse, vous devez créer une politique AWS Identity and Access Management (IAM) avec des autorisations permettant l'échange de AWS ressources entre Amazon

S3 et votre machine locale. AWS IoT SiteWise Pour plus d'informations sur la création de politiques IAM, consultez Création de politiques IAM.

Pour effectuer des opérations groupées, vous avez besoin des règles suivantes.

AWS IoT SiteWise politique

Cette politique permet d'accéder aux actions d' AWS IoT SiteWise API requises pour les opérations groupées :

```
{
    "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 politique

Cette politique permet d'accéder aux opérations AWS IoT TwinMaker d'API que vous utilisez pour travailler avec des opérations groupées :

```
{
    "Sid": "MetadataTransferJobApiAccess",
    "Effect": "Allow",
    "Action": [
        "iottwinmaker:CreateMetadataTransferJob",
        "iottwinmaker:CancelMetadataTransferJob",
        "iottwinmaker:GetMetadataTransferJob",
        "iottwinmaker:ListMetadataTransferJobs"
    ],
    "Resource": "*"
}
```

Politique Amazon S3

Cette politique donne accès aux compartiments Amazon S3 pour le transfert de métadonnées pour les opérations en masse.

For a specific Amazon S3 bucket

Si vous utilisez un bucket spécifique pour travailler avec les métadonnées de vos opérations groupées, cette politique permet d'accéder à ce 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

Si vous devez utiliser de nombreux compartiments différents pour travailler avec les métadonnées de vos opérations groupées, cette politique permet d'accéder à n'importe quel compartiment :

```
{
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:AbortMultipartUpload",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
    ],
    "Resource": "*"
}
```

Pour plus d'informations sur la résolution des problèmes liés aux opérations d'importation et d'exportation, consultezRésolution des problèmes d'importation et d'exportation en masse.

Exécution d'une tâche d'importation en bloc

L'importation en masse consiste à déplacer des métadonnées dans un AWS IoT SiteWise espace de travail. Par exemple, l'importation en masse peut déplacer des métadonnées d'un fichier local ou d'un fichier d'un compartiment Amazon S3 vers un AWS IoT SiteWise espace de travail.

Étape 1 : Préparation du fichier à importer

Téléchargez le fichier au format AWS IoT SiteWise natif pour importer les actifs et les modèles d'actifs. Pour plus d'informations, consultez AWS IoT SiteWise schéma de tâche de transfert de métadonnées.

Étape 2 : Chargez le fichier préparé sur Amazon S3

Téléchargez le fichier sur Amazon S3. Consultez la section Chargement d'un fichier vers Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service pour plus de détails.

Importer des métadonnées (console)

Vous pouvez utiliser le Console AWS IoT SiteWise pour importer des métadonnées en bloc. Suivez Étape 1 : Préparation du fichier à importer et Étape 2 : Chargez le fichier préparé sur Amazon S3 pour préparer un fichier prêt à être importé.

Importez des données depuis Amazon S3 vers Console AWS IoT SiteWise

1. Accédez à la console AWS IoT SiteWise.
2. Choisissez Bulk operations New dans le volet de navigation.
3. Choisissez Nouvelle importation pour démarrer le processus d'importation.
4. Sur la page Importer des métadonnées :
   - Choisissez Parcourir Amazon S3 pour afficher le compartiment et les fichiers Amazon S3.
   - Accédez au compartiment Amazon S3 qui contient le fichier d'importation préparé.
   - Sélectionnez le fichier à importer.
   - Passez en revue le fichier sélectionné, puis choisissez Importer.
5. La page Opérations groupées sur les SiteWise métadonnées Console AWS IoT SiteWise affiche la tâche d'importation nouvellement créée dans le tableau de progression des tâches.

Importer des métadonnées (AWS CLI)

Pour effectuer une opération d'importation, procédez comme suit :

Importez des données depuis Amazon S3 vers AWS CLI

1. Créez un fichier de métadonnées qui indique les ressources que vous souhaitez importer, en suivant leAWS IoT SiteWise schéma de tâche de transfert de métadonnées. Stockez ce fichier dans votre compartiment Amazon S3.

   Pour des exemples de fichiers de métadonnées à importer, consultezExemples d'importation de métadonnées.

2. Créez maintenant un fichier JSON avec le corps de la requête. Le corps de la demande indique la source et la destination de la tâche de transfert. Ce fichier est distinct du fichier de l'étape précédente. Assurez-vous de spécifier votre compartiment Amazon S3 en tant que source et `iotsitewise` en tant que destination.

   L'exemple suivant montre le corps de la demande :

   ```
   {
         "metadataTransferJobId": "your-transfer-job-Id",
         "sources": [{
             "type": "s3",
             "s3Configuration": {
                 "location": "arn:aws:s3:::your-S3-bucket-name/
   your_import_metadata.json"
             }
         }],
         "destination": {
             "type": "iotsitewise"
         }
     }
   ```

3. Appelez le `CreateMetadataTransferJob` en exécutant la AWS CLI commande suivante. Dans cet exemple, le fichier du corps de la demande de l'étape précédente est nommé`createMetadataTransferJobExport.json`.

   ```
   aws iottwinmaker create-metadata-transfer-job --region us-east-1 \
     --cli-input-json file://createMetadataTransferJobImport.json
   ```

   Cela créera une tâche de transfert de métadonnées et lancera le processus de transfert des ressources que vous avez sélectionnées.

Exécution d'une tâche d'exportation groupée

L'exportation en masse consiste à déplacer des métadonnées d'un AWS IoT SiteWise espace de travail vers un compartiment Amazon S3.

Lorsque vous exportez votre AWS IoT SiteWise contenu en masse vers Amazon S3, vous pouvez définir des filtres pour limiter les modèles d'actifs et les actifs spécifiques que vous souhaitez exporter.

Les filtres doivent être spécifiés dans une `iotSiteWiseConfiguration` section de la section sources de votre requête JSON.

> **Note**
>
> Vous pouvez inclure plusieurs filtres dans votre demande. L'opération groupée exportera les modèles d'actifs et les actifs correspondant à l'un des filtres.
> Si vous ne fournissez aucun filtre, l'opération groupée exporte tous vos modèles et actifs d'actifs.

Example corps de la demande avec filtres

```
{
      "metadataTransferJobId": "your-transfer-job-id",
      "sources": [
       {
        "type": "iotsitewise",
        "iotSiteWiseConfiguration": {
          "filters": [
           {
              "filterByAssetModel": {
                  "assetModelId": "asset model ID"
              }
            },
            {
              "filterByAssetModel": {
                  "assetModelId": "asset model ID",
                  "includeAssets": true
              }
            },
            {
              "filterByAssetModel": {
                  "assetModelId": "asset model ID",
                  "includeOffspring": true
               }
             }
           ]
          }
        }
       ],
```

```
        "destination": {
           "type": "s3",
           "s3Configuration": {
             "location": "arn:aws:s3:::your-S3-bucket-location"
           }
        }
}
```

Exporter les métadonnées (console)

La procédure suivante explique l'action d'exportation de la console :

Créez une tâche d'exportation dans le Console AWS IoT SiteWise

1. Accédez à la console AWS IoT SiteWise.
2. Choisissez Bulk operations New dans le volet de navigation.
3. Choisissez Nouvelle exportation pour démarrer le processus d'exportation.
4. Sur la page Exporter les métadonnées :

   - Entrez le nom de la tâche d'exportation. Il s'agit du nom utilisé pour le fichier exporté dans votre compartiment Amazon S3.
   - Choisissez les ressources à exporter, ce qui définit les filtres pour le travail :
     - Exportez tous les actifs et modèles d'actifs. Utilisez des filtres sur les actifs et les modèles d'actifs.
     - Exportez des actifs. Filtrez en fonction de vos actifs.
       - Sélectionnez la ressource à utiliser pour le filtre d'exportation.
       - (Facultatif) Ajoutez la descendance ou le modèle d'actif associé.
     - Exportez des modèles d'actifs. Filtrez en fonction de vos modèles d'actifs.
       - Sélectionnez le modèle de ressource à utiliser pour le filtre d'exportation.
       - (Facultatif) Ajoutez la progéniture, ou l'actif associé, ou les deux.
     - Choisissez Suivant.
   - Accédez au compartiment Amazon S3 :
     - Choisissez Parcourir Amazon S3 pour afficher le compartiment et les fichiers Amazon S3.
     - Accédez au compartiment Amazon S3 dans lequel le fichier doit être placé.
     - Choisissez Suivant.
   - Passez en revue la tâche d'exportation et choisissez Exporter.

5. La page Opérations groupées sur les SiteWise métadonnées Console AWS IoT SiteWise affiche la tâche d'importation nouvellement créée dans le tableau de progression des tâches.

Pour connaître les différentes manières d'utiliser les filtres lors de l'exportation de métadonnées, consultezExemples de métadonnées d'exportation.

Exporter les métadonnées (AWS CLI)

La procédure suivante explique l'opération AWS CLI d'exportation :

Exporter des données depuis AWS IoT SiteWise Amazon S3

1. Créez un fichier JSON avec le corps de votre requête. Le corps de la demande indique la source et la destination de la tâche de transfert. L'exemple suivant montre un exemple de corps de demande :

```
{
    "metadataTransferJobId": "your-transfer-job-Id",
    "sources": [{
        "type": "iotsitewise"
    }],
    "destination": {
        "type": "s3",
        "s3Configuration": {
            "location": "arn:aws:s3:::your-S3-bucket-location"
        }
    }
}
```

   Assurez-vous de spécifier votre compartiment Amazon S3 comme destination de la tâche de transfert de métadonnées.

   > **Note**
   >
   > Cet exemple exportera tous vos modèles d'actifs et actifs. Pour limiter l'exportation à des modèles d'actifs ou à des actifs spécifiques, vous pouvez inclure des filtres dans le corps de votre demande. Pour plus d'informations sur l'application de filtres d'exportation, consultezExemples de métadonnées d'exportation.

2. Enregistrez le corps du fichier de votre demande pour l'utiliser à l'étape suivante. Dans cet exemple, le fichier est nommé `createMetadataTransferJobExport.json`.
3. Appelez le `CreateMetadataTransferJob` en exécutant la AWS CLI commande suivante :

```
aws iottwinmaker create-metadata-transfer-job --region us-east-1 \
        --cli-input-json file://createMetadataTransferJobExport.json
```

   Remplacez le fichier JSON d'entrée `createMetadataTransferJobExport.json` par votre propre nom de fichier de transfert.

Suivi de l'avancement des tâches et gestion des erreurs

Le traitement d'une tâche en masse prend du temps. Chaque tâche est traitée dans l'ordre de AWS IoT SiteWise réception de la demande. Il est traité one-at-a-time pour chaque compte. Lorsqu'une tâche est terminée, la suivante en file d'attente démarre automatiquement le traitement. AWS IoT SiteWise résout les tâches de manière asynchrone et met à jour le statut de chacune au fur et à mesure de son avancement. Chaque tâche possède un champ d'état qui contient l'état de la ressource et un message d'erreur, le cas échéant.

L'état peut avoir l'une des valeurs suivantes :

- `VALIDATING`— Validation de la tâche, y compris le format de fichier soumis et son contenu.
- `PENDING`— La tâche est dans une file d'attente. Vous pouvez annuler des tâches dans cet état depuis la AWS IoT SiteWise console, mais tous les autres états continueront jusqu'à la fin.
- `RUNNING`— Traitement de la tâche. Il s'agit de créer et de mettre à jour des ressources telles que définies par le fichier d'importation, ou d'exporter des ressources en fonction des filtres de tâches d'exportation choisis. En cas d'annulation, aucune ressource importée par cette tâche n'est supprimée. Pour plus d'informations, consultez Consulter la progression et les détails de la tâche (console).
- `CANCELLING`— L'offre d'emploi est activement annulée.
- `ERROR`— Une ou plusieurs ressources n'ont pas pu être traitées. Consultez le rapport de travail détaillé pour plus d'informations. Pour plus d'informations, consultez Inspecter les détails de l'erreur (console).
- `COMPLETED`— Job terminé sans erreur.

- `CANCELLED`— La tâche est annulée et n'est pas mise en file d'attente. Si vous avez annulé une `RUNNING` tâche, les ressources déjà importées par cette tâche au moment de l'annulation ne sont pas supprimées de AWS IoT SiteWise.

Rubriques

- Suivi de l'avancement des tâches
- Inspectez les erreurs

Suivi de l'avancement des tâches

Consulter la progression et les détails de la tâche (console)

Consultez Importer des métadonnées (console) ou Exporter les métadonnées (console) pour démarrer une tâche groupée.

Vue d'ensemble de l'avancement des tâches dans la AWS IoT SiteWise console :

1. Accédez à la console AWS IoT SiteWise.
2. Choisissez Bulk operations New dans le volet de navigation.
3. Le tableau de progression des tâches de la AWS IoT SiteWise console affiche la liste des tâches exécutées en bloc.
4. La colonne Type de tâche indique s'il s'agit d'une tâche d'exportation ou d'importation. Les colonnes Date d'importation indiquent la date de début de la tâche.
5. La colonne Status affiche le statut de la tâche. Vous pouvez sélectionner une tâche pour en voir les détails.
6. La tâche sélectionnée affiche Success en cas de réussite, ou une liste d'échecs en cas d'échec de la tâche. Une description de l'erreur est également affichée pour chaque type de ressource.

Vue d'ensemble des détails du job dans la AWS IoT SiteWise console :

Le tableau de progression des tâches de la AWS IoT SiteWise console affiche la liste des tâches exécutées en bloc.

1. Choisissez un poste pour obtenir plus de détails.
2. Pour une tâche d'importation, `Data source ARN` représente l'emplacement du fichier d'importation sur Amazon S3.

3. Pour une tâche d'exportation, le `Data destination ARN` représente l'emplacement du fichier sur Amazon S3 après l'exportation.
4. Les `Status` et`Status reason`, fournissent des détails supplémentaires sur le travail en cours. Pour plus d'informations, consultez Suivi de l'avancement des tâches et gestion des erreurs.
5. Le `Queued position` représente la position de la tâche dans la file d'attente des processus. Les tâches sont traitées une par une. Une position en file d'attente de 1 indique que le travail sera traité ensuite.
6. La page de détails des tâches affiche également le nombre d'avancement des tâches.
   - Les types de comptage de l'avancement des tâches sont les suivants :
     i. `Total resources`— Indique le nombre total d'actifs dans le processus de transfert.
     ii. `Succeeded`— Indique le nombre d'actifs transférés avec succès au cours du processus.
     iii. `Failed`— Indique le nombre d'actifs défaillants au cours du processus.
     iv. `Skipped`— Indique le nombre d'actifs ignorés au cours du processus.
7. Un statut de tâche égal `PENDING` ou `VALIDATING` affiche la progression de toutes les tâches comme étant pris en compte–. Cela indique que le nombre de progrès des tâches est en cours d'évaluation.
8. Un statut de tâche de `RUNNING` affiche le `Total resources` nombre de tâches soumises pour traitement. Les dénombrements détaillés (`Succeeded`Failed, et`Skipped`) s'appliquent aux ressources traitées. La somme des dénombrements détaillés est inférieure au `Total resources` nombre, jusqu'à ce que le statut du poste soit `COMPLETED` ou`ERROR`.
9. Si le statut d'une tâche est `COMPLETED` ou`ERROR`, le `Total resources` nombre est égal à la somme des dénombrements détaillés (`Succeeded`Failed, et`Skipped`).
10. Si le statut d'une tâche est défini comme `ERROR` tel, consultez le tableau des échecs des tâches pour plus de détails sur les erreurs et les échecs spécifiques. Pour plus d'informations, consultez Inspecter les détails de l'erreur (console).

Examiner l'avancement et les détails du travail (AWS CLI)

Après avoir démarré une opération groupée, vous pouvez vérifier ou mettre à jour son statut à l'aide des actions d'API suivantes :

- Pour récupérer des informations sur une tâche spécifique, utilisez l'action GetMetadataTransferJobAPI.

  Récupérez des informations avec l'**`GetMetadataTransferJob`**API :

  1. Créez et exécutez une tâche de transfert. Appelez l'API `GetMetadataTransferJob`.

     Example AWS CLI commande :

     ```
     aws iottwinmaker get-metadata-transfer-job \
             --metadata-transfer-job-id your_metadata_transfer_job_id \
             --region your_region
     ```

  2. L'`GetMetadataTransferJob`API renvoie un `MetadataTransferJobProgress` objet avec les paramètres suivants :

     - SucceededCount — Indique le nombre d'actifs transférés avec succès au cours du processus.
     - FailedCount — Indique le nombre d'actifs défaillants au cours du processus.
     - SkippedCount — Indique le nombre de ressources ignorées au cours du processus.
     - TotalCount — Indique le nombre total d'actifs dans le processus de transfert.

     Ces paramètres indiquent l'état d'avancement de la tâche. Si le statut est le cas`RUNNING`, ils permettent de suivre le nombre de ressources restant à traiter.

     Si vous rencontrez des erreurs de validation du schéma, ou si FailedCount est supérieur ou égal à 1, l'état d'avancement de la tâche passe à. `ERROR` Un rapport d'erreur complet relatif à la tâche est placé dans votre compartiment Amazon S3. Pour plus d'informations, consultez Inspectez les erreurs.

- Pour répertorier les tâches en cours, utilisez l'action ListMetadataTransferJobsAPI.

  Utilisez un fichier JSON pour filtrer les tâches renvoyées en fonction de leur état actuel. Consultez la procédure suivante :

  1. Pour spécifier les filtres que vous souhaitez utiliser, créez un fichier JSON AWS CLI d'entrée. Vous souhaitez utiliser :

     ```
     {
         "sourceType": "s3",
     ```

```
    "destinationType": "iottwinmaker",
    "filters": [{
        "state": "COMPLETED"
    }]
}
```

Pour obtenir la liste des `state` valeurs valides, consultez la section ListMetadataTransferJobsFiltrer dans le guide de référence de l'AWS IoT TwinMaker API.

2. Utilisez le fichier JSON comme argument dans l' AWS CLI exemple de commande suivant :

```
aws iottwinmaker list-metadata-transfer-job --region your_region \
        --cli-input-json file://ListMetadataTransferJobsExample.json
```

- Pour annuler une tâche, utilisez l'action CancelMetadataTransferJobAPI. Cette API annule la tâche de transfert de métadonnées spécifique, sans affecter les ressources déjà exportées ou importées :

```
aws iottwinmaker cancel-metadata-transfer-job \
        --region your_region \
        --metadata-transfer-job-id job-to-cancel-id
```

Inspectez les erreurs

Inspecter les détails de l'erreur (console)

Détails de l'erreur dans la AWS IoT SiteWise console :

1. Accédez à la console AWS IoT SiteWise.
2. Consultez le tableau de progression des tâches Console AWS IoT SiteWise pour obtenir la liste des tâches liées aux opérations groupées.
3. Sélectionnez une tâche pour afficher les détails de la tâche.
4. Si le statut d'une tâche est `COMPLETED` ou`ERROR`, le `Total resources` nombre est égal à la somme des dénombrements détaillés (`SucceededFailed`, et`Skipped`).
5. Si le statut d'une tâche est défini comme `ERROR` tel, consultez le tableau des échecs des tâches pour plus de détails sur les erreurs et les échecs spécifiques.
6. Le tableau des échecs de tâches affiche le contenu du rapport de tâche. Le `Resource type` champ indique l'emplacement de l'erreur ou des défaillances, par exemple :

- Par exemple, une erreur de validation `Bulk operations template` dans le `Resource type` champ indique que le modèle d'importation et le format de fichier du schéma de métadonnées ne correspondent pas. Pour plus d'informations, consultez AWS IoT SiteWise schéma de tâche de transfert de métadonnées.
- Un échec `Asset` dans le `Resource type` champ indique que l'actif n'a pas été créé en raison d'un conflit avec un autre actif. Consultez la section Erreurs courantes pour plus d'informations sur les erreurs et les conflits liés aux AWS IoT SiteWise ressources.

Inspecter les détails de l'erreur (AWS CLI)

Pour gérer et diagnostiquer les erreurs produites lors d'une tâche de transfert, consultez la procédure suivante concernant l'utilisation de l'action `GetMetadataTransferJob` API :

1. Après avoir créé et exécuté une tâche de transfert, appelez GetMetadataTransferJob:

   ```
   aws iottwinmaker get-metadata-transfer-job \
           --metadata-transfer-job-id your_metadata_transfer_job_id \
           --region us-east-1
   ```

2. Une fois que l'état de la tâche est passé à zéro`COMPLETED`, vous pouvez commencer à vérifier les résultats de la tâche.
3. Lorsque vous appelez`GetMetadataTransferJob`, il renvoie un objet appelé `MetadataTransferJobProgress`.

   L' MetadataTransferJobProgress objet contient les paramètres suivants :

   - FailedCount : indique le nombre d'actifs défaillants pendant le processus de transfert.
   - SkippedCount : indique le nombre d'actifs ignorés pendant le processus de transfert.
   - SucceededCount : indique le nombre d'actifs qui ont réussi pendant le processus de transfert.
   - TotalCount : indique le nombre total d'actifs impliqués dans le processus de transfert.
4. En outre, l'appel d'API renvoie un élément `reportUrl` contenant une URL présignée. Si votre tâche de transfert présente des problèmes que vous devez approfondir, consultez cette URL.

Exemples d'importation de métadonnées

Cette section explique comment créer des fichiers de métadonnées pour importer des modèles d'actifs et des actifs en une seule opération d'importation en bloc.

Exemple d'importation en masse

Vous pouvez importer de nombreux modèles et actifs en une seule opération d'importation en bloc. L'exemple suivant montre comment créer un fichier de métadonnées à cette fin.

Dans cet exemple de scénario, plusieurs sites de travail contiennent des robots industriels dans des cellules de travail.

L'exemple définit deux modèles d'actifs :

- `RobotModel1`: Ce modèle d'actif représente un type particulier de robot que vous avez sur vos sites de travail. Le robot possède une propriété de mesure,`Temperature`.
- `WorkCell`: Ce modèle d'actif représente un ensemble de robots au sein de l'un de vos sites de travail. Le modèle d'actifs définit une hiérarchie pour représenter la relation entre une cellule de travail et des robots. `robotHierarchyOEM1`

L'exemple définit également certains actifs :

- `WorkCell1`: une cellule de travail au sein de votre site de Boston
- `RobotArm123456`: un robot au sein de cette cellule de travail
- `RobotArm987654`: un autre robot au sein de cette cellule de travail

Le fichier de métadonnées JSON suivant définit ces modèles et actifs d'actifs. L'exécution d'une importation groupée avec ces métadonnées crée les modèles d'actifs et les actifs qu'ils contiennent AWS IoT SiteWise, y compris leurs relations hiérarchiques.

Fichier de métadonnées à importer

```
{
    "assetModels": [
        {
            "assetModelExternalId": "Robot.OEM1.3536",
            "assetModelName": "RobotModel1",
            "assetModelProperties": [
```

```
                {
                    "dataType": "DOUBLE",
                    "externalId": "Temperature",
                    "name": "Temperature",
                    "type": {
                        "measurement": {
                            "processingConfig": {
                                "forwardingConfig": {
                                    "state": "ENABLED"
                                }
                            }
                        }
                    },
                    "unit": "fahrenheit"
                }
            ]
        },
        {
            "assetModelExternalId": "ISA95.WorkCell",
            "assetModelName": "WorkCell",
            "assetModelProperties": [],
            "assetModelHierarchies": [
                {
                    "externalId": "workCellHierarchyWithOEM1Robot",
                    "name": "robotHierarchyOEM1",
                    "childAssetModelExternalId": "Robot.OEM1.3536"
                }
            ]
        }
    ],
    "assets": [
        {
            "assetExternalId": "Robot.OEM1.3536.123456",
            "assetName": "RobotArm123456",
            "assetModelExternalId": "Robot.OEM1.3536"
        },
        {
            "assetExternalId": "Robot.OEM1.3536.987654",
            "assetName": "RobotArm987654",
            "assetModelExternalId": "Robot.OEM1.3536"
        },
        {
            "assetExternalId": "BostonSite.Area1.Line1.WorkCell1",
            "assetName": "WorkCell1",
```

```
            "assetModelExternalId": "ISA95.WorkCell",
            "assetHierarchies": [
                {
                    "externalId": "workCellHierarchyWithOEM1Robot",
                    "childAssetExternalId": "Robot.OEM1.3536.123456"
                },
                {
                    "externalId": "workCellHierarchyWithOEM1Robot",
                    "childAssetExternalId": "Robot.OEM1.3536.987654"
                }
            ]
        }
    ]
}
```

Exemple d'intégration initiale de modèles et d'actifs

Dans cet exemple de scénario, vous avez plusieurs sites de travail qui contiennent des robots industriels dans une entreprise.

L'exemple définit plusieurs modèles d'actifs :

- `Sample_Enterprise`— Ce modèle d'actifs représente l'entreprise dont les sites font partie. Le modèle d'actifs définit une hiérarchie pour représenter la relation entre les sites et l'entreprise. `Enterprise to Site`
- `Sample_Site`— Ce modèle d'actifs représente les sites de fabrication au sein de l'entreprise. Le modèle d'actifs définit une hiérarchie pour représenter la relation entre les lignes et le site. `Site to Line`
- `Sample_Welding Line`— Ce modèle d'actifs représente une chaîne de montage sur les sites de travail. Le modèle d'actifs définit une hiérarchie pour représenter la relation entre les robots et la ligne. `Line to Robot`
- `Sample_Welding Robot`— Ce modèle d'actifs représente un type particulier de robot sur vos sites de travail.

L'exemple définit également les actifs en fonction des modèles d'actifs.

- `Sample_AnyCompany Motor`— Cet actif est créé à partir du modèle `Sample_Enterprise` d'actif.
- `Sample_Chicago`— Cet actif est créé à partir du modèle `Sample_Site` d'actif.

- `Sample_Welding Line 1`— Cet actif est créé à partir du modèle `Sample_Welding Line` d'actif.
- `Sample_Welding Robot 1`— Cet actif est créé à partir du modèle `Sample_Welding Robot` d'actif.
- `Sample_Welding Robot 2`— Cet actif est créé à partir du modèle `Sample_Welding Robot` d'actif.

Le fichier de métadonnées JSON suivant définit ces modèles et actifs d'actifs. L'exécution d'une importation groupée avec ces métadonnées crée les modèles d'actifs et les actifs qu'ils contiennent AWS IoT SiteWise, y compris leurs relations hiérarchiques.

Fichier JSON pour intégrer les actifs et les modèles à importer

```
{
    "assetModels": [
        {
            "assetModelExternalId": "External_Id_Welding_Robot",
            "assetModelName": "Sample_Welding Robot",
            "assetModelProperties": [
                {
                    "dataType": "STRING",
                    "externalId": "External_Id_Welding_Robot_Serial_Number",
                    "name": "Serial Number",
                    "type": {
                        "attribute": {
                            "defaultValue": "-"
                        }
                    },
                    "unit": "-"
                },
                {
                    "dataType": "DOUBLE",
                    "externalId": "External_Id_Welding_Robot_Cycle_Count",
                    "name": "CycleCount",
                    "type": {
                        "measurement": {}
                    },
                    "unit": "EA"
                },
                {
```

```
                    "dataType": "DOUBLE",
                    "externalId": "External_Id_Welding_Robot_Joint_1_Current",
                    "name": "Joint 1 Current",
                    "type": {
                        "measurement": {}
                    },
                    "unit": "Amps"
                },
                {
                    "dataType": "DOUBLE",
                    "externalId": "External_Id_Welding_Robot_Joint_1_Max_Current",
                    "name": "Max Joint 1 Current",
                    "type": {
                        "metric": {
                            "expression": "max(joint1current)",
                            "variables": [
                                {
                                    "name": "joint1current",
                                    "value": {
                                        "propertyExternalId":
"External_Id_Welding_Robot_Joint_1_Current"
                                    }
                                }
                            ],
                            "window": {
                                "tumbling": {
                                    "interval": "5m"
                                }
                            }
                        }
                    },
                    "unit": "Amps"
                }
            ]
        },
        {
            "assetModelExternalId": "External_Id_Welding_Line",
            "assetModelName": "Sample_Welding Line",
            "assetModelProperties": [
                {
                    "dataType": "DOUBLE",
                    "externalId": "External_Id_Welding_Line_Availability",
                    "name": "Availability",
                    "type": {
```

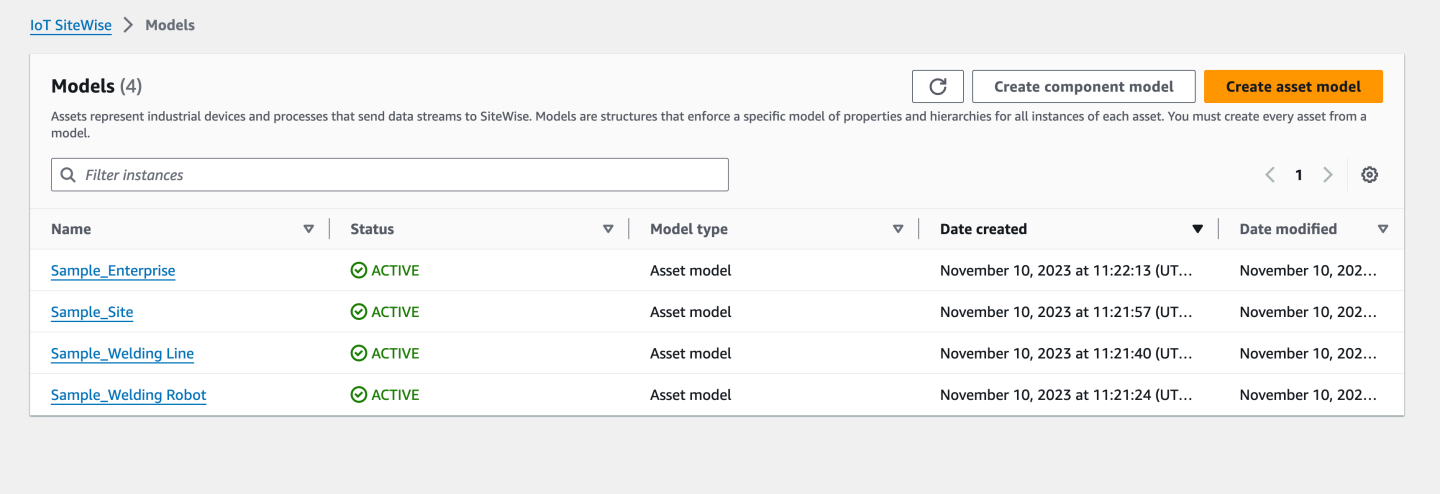
```
                    "measurement": {}
                },
                "unit": "%"
            }
        ],
        "assetModelHierarchies": [
            {
                "externalId": "External_Id_Welding_Line_TO_Robot",
                "name": "Line to Robot",
                "childAssetModelExternalId": "External_Id_Welding_Robot"
            }
        ]
    },
    {
        "assetModelExternalId": "External_Id_Site",
        "assetModelName": "Sample_Site",
        "assetModelProperties": [
            {
                "dataType": "STRING",
                "externalId": "External_Id_Site_Street_Address",
                "name": "Street Address",
                "type": {
                    "attribute": {
                        "defaultValue": "-"
                    }
                },
                "unit": "-"
            }
        ],
        "assetModelHierarchies": [
            {
                "externalId": "External_Id_Site_TO_Line",
                "name": "Site to Line",
                "childAssetModelExternalId": "External_Id_Welding_Line"
            }
        ]
    },
    {
        "assetModelExternalId": "External_Id_Enterprise",
        "assetModelName": "Sample_Enterprise",
        "assetModelProperties": [
            {
                "dataType": "STRING",
                "name": "Company Name",
```

```
                    "externalId": "External_Id_Enterprise_Company_Name",
                    "type": {
                        "attribute": {
                            "defaultValue": "-"
                        }
                    },
                    "unit": "-"
                }
            ],
            "assetModelHierarchies": [
                {
                    "externalId": "External_Id_Enterprise_TO_Site",
                    "name": "Enterprise to Site",
                    "childAssetModelExternalId": "External_Id_Site"
                }
            ]
        }
    ],
    "assets": [
        {
            "assetExternalId": "External_Id_Welding_Robot_1",
            "assetName": "Sample_Welding Robot 1",
            "assetModelExternalId": "External_Id_Welding_Robot",
            "assetProperties": [
                {
                    "externalId": "External_Id_Welding_Robot_Serial_Number",
                    "attributeValue": "S1000"
                },
                {
                    "externalId": "External_Id_Welding_Robot_Cycle_Count",
                    "alias": "AnyCompany/Chicago/Welding Line/S1000/Count"
                },
                {
                    "externalId": "External_Id_Welding_Robot_Joint_1_Current",
                    "alias": "AnyCompany/Chicago/Welding Line/S1000/1/Current"
                }
            ]
        },
        {
            "assetExternalId": "External_Id_Welding_Robot_2",
            "assetName": "Sample_Welding Robot 2",
            "assetModelExternalId": "External_Id_Welding_Robot",
            "assetProperties": [
                {
```

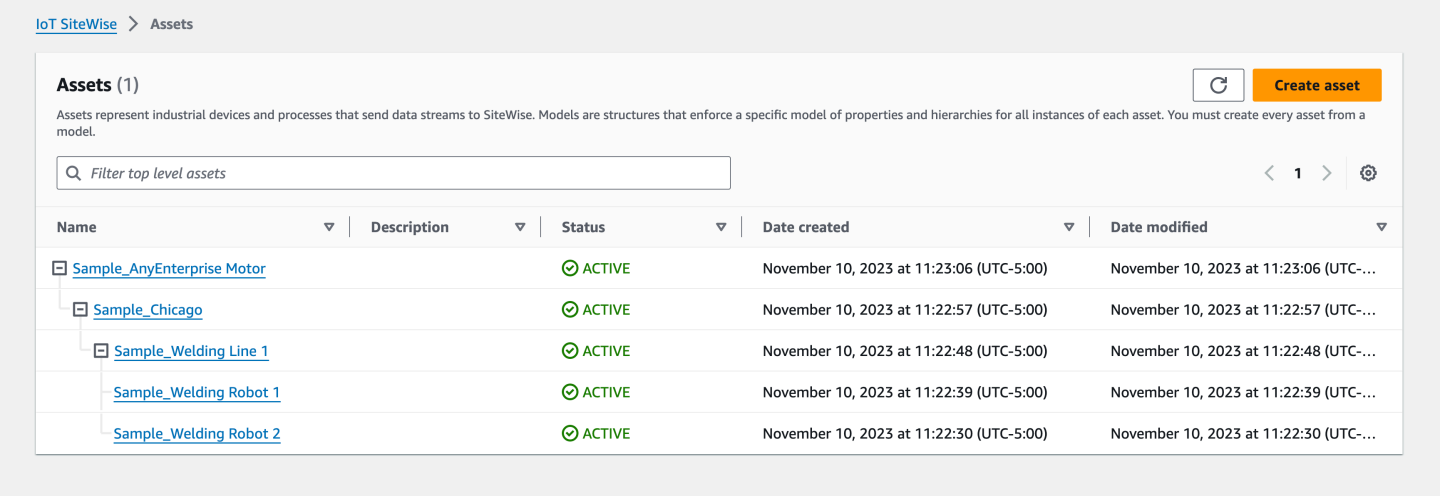
```
                    "externalId": "External_Id_Welding_Robot_Serial_Number",
                    "attributeValue": "S2000"
                },
                {
                    "externalId": "External_Id_Welding_Robot_Cycle_Count",
                    "alias": "AnyCompany/Chicago/Welding Line/S2000/Count"
                },
                {
                    "externalId": "External_Id_Welding_Robot_Joint_1_Current",
                    "alias": "AnyCompany/Chicago/Welding Line/S2000/1/Current"
                }
            ]
        },
        {
            "assetExternalId": "External_Id_Welding_Line_1",
            "assetName": "Sample_Welding Line 1",
            "assetModelExternalId": "External_Id_Welding_Line",
            "assetProperties": [
                {
                    "externalId": "External_Id_Welding_Line_Availability",
                    "alias": "AnyCompany/Chicago/Welding Line/Availability"
                }
            ],
            "assetHierarchies": [
                {
                    "externalId": "External_Id_Welding_Line_TO_Robot",
                    "childAssetExternalId": "External_Id_Welding_Robot_1"
                },
                {
                    "externalId": "External_Id_Welding_Line_TO_Robot",
                    "childAssetExternalId": "External_Id_Welding_Robot_2"
                }
            ]
        },
        {
            "assetExternalId": "External_Id_Site_Chicago",
            "assetName": "Sample_Chicago",
            "assetModelExternalId": "External_Id_Site",
            "assetHierarchies": [
                {
                    "externalId": "External_Id_Site_TO_Line",
                    "childAssetExternalId": "External_Id_Welding_Line_1"
                }
            ]
```

```
        },
        {
            "assetExternalId": "External_Id_Enterprise_AnyCompany",
            "assetName": "Sample_AnyEnterprise Motor",
            "assetModelExternalId": "External_Id_Enterprise",
            "assetHierarchies": [
                {
                    "externalId": "External_Id_Enterprise_TO_Site",
                    "childAssetExternalId": "External_Id_Site_Chicago"
                }
            ]
        }
    ]
}
```

La capture d'écran suivante montre les modèles qui s'affichent Console AWS IoT SiteWise après l'exécution de l'exemple de code précédent.



La capture d'écran suivante montre les modèles, les actifs et les hiérarchies qui s'affichent Console AWS IoT SiteWise après l'exécution de l'exemple de code précédent.



Exemple d'intégration d'actifs supplémentaires

Cet exemple définit les actifs supplémentaires à importer dans un modèle d'actif existant dans votre compte :

- `Sample_Welding Line 2`— Cet actif est créé à partir du modèle `Sample_Welding Line` d'actif.
- `Sample_Welding Robot 3`— Cet actif est créé à partir du modèle `Sample_Welding Robot` d'actif.
- `Sample_Welding Robot 4`— Cet actif est créé à partir du modèle `Sample_Welding Robot` d'actif.

Pour créer les actifs initiaux pour cet exemple, reportez-vous àExemple d'intégration initiale de modèles et d'actifs.

Le fichier de métadonnées JSON suivant définit ces modèles et actifs d'actifs. L'exécution d'une importation groupée avec ces métadonnées crée les modèles d'actifs et les actifs qu'ils contiennent AWS IoT SiteWise, y compris leurs relations hiérarchiques.

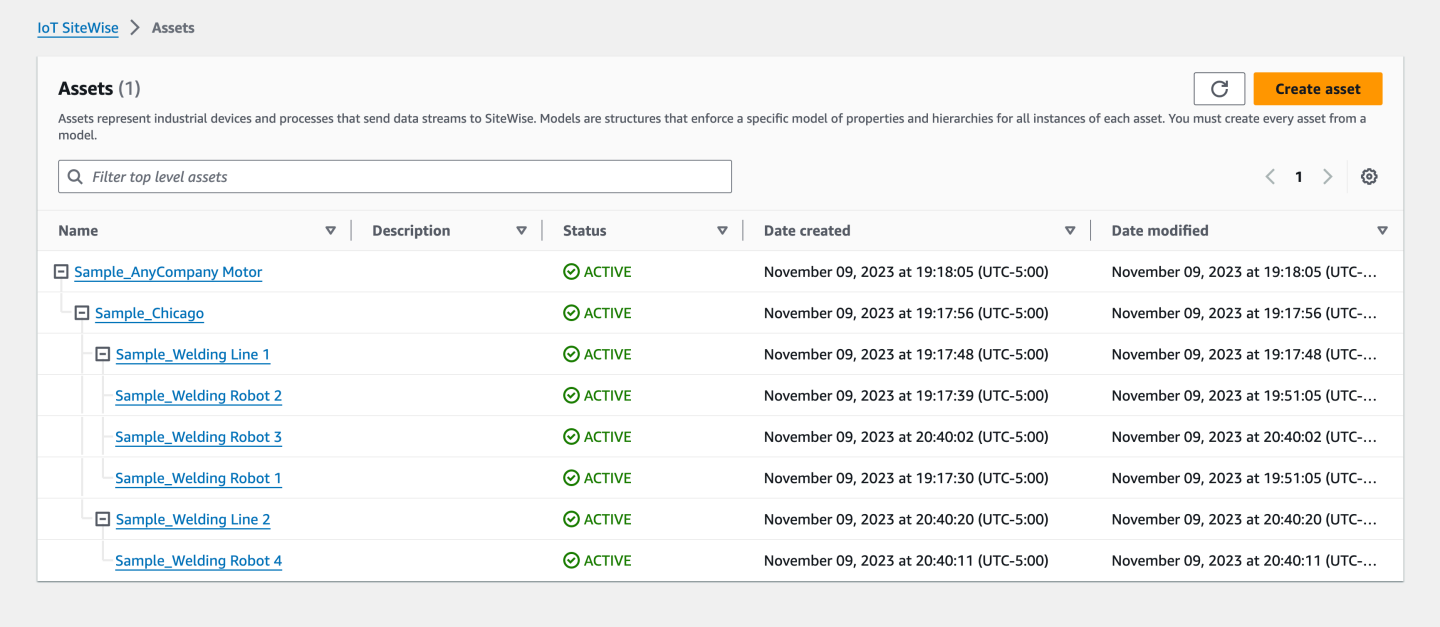
Fichier JSON pour intégrer des ressources supplémentaires

```
{
    "assets": [
        {
            "assetExternalId": "External_Id_Welding_Robot_3",
            "assetName": "Sample_Welding Robot 3",
```

```
            "assetModelExternalId": "External_Id_Welding_Robot",
            "assetProperties": [
                {
                    "externalId": "External_Id_Welding_Robot_Serial_Number",
                    "attributeValue": "S3000"
                },
                {
                    "externalId": "External_Id_Welding_Robot_Cycle_Count",
                    "alias": "AnyCompany/Chicago/Welding Line/S3000/Count"
                },
                {
                    "externalId": "External_Id_Welding_Robot_Joint_1_Current",
                    "alias": "AnyCompany/Chicago/Welding Line/S3000/1/Current"
                }
            ]
        },
        {
            "assetExternalId": "External_Id_Welding_Robot_4",
            "assetName": "Sample_Welding Robot 4",
            "assetModelExternalId": "External_Id_Welding_Robot",
            "assetProperties": [
                {
                    "externalId": "External_Id_Welding_Robot_Serial_Number",
                    "attributeValue": "S4000"
                },
                {
                    "externalId": "External_Id_Welding_Robot_Cycle_Count",
                    "alias": "AnyCompany/Chicago/Welding Line/S4000/Count"
                },
                {
                    "externalId": "External_Id_Welding_Robot_Joint_1_Current",
                    "alias": "AnyCompany/Chicago/Welding Line/S4000/1/Current"
                }
            ]
        },
        {
            "assetExternalId": "External_Id_Welding_Line_1",
            "assetName": "Sample_Welding Line 1",
            "assetModelExternalId": "External_Id_Welding_Line",
            "assetHierarchies": [
                {
                    "externalId": "External_Id_Welding_Line_TO_Robot",
                    "childAssetExternalId": "External_Id_Welding_Robot_1"
                },
```

```
                {
                    "externalId": "External_Id_Welding_Line_TO_Robot",
                    "childAssetExternalId": "External_Id_Welding_Robot_2"
                },
                {
                    "externalId": "External_Id_Welding_Line_TO_Robot",
                    "childAssetExternalId": "External_Id_Welding_Robot_3"
                }
            ]
        },
        {
            "assetExternalId": "External_Id_Welding_Line_2",
            "assetName": "Sample_Welding Line 2",
            "assetModelExternalId": "External_Id_Welding_Line",
            "assetHierarchies": [
                {
                    "externalId": "External_Id_Welding_Line_TO_Robot",
                    "childAssetExternalId": "External_Id_Welding_Robot_4"
                }
            ]
        },
        {
            "assetExternalId": "External_Id_Site_Chicago",
            "assetName": "Sample_Chicago",
            "assetModelExternalId": "External_Id_Site",
            "assetHierarchies": [
                {
                    "externalId": "External_Id_Site_TO_Line",
                    "childAssetExternalId": "External_Id_Welding_Line_1"
                },
                {
                    "externalId": "External_Id_Site_TO_Line",
                    "childAssetExternalId": "External_Id_Welding_Line_2"
                }
            ]
        }
    ]
}
```

La capture d'écran suivante montre les modèles, les actifs et les hiérarchies qui s'affichent Console AWS IoT SiteWise après l'exécution de l'exemple de code précédent.



Exemple d'intégration de nouvelles propriétés

Cet exemple définit de nouvelles propriétés sur les modèles d'actifs existants. Veillez Exemple d'intégration d'actifs supplémentaires à intégrer des actifs et des modèles supplémentaires.

- `Joint 1 Temperature`— Cette propriété est ajoutée au modèle `Sample_Welding Robot` d'actif. Cette nouvelle propriété se propagera également à chaque actif créé à partir du modèle `Sample_Welding Robot` d'actif.

Pour ajouter une nouvelle propriété à un modèle d'actif existant, consultez l'exemple de fichier de métadonnées JSON suivant. Comme indiqué dans le JSON, la définition complète du modèle `Sample_Welding Robot` d'actif existant doit être fournie avec la nouvelle propriété. Si la liste complète des propriétés de la définition existante n'est pas fournie, AWS IoT SiteWise supprime les propriétés omises.

Fichier JSON pour intégrer de nouvelles propriétés

Cet exemple ajoute une nouvelle propriété `Joint 1 Temperature` au modèle d'actif.

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

Exemples de métadonnées d'exportation

Lorsque vous exportez votre AWS IoT SiteWise contenu en masse vers Amazon S3, vous pouvez définir des filtres pour limiter les modèles d'actifs et les actifs spécifiques que vous souhaitez exporter.

Vous spécifiez les filtres dans une `iotSiteWiseConfiguration` section de la `sources` section du corps de votre demande.

> **Note**
>
> Vous pouvez inclure plusieurs filtres. L'opération groupée exportera tout modèle de ressource ou ressource correspondant à l'un des filtres.
> Si vous ne fournissez aucun filtre, l'opération exportera tous vos modèles et actifs d'actifs.

```
{
    "metadataTransferJobId": "your-transfer-job-id",
    "sources": [{
        "type": "iotsitewise",
        "iotSiteWiseConfiguration": {
            "filters": [{
                list of filters
            }]
        }
    }],
    "destination": {
        "type": "s3",
        "s3Configuration": {
            "location": "arn:aws:s3:::your-S3-bucket-location"
        }
    }
}
```

Filtrage par modèle d'actif

Vous pouvez filtrer un modèle d'actif spécifique. Vous pouvez également inclure tous les actifs utilisant ce modèle, ou tous les modèles d'actifs au sein de sa hiérarchie. Vous ne pouvez pas inclure à la fois les actifs et la hiérarchie.

Pour plus d'informations sur les hiérarchies, consultez Définition de hiérarchies de modèles d'actifs.

Asset model

Ce filtre inclut le modèle d'actif spécifié :

```
"filterByAssetModel": {
    "assetModelId": "asset model ID"
}
```

Asset model and its assets

Ce filtre inclut le modèle d'actif spécifié, ainsi que tous les actifs utilisant ce modèle d'actif :

```
"filterByAssetModel": {
    "assetModelId": "asset model ID",
    "includeAssets": true
```

```
}
```

Asset model and its hierarchy

Ce filtre inclut le modèle d'actif spécifié, ainsi que tous les modèles d'actifs associés dans sa hiérarchie :

```
"filterByAssetModel": {
    "assetModelId": "asset model ID",
    "includeOffspring": true
}
```

Filtrer par actif

Vous pouvez filtrer un actif spécifique. Vous pouvez également inclure son modèle d'actif ou tous les actifs associés dans sa hiérarchie. Vous ne pouvez pas inclure à la fois le modèle et la hiérarchie des actifs.

Pour plus d'informations sur les hiérarchies, consultez Définition de hiérarchies de modèles d'actifs.

Asset

Ce filtre inclut l'actif spécifié :

```
"filterByAsset": {
    "assetId": "asset ID"
}
```

Asset and its asset model

Ce filtre inclut l'actif spécifié, ainsi que le modèle d'actif qu'il utilise :

```
"filterByAsset": {
    "assetId": "asset ID",
    "includeAssetModel": true
}
```

Asset and its hierarchy

Ce filtre inclut l'actif spécifié, ainsi que tous les actifs associés dans sa hiérarchie :

```
"filterByAsset": {
    "assetId": "asset ID",
    "includeOffspring": true
}
```

AWS IoT SiteWise schéma de tâche de transfert de métadonnées

Utilisez le schéma des tâches de transfert de AWS IoT SiteWise métadonnées à titre de référence lorsque vous effectuez vos propres opérations d'importation et d'exportation en bloc :

```
{
  "$schema": "https://json-schema.org/draft/2020-12/schema",
  "title": "IoTSiteWise",
  "description": "Metadata transfer job resource schema for IoTSiteWise",
  "definitions": {
    "Name": {
      "type": "string",
      "minLength": 1,
      "maxLength": 256,
      "pattern": "[^\\u0000-\\u001F\\u007F]+"
    },
    "Description": {
      "type": "string",
      "minLength": 1,
      "maxLength": 2048,
      "pattern": "[^\\u0000-\\u001F\\u007F]+"
    },
    "ID": {
      "type": "string",
      "minLength": 36,
      "maxLength": 36,
      "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}$"
    },
    "ExternalId": {
      "type": "string",
      "minLength": 2,
      "maxLength": 128,
      "pattern": "[a-zA-Z0-9_][a-zA-Z_\\-0-9.:]*[a-zA-Z0-9_]+"
    },
    "AttributeValue": {
      "description": "The value of the property attribute.",
```

```
      "type": "string",
      "minLength": 1,
      "maxLength": 1024,
      "pattern": "[^\\u0000-\\u001F\\u007F]+"
    },
    "PropertyUnit": {
      "description": "The unit of measure (such as Newtons or RPM) of the asset
property.",
      "type": "string",
      "minLength": 1,
      "maxLength": 256,
      "pattern": "[^\\u0000-\\u001F\\u007F]+"
    },
    "PropertyAlias": {
      "description": "The property alias that identifies the property.",
      "type": "string",
      "minLength": 1,
      "maxLength": 1000,
      "pattern": "[^\\u0000-\\u001F\\u007F]+"
    },
    "AssetProperty": {
      "description": "The asset property's definition, alias, unit, and notification
state.",
      "type": "object",
      "additionalProperties": false,
      "anyOf": [
        {
          "required": [
            "id"
          ]
        },
        {
          "required": [
            "externalId"
          ]
        }
      ],
      "properties": {
        "id": {
          "description": "The ID of the asset property.",
          "$ref": "#/definitions/ID"
        },
        "externalId": {
          "description": "The ExternalID of the asset property.",
```

```
          "$ref": "#/definitions/ExternalId"
        },
        "alias": {
          "$ref": "#/definitions/PropertyAlias"
        },
        "unit": {
          "$ref": "#/definitions/PropertyUnit"
        },
        "attributeValue": {
          "$ref": "#/definitions/AttributeValue"
        },
        "retainDataOnAliasChange": {
          "type": "string",
          "default": "TRUE",
          "enum": [
            "TRUE",
            "FALSE"
          ]
        },
        "propertyNotificationState": {
          "description": "The MQTT notification state (ENABLED or DISABLED) for this
asset property.",
          "type": "string",
          "enum": [
            "ENABLED",
            "DISABLED"
          ]
        }
      }
    },
    "AssetHierarchy": {
      "description": "A hierarchy specifies allowed parent/child asset relationships.",
      "type": "object",
      "additionalProperties": false,
      "anyOf": [
        {
          "required": [
            "id",
            "childAssetId"
          ]
        },
        {
          "required": [
            "externalId",
```

```
            "childAssetId"
          ]
        },
        {
          "required": [
            "id",
            "childAssetExternalId"
          ]
        },
        {
          "required": [
            "externalId",
            "childAssetExternalId"
          ]
        }
      ],
      "properties": {
        "id": {
          "description": "The ID of a hierarchy in the parent asset's model.",
          "$ref": "#/definitions/ID"
        },
        "externalId": {
          "description": "The ExternalID of a hierarchy in the parent asset's model.",
          "$ref": "#/definitions/ExternalId"
        },
        "childAssetId": {
          "description": "The ID of the child asset to be associated.",
          "$ref": "#/definitions/ID"
        },
        "childAssetExternalId": {
          "description": "The ExternalID of the child asset to be associated.",
          "$ref": "#/definitions/ExternalId"
        }
      }
    },
    "Tag": {
      "type": "object",
      "additionalProperties": false,
      "required": [
        "key",
        "value"
      ],
      "properties": {
        "key": {
```

```
          "type": "string"
        },
        "value": {
          "type": "string"
        }
      }
    },
    "AssetModelType": {
      "type": "string",
      "default": null,
      "enum": [
        "ASSET_MODEL",
        "COMPONENT_MODEL"
      ]
    },
    "AssetModelCompositeModel": {
      "description": "Contains a composite model definition in an asset model. This
composite model definition is applied to all assets created from the asset model.",
      "type": "object",
      "additionalProperties": false,
      "anyOf": [
        {
          "required": [
            "id"
          ]
        },
        {
          "required": [
            "externalId"
          ]
        }
      ],
      "required": [
        "name",
        "type"
      ],
      "properties": {
        "id": {
          "description": "The ID of the asset model composite model.",
          "$ref": "#/definitions/ID"
        },
        "externalId": {
          "description": "The ExternalID of the asset model composite model.",
          "$ref": "#/definitions/ExternalId"
```

```
        },
        "parentId": {
          "description": "The ID of the parent asset model composite model.",
          "$ref": "#/definitions/ID"
        },
        "parentExternalId": {
          "description": "The ExternalID of the parent asset model composite model.",
          "$ref": "#/definitions/ExternalId"
        },
        "composedAssetModelId": {
          "description": "The ID of the composed asset model.",
          "$ref": "#/definitions/ID"
        },
        "composedAssetModelExternalId": {
          "description": "The ExternalID of the composed asset model.",
          "$ref": "#/definitions/ExternalId"
        },
        "description": {
          "description": "A description for the asset composite model.",
          "$ref": "#/definitions/Description"
        },
        "name": {
          "description": "A unique, friendly name for the asset composite model.",
          "$ref": "#/definitions/Name"
        },
        "type": {
          "description": "The type of the composite model. For alarm composite models,
this type is AWS/ALARM.",
          "$ref": "#/definitions/Name"
        },
        "properties": {
          "description": "The property definitions of the asset model.",
          "type": "array",
          "items": {
            "$ref": "#/definitions/AssetModelProperty"
          }
        }
      }
    },
    "AssetModelProperty": {
      "description": "Contains information about an asset model property.",
      "type": "object",
      "additionalProperties": false,
      "anyOf": [
```

```
        {
          "required": [
            "id"
          ]
        },
        {
          "required": [
            "externalId"
          ]
        }
      ],
      "required": [
        "name",
        "dataType",
        "type"
      ],
      "properties": {
        "id": {
          "description": "The ID of the asset model property.",
          "$ref": "#/definitions/ID"
        },
        "externalId": {
          "description": "The ExternalID of the asset model property.",
          "$ref": "#/definitions/ExternalId"
        },
        "name": {
          "description": "The name of the asset model property.",
          "$ref": "#/definitions/Name"
        },
        "dataType": {
          "description": "The data type of the asset model property.",
          "$ref": "#/definitions/DataType"
        },
        "dataTypeSpec": {
          "description": "The data type of the structure for this property.",
          "$ref": "#/definitions/Name"
        },
        "unit": {
          "description": "The unit of the asset model property, such as Newtons or
RPM.",
          "type": "string",
          "minLength": 1,
          "maxLength": 256,
          "pattern": "[^\\u0000-\\u001F\\u007F]+"
```

```
        },
        "type": {
          "description": "The property type",
          "$ref": "#/definitions/PropertyType"
        }
      }
    },
    "DataType": {
      "type": "string",
      "enum": [
        "STRING",
        "INTEGER",
        "DOUBLE",
        "BOOLEAN",
        "STRUCT"
      ]
    },
    "PropertyType": {
      "description": "Contains a property type, which can be one of attribute,
 measurement, metric, or transform.",
      "type": "object",
      "additionalProperties": false,
      "properties": {
        "attribute": {
          "$ref": "#/definitions/Attribute"
        },
        "transform": {
          "$ref": "#/definitions/Transform"
        },
        "metric": {
          "$ref": "#/definitions/Metric"
        },
        "measurement": {
          "$ref": "#/definitions/Measurement"
        }
      }
    },
    "Attribute": {
      "type": "object",
      "additionalProperties": false,
      "properties": {
        "defaultValue": {
          "type": "string",
          "minLength": 1,
```

```
          "maxLength": 1024,
          "pattern": "[^\\u0000-\\u001F\\u007F]+"
        }
      }
    },
    "Transform": {
      "type": "object",
      "additionalProperties": false,
      "required": [
        "expression",
        "variables"
      ],
      "properties": {
        "expression": {
          "description": "The mathematical expression that defines the transformation
function.",
          "type": "string",
          "minLength": 1,
          "maxLength": 1024
        },
        "variables": {
          "description": "The list of variables used in the expression.",
          "type": "array",
          "items": {
            "$ref": "#/definitions/ExpressionVariable"
          }
        },
        "processingConfig": {
          "$ref": "#/definitions/TransformProcessingConfig"
        }
      }
    },
    "TransformProcessingConfig": {
      "description": "The processing configuration for the given transform property.",
      "type": "object",
      "additionalProperties": false,
      "required": [
        "computeLocation"
      ],
      "properties": {
        "computeLocation": {
          "description": "The compute location for the given transform property.",
          "$ref": "#/definitions/ComputeLocation"
        },
```

```
        "forwardingConfig": {
          "description": "The forwarding configuration for a given property.",
          "$ref": "#/definitions/ForwardingConfig"
        }
      }
    },
    "Metric": {
      "type": "object",
      "additionalProperties": false,
      "required": [
        "expression",
        "variables",
        "window"
      ],
      "properties": {
        "expression": {
          "description": "The mathematical expression that defines the metric
aggregation function.",
          "type": "string",
          "minLength": 1,
          "maxLength": 1024
        },
        "variables": {
          "description": "The list of variables used in the expression.",
          "type": "array",
          "items": {
            "$ref": "#/definitions/ExpressionVariable"
          }
        },
        "window": {
          "description": "The window (time interval) over which AWS IoT SiteWise
computes the metric's aggregation expression",
          "$ref": "#/definitions/MetricWindow"
        },
        "processingConfig": {
          "$ref": "#/definitions/MetricProcessingConfig"
        }
      }
    },
    "MetricProcessingConfig": {
      "description": "The processing configuration for the metric.",
      "type": "object",
      "additionalProperties": false,
      "required": [
```

```
        "computeLocation"
      ],
      "properties": {
        "computeLocation": {
          "description": "The compute location for the given metric property.",
          "$ref": "#/definitions/ComputeLocation"
        }
      }
    },
    "ComputeLocation": {
      "type": "string",
      "enum": [
        "EDGE",
        "CLOUD"
      ]
    },
    "ForwardingConfig": {
      "type": "object",
      "additionalProperties": false,
      "required": [
        "state"
      ],
      "properties": {
        "state": {
          "type": "string",
          "enum": [
            "ENABLED",
            "DISABLED"
          ]
        }
      }
    },
    "MetricWindow": {
      "description": "Contains a time interval window used for data aggregate
computations (for example, average, sum, count, and so on).",
      "type": "object",
      "additionalProperties": false,
      "properties": {
        "tumbling": {
          "description": "The tumbling time interval window.",
          "type": "object",
          "additionalProperties": false,
          "required": [
            "interval"
```

```
          ],
          "properties": {
            "interval": {
              "description": "The time interval for the tumbling window.",
              "type": "string",
              "minLength": 2,
              "maxLength": 23
            },
            "offset": {
              "description": "The offset for the tumbling window.",
              "type": "string",
              "minLength": 2,
              "maxLength": 25
            }
          }
        }
      }
    },
    "ExpressionVariable": {
      "type": "object",
      "additionalProperties": false,
      "required": [
        "name",
        "value"
      ],
      "properties": {
        "name": {
          "description": "The friendly name of the variable to be used in the
expression.",
          "type": "string",
          "minLength": 1,
          "maxLength": 64,
          "pattern": "^[a-z][a-z0-9_]*$"
        },
        "value": {
          "description": "The variable that identifies an asset property from which to
use values.",
          "$ref": "#/definitions/VariableValue"
        }
      }
    },
    "VariableValue": {
      "type": "object",
      "additionalProperties": false,
```

```
      "anyOf": [
        {
          "required": [
            "propertyId"
          ]
        },
        {
          "required": [
            "propertyExternalId"
          ]
        }
      ],
      "properties": {
        "propertyId": {
          "$ref": "#/definitions/ID"
        },
        "propertyExternalId": {
          "$ref": "#/definitions/ExternalId"
        },
        "hierarchyId": {
          "$ref": "#/definitions/ID"
        },
        "hierarchyExternalId": {
          "$ref": "#/definitions/ExternalId"
        }
      }
    },
    "Measurement": {
      "type": "object",
      "additionalProperties": false,
      "properties": {
        "processingConfig": {
          "$ref": "#/definitions/MeasurementProcessingConfig"
        }
      }
    },
    "MeasurementProcessingConfig": {
      "type": "object",
      "additionalProperties": false,
      "required": [
        "forwardingConfig"
      ],
      "properties": {
        "forwardingConfig": {
```

```
          "description": "The forwarding configuration for the given measurement
property.",
          "$ref": "#/definitions/ForwardingConfig"
        }
      }
    },
    "AssetModelHierarchy": {
      "description": "Contains information about an asset model hierarchy.",
      "type": "object",
      "additionalProperties": false,
      "anyOf": [
        {
          "required": [
            "id",
            "childAssetModelId"
          ]
        },
        {
          "required": [
            "id",
            "childAssetModelExternalId"
          ]
        },
        {
          "required": [
            "externalId",
            "childAssetModelId"
          ]
        },
        {
          "required": [
            "externalId",
            "childAssetModelExternalId"
          ]
        }
      ],
      "required": [
        "name"
      ],
      "properties": {
        "id": {
          "description": "The ID of the asset model hierarchy.",
          "$ref": "#/definitions/ID"
        },
```

```
        "externalId": {
          "description": "The ExternalID of the asset model hierarchy.",
          "$ref": "#/definitions/ExternalId"
        },
        "name": {
          "description": "The name of the asset model hierarchy.",
          "$ref": "#/definitions/Name"
        },
        "childAssetModelId": {
          "description": "The ID of the asset model. All assets in this hierarchy must
be instances of the child AssetModelId asset model.",
          "$ref": "#/definitions/ID"
        },
        "childAssetModelExternalId": {
          "description": "The ExternalID of the asset model. All assets in this
hierarchy must be instances of the child AssetModelId asset model.",
          "$ref": "#/definitions/ExternalId"
        }
      }
    },
    "AssetModel": {
      "type": "object",
      "additionalProperties": false,
      "anyOf": [
        {
          "required": [
            "assetModelId"
          ]
        },
        {
          "required": [
            "assetModelExternalId"
          ]
        }
      ],
      "required": [
        "assetModelName"
      ],
      "properties": {
        "assetModelId": {
          "description": "The ID of the asset model.",
          "$ref": "#/definitions/ID"
        },
        "assetModelExternalId": {
```

```
          "description": "The ID of the asset model.",
          "$ref": "#/definitions/ExternalId"
        },
        "assetModelName": {
          "description": "A unique, friendly name for the asset model.",
          "$ref": "#/definitions/Name"
        },
        "assetModelDescription": {
          "description": "A description for the asset model.",
          "$ref": "#/definitions/Description"
        },
        "assetModelType": {
          "description": "The type of the asset model.",
          "$ref": "#/definitions/AssetModelType"
        },
        "assetModelProperties": {
          "description": "The property definitions of the asset model.",
          "type": "array",
          "items": {
            "$ref": "#/definitions/AssetModelProperty"
          }
        },
        "assetModelCompositeModels": {
          "description": "The composite asset models that are part of this asset model.
Composite asset models are asset models that contain specific properties.",
          "type": "array",
          "items": {
            "$ref": "#/definitions/AssetModelCompositeModel"
          }
        },
        "assetModelHierarchies": {
          "description": "The hierarchy definitions of the asset model. Each hierarchy
specifies an asset model whose assets can be children of any other assets created from
this asset model.",
          "type": "array",
          "items": {
            "$ref": "#/definitions/AssetModelHierarchy"
          }
        },
        "tags": {
          "description": "A list of key-value pairs that contain metadata for the asset
model.",
          "type": "array",
          "items": {
```

```
            "$ref": "#/definitions/Tag"
          }
        }
      }
    },
    "Asset": {
      "type": "object",
      "additionalProperties": false,
      "anyOf": [
        {
          "required": [
            "assetId",
            "assetModelId"
          ]
        },
        {
          "required": [
            "assetExternalId",
            "assetModelId"
          ]
        },
        {
          "required": [
            "assetId",
            "assetModelExternalId"
          ]
        },
        {
          "required": [
            "assetExternalId",
            "assetModelExternalId"
          ]
        }
      ],
      "required": [
        "assetName"
      ],
      "properties": {
        "assetId": {
          "description": "The ID of the asset",
          "$ref": "#/definitions/ID"
        },
        "assetExternalId": {
          "description": "The external ID of the asset",
```

```
          "$ref": "#/definitions/ExternalId"
        },
        "assetModelId": {
          "description": "The ID of the asset model from which to create the asset.",
          "$ref": "#/definitions/ID"
        },
        "assetModelExternalId": {
          "description": "The ExternalID of the asset model from which to create the
asset.",
          "$ref": "#/definitions/ExternalId"
        },
        "assetName": {
          "description": "A unique, friendly name for the asset.",
          "$ref": "#/definitions/Name"
        },
        "assetDescription": {
          "description": "A description for the asset",
          "$ref": "#/definitions/Description"
        },
        "assetProperties": {
          "type": "array",
          "items": {
            "$ref": "#/definitions/AssetProperty"
          }
        },
        "assetHierarchies": {
          "type": "array",
          "items": {
            "$ref": "#/definitions/AssetHierarchy"
          }
        },
        "tags": {
          "description": "A list of key-value pairs that contain metadata for the
asset.",
          "type": "array",
          "uniqueItems": false,
          "items": {
            "$ref": "#/definitions/Tag"
          }
        }
      }
    }
  },
  "additionalProperties": false,
```

```
  "properties": {
    "assetModels": {
      "type": "array",
      "uniqueItems": false,
      "items": {
        "$ref": "#/definitions/AssetModel"
      }
    },
    "assets": {
      "type": "array",
      "uniqueItems": false,
      "items": {
        "$ref": "#/definitions/Asset"
      }
    }
  }
}
```

Surveillance des données à l'aide d'alarmes

Vous pouvez configurer des alarmes pour vos données afin d'avertir votre équipe lorsque l'équipement ou les processus ne fonctionnent pas de manière optimale. Les performances optimales d'une machine ou d'un procédé signifient que les valeurs de certaines métriques doivent se situer dans une plage de limites élevées et basses. Lorsque ces mesures sont en dehors de leur plage de fonctionnement, les opérateurs d'équipement doivent être avertis afin qu'ils puissent résoudre le problème. Utilisez les alarmes pour identifier rapidement les problèmes et avertir les opérateurs afin d'optimiser les performances de votre équipement et de vos processus.

Rubriques

- Types d'alarmes
- États d'alarme
- Propriétés de l'état de l'alarme
- Définition des alarmes sur les modèles d'actifs
- Configuration des alarmes sur les actifs
- Répondre aux alarmes
- Ingestion de l'état d'alarme externe

Types d'alarmes

Vous pouvez définir des alarmes qui sont détectées dans le AWS cloud et des alarmes que vous détectez à l'aide de processus externes. AWS IoT SiteWise prend en charge les types d'alarmes suivants :

- AWS IoT Events alarmes

  AWS IoT Events les alarmes sont des alarmes qui détectent AWS IoT Events. AWS IoT SiteWise envoie les valeurs des propriétés des actifs à un modèle d'alarme dans AWS IoT Events. AWS IoT Events Envoie ensuite l'état d'alarme à AWS IoT SiteWise. Vous pouvez configurer des options telles que le moment où l'alarme est détectée et les personnes à avertir lorsque l'état de l'alarme change. Vous pouvez également définir les AWS IoT Events actions qui se produisent lorsque l'état de l'alarme change.

Les alarmes in AWS IoT Events sont des instances de modèles d'alarme. Le modèle d'alarme indique le seuil et la gravité de l'alarme, ce qu'il faut faire lorsque l'état de l'alarme change, etc. Lorsque vous configurez chaque caractéristique du modèle d'alarme, vous spécifiez une propriété d'attribut à partir du modèle d'actif surveillé par l'alarme. Tous les actifs basés sur le modèle d'actif utilisent la valeur de l'attribut lors de l' AWS IoT Events évaluation de cette caractéristique de l'alarme. Pour plus d'informations, consultez la section Utilisation des alarmes dans le Guide du AWS IoT Events développeur.

Vous pouvez répondre à une AWS IoT Events alarme lorsqu'elle change d'état. Par exemple, vous pouvez accuser réception ou suspendre une alarme lorsqu'elle devient active. Vous pouvez également activer, désactiver et réinitialiser les alarmes.

SiteWise Les utilisateurs de Monitor peuvent visualiser, configurer et répondre aux AWS IoT Events alarmes dans les portails SiteWise Monitor. Pour plus d'informations, consultez la section Surveillance par alarmes dans le guide AWS IoT SiteWise Monitor d'application.

> **Note**
>
> AWS IoT Events des frais s'appliquent pour évaluer ces alarmes et transférer des données entre AWS IoT SiteWise et AWS IoT Events. Pour en savoir plus, consultez AWS IoT Events Tarification.

- Alarmes externes

  Les alarmes externes sont des alarmes que vous évaluez en dehors de celles-ci AWS IoT SiteWise. Utilisez des alarmes externes si vous disposez d'une source de données signalant l'état des alarmes. L'alarme externe contient une propriété de mesure dans laquelle vous ingérez les données d'état de l'alarme.

  Vous ne pouvez pas accuser réception ou suspendre une alarme externe lorsqu'elle change d'état.

  SiteWise Les utilisateurs de Monitor peuvent voir l'état des alarmes externes dans les portails SiteWise Monitor, mais ils ne peuvent ni configurer ces alarmes ni y répondre.

  AWS IoT SiteWise n'évalue pas l'état des alarmes externes.

États d'alarme

Les alarmes industrielles incluent des informations sur l'état de l'équipement ou du processus qu'elles surveillent et des informations (facultatives) sur la réponse de l'opérateur à l'état d'alarme.

Lorsque vous définissez une AWS IoT Events alarme, vous indiquez s'il faut activer ou non le flux d'accusé de réception. Le flux d'accusé de réception est activé par défaut. Lorsque vous activez cette option, les opérateurs peuvent accuser réception de l'alarme et laisser une note contenant des détails sur l'alarme ou les mesures qu'ils ont prises pour y remédier. Si un opérateur n'accuse pas réception d'une alarme active avant qu'elle ne devienne inactive, l'alarme se verrouille. L'état verrouillé indique que l'alarme est devenue active et n'a pas été confirmée. L'opérateur doit donc vérifier l'équipement ou le processus et accuser réception de l'alarme verrouillée.

Les alarmes présentent les états suivants :

- Normal (`Normal`) — L'alarme est activée mais inactive. Le procédé ou l'équipement industriel fonctionne comme prévu.
- Active (`Active`) — L'alarme est active. Le procédé ou l'équipement industriel se situe en dehors de sa plage de fonctionnement et nécessite une attention particulière.
- Reconnu (`Acknowledged`) — Un opérateur a confirmé l'état de l'alarme.

  Cet état s'applique uniquement aux alarmes pour lesquelles vous activez le flux d'accusé de réception.
- Verrouillé (`Latched`) — L'alarme est revenue à la normale mais elle était active et aucun opérateur ne l'a reconnue. Le processus ou l'équipement industriel nécessite l'attention d'un opérateur pour remettre l'alarme à la normale.

  Cet état s'applique uniquement aux alarmes pour lesquelles vous activez le flux d'accusé de réception.
- Snoozed (`SnoozeDisabled`) — L'alarme est désactivée car un opérateur l'a mise en veille. L'opérateur définit la durée pendant laquelle l'alarme se met en veille. Après cette durée, l'alarme revient à l'état normal.
- Désactivé (`Disabled`) — L'alarme est désactivée et ne sera pas détectée.

Propriétés de l'état de l'alarme

AWS IoT SiteWise stocke les données d'état d'alarme sous forme d'objet JSON sérialisé sous forme de chaîne. Cet objet contient l'état et des informations supplémentaires sur l'alarme, telles que les actions de réponse de l'opérateur et la règle évaluée par l'alarme.

Vous identifiez la propriété d'état de l'alarme par son nom et son type de structure,`AWS/ALARM_STATE`. Pour plus d'informations, consultez Définition des alarmes sur les modèles d'actifs.

L'objet de données d'état de l'alarme contient les informations suivantes :

`stateName`

État de l'alarme. Pour plus d'informations, consultez États d'alarme.

Type de données : `STRING`

`customerAction`

(Facultatif) Objet contenant des informations sur la réponse de l'opérateur à l'alarme. Les opérateurs peuvent activer, désactiver, accuser réception et suspendre les alarmes. Lorsqu'ils le font, les données d'état de l'alarme incluent leur réponse et la note qu'ils peuvent laisser lorsqu'ils répondent. Cet objet contient les informations suivantes :

`actionName`

Nom de l'action entreprise par l'opérateur pour répondre à l'alarme. Cette valeur contient l'une des chaînes suivantes :

- `ENABLE`
- `DISABLE`
- `SNOOZE`
- `ACKNOWLEDGE`
- `RESET`

Type de données : `STRING`

`enable`

(Facultatif) Objet présent `customerAction` lorsque l'opérateur active l'alarme. Lorsqu'un opérateur active l'alarme, l'état de l'alarme passe à`Normal`. Cet objet contient les informations suivantes :

`note`

(Facultatif) La note que le client quitte lorsqu'il active l'alarme.

Type de données : `STRING`

Longueur maximale : 128 caractères

`disable`

(Facultatif) Objet présent `customerAction` lorsque l'opérateur désactive l'alarme. Lorsqu'un opérateur active l'alarme, l'état de l'alarme passe à`Disabled`. Cet objet contient les informations suivantes :

`note`

(Facultatif) La note que le client quitte lorsqu'il désactive l'alarme.

Type de données : `STRING`

Longueur maximale : 128 caractères

`acknowledge`

(Facultatif) Objet présent `customerAction` lorsque l'opérateur confirme l'alarme. Lorsqu'un opérateur active l'alarme, l'état de l'alarme passe à`Acknowledged`. Cet objet contient les informations suivantes :

`note`

(Facultatif) La note que le client quitte lorsqu'il accuse réception de l'alarme.

Type de données : `STRING`

Longueur maximale : 128 caractères

`snooze`

(Facultatif) Objet présent `customerAction` lorsque l'opérateur déclenche l'alarme. Lorsqu'un opérateur active l'alarme, l'état de l'alarme passe à`SnoozeDisabled`. Cet objet contient les informations suivantes :

`snoozeDuration`

Durée en secondes pendant laquelle l'opérateur met l'alarme en veille. L'alarme passe à `Normal` l'état après cette durée.

Type de données : `INTEGER`

`note`

(Facultatif) La note que le client quitte lorsqu'il met l'alarme en veille.

Type de données : `STRING`

Longueur maximale : 128 caractères

`ruleEvaluation`

(Facultatif) Objet contenant des informations sur la règle qui évalue l'alarme. Cet objet contient les informations suivantes :

`simpleRule`

Objet contenant des informations relatives à une règle simple, qui compare la valeur d'une propriété à une valeur de seuil à l'aide d'un opérateur de comparaison. Cet objet contient les informations suivantes :

`inputProperty`

Valeur de la propriété évaluée par cette alarme.

Type de données : `DOUBLE`

`operator`

L'opérateur de comparaison utilisé par cette alarme pour comparer la propriété au seuil. Cette valeur contient l'une des chaînes suivantes :

- <— Inférieur à
- <=— Inférieur ou égal
- ==— Égal
- !=— Pas égal
- >=— Supérieur ou égal
- >— Supérieur à

Type de données : `STRING`

`threshold`

La valeur de seuil à laquelle cette alarme compare la valeur de la propriété.

Type de données : `DOUBLE`

Définition des alarmes sur les modèles d'actifs

Les modèles d'actifs favorisent la standardisation de vos données industrielles et de vos alarmes. Vous pouvez définir des définitions d'alarmes sur les modèles d'actifs afin de standardiser les alarmes pour tous les actifs en fonction d'un modèle d'actif.

Vous utilisez des modèles d'actifs composites pour définir des alarmes sur les modèles d'actifs. Les modèles d'actifs composites sont des modèles d'actifs qui normalisent un ensemble spécifique de propriétés sur un autre modèle d'actif. Les modèles d'actifs composites garantissent la présence de certaines propriétés sur un modèle d'actif. Les alarmes ont des propriétés de type, d'état et (facultatives) de source, de sorte que le modèle composite d'alarme garantit l'existence de ces propriétés.

Chaque modèle d'actif composite possède un type qui définit les propriétés de ce modèle composite. Les modèles composites d'alarme définissent les propriétés du type d'alarme, de l'état de l'alarme et de la source d'alarme (en option). Lorsque vous créez un actif à partir d'un modèle d'actif avec des modèles composites, l'actif inclut les propriétés du modèle composite ainsi que les propriétés que vous spécifiez dans le modèle d'actif.

Chaque propriété d'un modèle composite doit porter le nom qui l'identifie pour son type de modèle composite. Les propriétés du modèle composite prennent en charge les propriétés contenant des types de données complexes. Ces propriétés ont le type de `STRUCT` données et un `dataTypeSpec` trait qui spécifie le type de données complexe de la propriété. Les propriétés de type de données complexes contiennent des données JSON sérialisées sous forme de chaînes.

Les modèles composites d'alarme présentent les propriétés suivantes. Chaque propriété doit porter le nom qui l'identifie pour ce type de modèle composite.

Type d'alarme

Type d'alarme. Spécifiez l'un des éléments suivants :

- `IOT_EVENTS`— Une AWS IoT Events alarme. AWS IoT SiteWise envoie des données AWS IoT Events à pour évaluer l'état de cette alarme. Vous devez spécifier la propriété de la source d'alarme pour définir le modèle AWS IoT Events d'alarme pour cette définition d'alarme.
- `EXTERNAL`— Une alarme externe. Vous ingérez l'état de l'alarme sous forme de mesure.

Nom de la propriété : `AWS/ALARM_TYPE`

Type de propriété : attribut

Type de données : `STRING`

État de l'alarme

Les données chronologiques relatives à l'état de l'alarme. Il s'agit d'un objet sérialisé sous forme de chaîne contenant l'état et d'autres informations relatives à l'alarme. Pour plus d'informations, consultez Propriétés de l'état de l'alarme.

Nom de la propriété : `AWS/ALARM_STATE`

Type de propriété : mesure

Type de données : `STRUCT`

Type de structure de données : `AWS/ALARM_STATE`

Source d'alarme

(Facultatif) Le nom de ressource Amazon (ARN) de la ressource qui évalue l'état de l'alarme. Pour les AWS IoT Events alarmes, il s'agit de l'ARN du modèle d'alarme.

Nom de la propriété : `AWS/ALARM_SOURCE`

Type de propriété : attribut

Type de données : `STRING`

Example Exemple de modèle composite d'alarme

Le modèle d'actif suivant représente une chaudière dotée d'une alarme pour surveiller sa température. AWS IoT SiteWise envoie les données de température AWS IoT Events pour détecter l'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": {}
          }
        }
      ]
    }
```

```
  ]
}
```

Rubriques

- Définition des AWS IoT Events alarmes
- Définition des alarmes externes

Définition des AWS IoT Events alarmes

Lorsque vous créez une AWS IoT Events alarme, AWS IoT SiteWise envoie les valeurs des propriétés des actifs AWS IoT Events à pour évaluer l'état de l'alarme. AWS IoT Events les définitions des alarmes dépendent du modèle d'alarme dans lequel vous les définissez AWS IoT Events. Pour définir une AWS IoT Events alarme sur un modèle d'actif, vous définissez un modèle composite d'alarme qui spécifie le modèle AWS IoT Events d'alarme comme propriété de source d'alarme.

AWS IoT Events les alarmes dépendent d'entrées telles que les seuils d'alarme et les paramètres de notification des alarmes. Vous définissez ces entrées sous forme d'attributs dans le modèle d'actif. Vous pouvez ensuite personnaliser ces entrées pour chaque ressource en fonction du modèle. La AWS IoT SiteWise console peut créer ces attributs pour vous. Si vous définissez des alarmes avec l'API AWS CLI or, vous devez définir manuellement ces attributs sur le modèle d'actif.

Vous pouvez également définir d'autres actions qui se produisent lorsque votre alarme est détectée, telles que des actions de notification d'alarme personnalisées. Par exemple, vous pouvez configurer une action qui envoie une notification push à une rubrique Amazon SNS. Pour plus d'informations sur les actions que vous pouvez définir, consultez la section Utilisation d'autres AWS services dans le Guide du AWS IoT Events développeur.

Lorsque vous mettez à jour ou supprimez un modèle d'actif, vous AWS IoT SiteWise pouvez vérifier si un modèle d'alarme AWS IoT Events surveille une propriété d'actif associée à ce modèle d'actif. Cela vous empêche de supprimer une propriété de ressource actuellement AWS IoT Events utilisée par une alarme. Pour activer cette fonctionnalité dans AWS IoT SiteWise, vous devez avoir l'`iotevents:ListInputRoutings`autorisation. Cette autorisation permet de passer AWS IoT SiteWise des appels à l'opération de l'API ListInputRoutings prise en charge par AWS IoT Events. Pour plus d'informations, consultez ListInputRoutings Autorisation (facultative).

> **Note**
>
> La fonction de notification d'alarme n'est pas disponible dans la région Chine (Pékin).

Rubriques

- Exigences relatives aux notifications d'alarme
- Définition d'une AWS IoT Events alarme (AWS IoT SiteWise console)
- Définition d'une AWS IoT Events alarme (AWS IoT Events console)
- Définition d'une AWS IoT Events alarme (AWS CLI)

Exigences relatives aux notifications d'alarme

AWS IoT Events utilise une AWS Lambda fonction de votre AWS compte pour envoyer des notifications d'alarme. Vous devez créer cette fonction Lambda dans la même AWS région que vos alarmes pour activer les notifications d'alarme. Cette fonction Lambda utilise Amazon Simple Notification Service (Amazon SNS) pour envoyer des notifications par SMS et Amazon Simple Email Service (Amazon SES) pour envoyer des notifications par e-mail. Lorsque vous créez l' AWS IoT Events alarme, vous configurez les protocoles et les paramètres utilisés par l'alarme pour envoyer des notifications.

AWS IoT Events fournit un modèle de AWS CloudFormation pile que vous pouvez utiliser pour créer cette fonction Lambda dans votre compte. Pour plus d'informations, consultez la section Fonction Lambda de notification d'alarme dans le Guide du AWS IoT Events développeur.

Définition d'une AWS IoT Events alarme (AWS IoT SiteWise console)

Vous pouvez utiliser la AWS IoT SiteWise console pour définir une AWS IoT Events alarme sur un modèle d'actif existant. Pour définir une AWS IoT Events alarme sur un nouveau modèle d'actif, créez le modèle d'actif, puis procédez comme suit. Pour plus d'informations, consultez Création de modèles de ressources.

> **Important**
>
> Chaque alarme nécessite un attribut qui spécifie la valeur de seuil à comparer pour l'alarme. Vous devez définir l'attribut de valeur seuil sur le modèle d'actif avant de pouvoir définir une alarme.

Prenons un exemple où vous souhaitez définir une alarme qui détecte lorsqu'une éolienne dépasse sa vitesse nominale maximale de 50 mi/h. Avant de définir l'alarme, vous devez définir un attribut (Vitesse maximale du vent) avec une valeur par défaut de`50`.

Pour définir une AWS IoT Events alarme sur un modèle d'actif

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Models (Modèles).
3. Choisissez le modèle d'actif pour lequel vous souhaitez définir une alarme.
4. Choisissez l'onglet Alarme.
5. Choisissez Ajouter une alarme.
6. Dans la section Options du type d'alarme, choisissez AWS IoT Events alarme.
7. Dans la section Détails de l'alarme, procédez comme suit :
   a. Saisissez un nom pour votre alarme.
   b. (Facultatif) Entrez une description pour votre alarme.
8. Dans la section Définitions des seuils, vous définissez le moment où l'alarme est détectée et la gravité de l'alarme. Procédez comme suit :
   a. Sélectionnez la propriété sur laquelle l'alarme est détectée. Chaque fois que cette propriété reçoit une nouvelle valeur, elle AWS IoT SiteWise envoie la valeur AWS IoT Events à pour évaluer l'état de l'alarme.
   b. Sélectionnez l'opérateur à utiliser pour comparer la propriété à la valeur de seuil. Sélectionnez parmi les options suivantes :
      - < inférieur à
      - <= inférieur ou égal
      - == égal
      - ! = différent
      - >= supérieur ou égal
      - > supérieur à
   c. Pour Valeur, sélectionnez la propriété d'attribut à utiliser comme valeur de seuil. AWS IoT Events compare la valeur de la propriété avec la valeur de cet attribut.

d. Entrez le niveau de gravité de l'alarme. Utilisez un chiffre que votre équipe comprend pour refléter la gravité de cette alarme.

9. (Facultatif) Dans la section Paramètres de notification - facultatif, procédez comme suit :

a. Choisissez Active.

> **Note**
>
> Si vous choisissez Inactif, vous et votre équipe ne recevrez aucune notification d'alarme.

b. Dans Destinataire, choisissez le destinataire.

> **Important**
>
> Vous pouvez envoyer des notifications d'alarme aux AWS IAM Identity Center utilisateurs. Pour utiliser cette fonctionnalité, vous devez activer IAM Identity Center. Vous ne pouvez activer IAM Identity Center que dans une seule AWS région à la fois. Cela signifie que vous ne pouvez définir des notifications d'alarme que dans la région où vous activez IAM Identity Center. Pour plus d'informations, consultez Démarrer dans le Guide de l'utilisateur AWS IAM Identity Center .

c. Pour Protocole, choisissez l'une des options suivantes :

- Courrier électronique et texto : l'alarme avertit les utilisateurs de l'IAM Identity Center par SMS et e-mail.
- E-mail : l'alarme avertit les utilisateurs de l'IAM Identity Center par un message électronique.
- Texte — L'alarme avertit les utilisateurs de l'IAM Identity Center par un message SMS.

d. Pour Expéditeur, choisissez l'expéditeur.

> **Important**
>
> Vous devez vérifier l'adresse e-mail de l'expéditeur dans Amazon Simple Email Service (Amazon SES). Pour plus d'informations, consultez la section Vérification des adresses e-mail dans Amazon SES, dans le manuel Amazon Simple Email Service Developer Guide.

10. Dans la section État de l'actif par défaut, vous pouvez définir l'état par défaut des alarmes créées à partir de ce modèle d'actif.

    > **Note**
    >
    > Vous activerez ou désactivez cette alarme pour les actifs que vous créez à partir de ce modèle d'actif lors d'une étape ultérieure.

11. Dans la section Paramètres avancés, vous pouvez configurer les autorisations, les paramètres de notification supplémentaires, les actions relatives à l'état de l'alarme, le modèle d'alarme dans SiteWise Monitor et le flux d'accusé de réception.

    > **Note**
    >
    > AWS IoT Events les alarmes nécessitent les rôles de service suivants :
    >
    > - Rôle censé envoyer AWS IoT Events des valeurs d'état d'alarme à AWS IoT SiteWise.
    > - Rôle censé envoyer AWS IoT Events des données à Lambda. Vous n'avez besoin de ce rôle que si votre alarme envoie des notifications.

    Dans la section Autorisations, procédez comme suit :

    a. Pour AWS IoT Events le rôle, utilisez un rôle existant ou créez-en un avec les autorisations requises. Ce rôle nécessite l'`iotsitewise:BatchPutAssetPropertyValue`autorisation et une relation de confiance qui permettent à iotevents.amazonaws.com d'assumer le rôle.

    b. Pour le rôle AWS IoT Events Lambda, utilisez un rôle existant ou créez-en un avec les autorisations requises. Ce rôle nécessite les `sso-directory:DescribeUser` autorisations `lambda:InvokeFunction` et une relation de confiance qui permet `iotevents.amazonaws.com` d'assumer le rôle.

12. (Facultatif) Dans la section Paramètres de notification supplémentaires, procédez comme suit :

    a. Pour l'attribut Recipient, vous définissez un attribut dont la valeur indique le destinataire de la notification. Vous pouvez choisir les utilisateurs d'IAM Identity Center comme destinataires.

       Vous pouvez créer un attribut ou utiliser un attribut existant dans le modèle d'actif.

- Si vous choisissez Créer un nouvel attribut de destinataire, spécifiez le nom de l'attribut de destinataire et la valeur par défaut du destinataire (facultatif) pour l'attribut.
- Si vous choisissez Utiliser un attribut de destinataire existant, sélectionnez l'attribut dans Nom d'attribut du destinataire. L'alarme utilise la valeur par défaut de l'attribut que vous avez choisi.

Vous pouvez remplacer la valeur par défaut de chaque actif que vous créez à partir de ce modèle d'actif.

b. Pour l'attribut de message personnalisé, vous définissez un attribut dont la valeur indique le message personnalisé à envoyer en plus du message de changement d'état par défaut. Par exemple, vous pouvez spécifier un message qui aidera votre équipe à comprendre comment traiter cette alarme.

   Vous pouvez choisir de créer un attribut ou d'utiliser un attribut existant dans le modèle d'actif.

   - Si vous choisissez de créer un nouvel attribut de message personnalisé, spécifiez le nom de l'attribut de message personnalisé et la valeur par défaut du message personnalisé (facultatif) pour l'attribut.
   - Si vous choisissez Utiliser un attribut de message personnalisé existant, sélectionnez l'attribut dans Nom de l'attribut de message personnalisé. L'alarme utilise la valeur par défaut de l'attribut que vous avez choisi.

   Vous pouvez remplacer la valeur par défaut de chaque actif que vous créez à partir de ce modèle d'actif.

c. Pour Gérer votre fonction Lambda, effectuez l'une des opérations suivantes :

   - Pour AWS IoT SiteWise créer une nouvelle fonction Lambda, choisissez Create a new Lambda from a AWS managed template.
   - Pour utiliser une fonction Lambda existante, choisissez Utiliser une fonction Lambda existante et choisissez le nom de la fonction.

   Pour plus d'informations, consultez la section Gestion des notifications d'alarme dans le Guide du AWS IoT Events développeur.

13. (Facultatif) Dans la section Définir l'action d'état, procédez comme suit :

a. Choisissez l'action Modifier.

b. Sous Ajouter des actions d'état d'alarme, ajoutez des actions, puis choisissez Enregistrer.

   Vous pouvez ajouter jusqu'à 10 actions.

AWS IoT Events peut effectuer des actions lorsque l'alarme est active. Vous pouvez définir des actions intégrées pour utiliser un temporisateur ou définir une variable, ou envoyer des données à d'autres AWS ressources. Pour plus d'informations, consultez la section Actions prises en charge dans le Guide du AWS IoT Events développeur.

14. (Facultatif) Sous Gérer le modèle d'alarme dans le SiteWise moniteur - facultatif, choisissez Actif ou Inactif.

    Utilisez cette option pour mettre à jour le modèle d'alarme dans SiteWise Monitorss. Cette option est activée par défaut.

15. Sous Accusation du flux, sélectionnez Actif ou Inactif. Pour plus d'informations sur le flux d'accusé de réception, consultezÉtats d'alarme.

16. Choisissez Ajouter une alarme.

> **Note**
>
> La AWS IoT SiteWise console envoie plusieurs demandes d'API pour ajouter l'alarme au modèle d'actif. Lorsque vous choisissez Ajouter une alarme, la console ouvre une boîte de dialogue qui indique la progression de ces demandes d'API. Restez sur cette page jusqu'à ce que chaque demande d'API aboutisse ou jusqu'à ce qu'une demande d'API échoue. Si une demande échoue, fermez la boîte de dialogue, corrigez le problème et choisissez Ajouter une alarme pour réessayer.

Définition d'une AWS IoT Events alarme (AWS IoT Events console)

Vous pouvez utiliser la AWS IoT Events console pour définir une AWS IoT Events alarme sur un modèle d'actif existant. Pour définir une AWS IoT Events alarme sur un nouveau modèle d'actif, créez le modèle d'actif, puis procédez comme suit. Pour plus d'informations, consultez Création de modèles de ressources.

> **Important**
>
> Chaque alarme nécessite un attribut qui spécifie la valeur de seuil à comparer pour l'alarme. Vous devez définir l'attribut de valeur seuil sur le modèle d'actif avant de pouvoir définir une alarme.
> Prenons un exemple où vous souhaitez définir une alarme qui détecte lorsqu'une éolienne dépasse sa vitesse nominale maximale de 50 mi/h. Avant de définir l'alarme, vous devez définir un attribut (Vitesse maximale du vent) avec une valeur par défaut de`50`.

Pour définir une AWS IoT Events alarme sur un modèle d'actif

1. Accédez à la console AWS IoT Events.
2. Dans le volet de navigation, sélectionnez Modèles d'alarme.
3. Choisissez Créer un modèle d'alarme.
4. Saisissez un nom pour votre alarme.
5. (Facultatif) Entrez une description pour votre alarme.
6. Dans la section Cible de l'alarme, procédez comme suit :
   a. Pour les options Target, choisissez la propriété de l'AWS IoT SiteWise actif.
   b. Choisissez le modèle d'actif pour lequel vous souhaitez ajouter l'alarme.
7. Dans la section Définitions des seuils, vous définissez le moment où l'alarme est détectée et la gravité de l'alarme. Procédez comme suit :
   a. Sélectionnez la propriété sur laquelle l'alarme est détectée. Chaque fois que cette propriété reçoit une nouvelle valeur, elle AWS IoT SiteWise envoie la valeur AWS IoT Events à pour évaluer l'état de l'alarme.
   b. Sélectionnez l'opérateur à utiliser pour comparer la propriété à la valeur de seuil. Sélectionnez parmi les options suivantes :
      - < inférieur à
      - <= inférieur ou égal
      - == égal
      - ! = différent
      - >= supérieur ou égal

- > supérieur à

c. Pour Valeur, sélectionnez la propriété d'attribut à utiliser comme valeur de seuil. AWS IoT Events compare la valeur de la propriété avec la valeur de cet attribut.

d. Entrez le niveau de gravité de l'alarme. Utilisez un chiffre que votre équipe comprend pour refléter la gravité de cette alarme.

8. (Facultatif) Dans la section Paramètres de notification - facultatif, procédez comme suit :

a. Pour Protocole, choisissez l'une des options suivantes :

- Courrier électronique et texto : l'alarme avertit les utilisateurs de l'IAM Identity Center par SMS et e-mail.
- E-mail : l'alarme avertit les utilisateurs de l'IAM Identity Center par un message électronique.
- Texte — L'alarme avertit les utilisateurs de l'IAM Identity Center par un message SMS.

b. Pour Expéditeur, choisissez l'expéditeur.

> **Important**
>
> Vous devez vérifier l'adresse e-mail de l'expéditeur dans Amazon Simple Email Service (Amazon SES). Pour plus d'informations, consultez la section Vérification des adresses e-mail dans Amazon SES, dans le manuel Amazon Simple Email Service Developer Guide.

c. Choisissez l'attribut dans Attribut du destinataire (facultatif). L'alarme utilise la valeur par défaut de l'attribut que vous avez choisi.

d. Choisissez l'attribut dans Attribut de message personnalisé - facultatif. L'alarme utilise la valeur par défaut de l'attribut que vous avez choisi.

9. Dans la section Instance, spécifiez l'état par défaut pour cette alarme. Vous pouvez activer ou désactiver cette alarme pour tous les actifs que vous créez à partir de ce modèle d'actif lors d'une étape ultérieure.

10. Dans les paramètres avancés, vous pouvez configurer les autorisations, les paramètres de notification supplémentaires, les actions relatives à l'état de l'alarme, le modèle d'alarme dans SiteWise Monitor et le flux d'accusé de réception.

> **Note**
>
> AWS IoT Events les alarmes nécessitent les rôles de service suivants :
>
> - Rôle censé envoyer AWS IoT Events des valeurs d'état d'alarme à AWS IoT SiteWise.
> - Rôle censé envoyer AWS IoT Events des données à Lambda. Vous n'avez besoin de ce rôle que si votre alarme envoie des notifications.

a. Dans la section Accusation de réception, choisissez Activé ou Désactivé. Pour plus d'informations sur le flux d'accusé de réception, consultezÉtats d'alarme.

b. Dans la section Autorisations, procédez comme suit :

   i. Pour AWS IoT Events le rôle, utilisez un rôle existant ou créez-en un avec les autorisations requises. Ce rôle nécessite l'`iotsitewise:BatchPutAssetPropertyValue`autorisation et une relation de confiance qui permettent à iotevents.amazonaws.com d'assumer le rôle.

   ii. Pour le rôle Lambda, utilisez un rôle existant ou créez-en un avec les autorisations requises. Ce rôle nécessite les `sso-directory:DescribeUser` autorisations `lambda:InvokeFunction` et une relation de confiance qui permet `iotevents.amazonaws.com` d'assumer le rôle.

c. (Facultatif) Dans le volet Paramètres de notification supplémentaires, procédez comme suit :

   - Pour Gérer votre fonction Lambda, effectuez l'une des opérations suivantes :
     - Pour AWS IoT Events créer une nouvelle fonction Lambda, choisissez Create a new Lambda function.
     - Pour utiliser une fonction Lambda existante, choisissez Utiliser une fonction Lambda existante et choisissez le nom de la fonction.

   Pour plus d'informations, consultez la section Gestion des notifications d'alarme dans le Guide du AWS IoT Events développeur.

d. (Facultatif) Dans la section Définir l'action d'état - facultatif, procédez comme suit :

   - Sous Actions relatives à l'état d'alarme, ajoutez des actions, puis choisissez Enregistrer.

Vous pouvez ajouter jusqu'à 10 actions.

AWS IoT Events peut effectuer des actions lorsque l'alarme est active. Vous pouvez définir des actions intégrées pour utiliser un temporisateur ou définir une variable, ou envoyer des données à d'autres AWS ressources. Pour plus d'informations, consultez la section Actions prises en charge dans le Guide du AWS IoT Events développeur.

11. Choisissez Créer.

> **Note**
>
> La AWS IoT Events console envoie plusieurs demandes d'API pour ajouter l'alarme au modèle d'actif. Lorsque vous choisissez Ajouter une alarme, la console ouvre une boîte de dialogue qui indique la progression de ces demandes d'API. Restez sur cette page jusqu'à ce que chaque demande d'API aboutisse ou jusqu'à ce qu'une demande d'API échoue. Si une demande échoue, fermez la boîte de dialogue, corrigez le problème et choisissez Ajouter une alarme pour réessayer.

Définition d'une AWS IoT Events alarme (AWS CLI)

Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour définir une AWS IoT Events alarme qui surveille la propriété d'un actif. Vous pouvez définir l'alarme sur un modèle d'actif nouveau ou existant. Après avoir défini l'alarme sur le modèle d'actif, vous créez une alarme AWS IoT Events et vous la connectez au modèle d'actif. Dans ce processus, vous devez effectuer les opérations suivantes :

Étapes

- Étape 1 : Définition d'une alarme sur un modèle d'actif
- Étape 2 : Définition d'un modèle AWS IoT Events d'alarme
- Étape 3 : Activation du flux de données entre AWS IoT SiteWise et AWS IoT Events

Étape 1 : Définition d'une alarme sur un modèle d'actif

Ajoutez une définition d'alarme et les propriétés associées à un modèle d'actif nouveau ou existant.

Pour définir une alarme sur un modèle d'actif (CLI)

1. Créez un fichier, appelé `asset-model-payload.json`. Suivez les étapes décrites dans ces autres sections pour ajouter les détails de votre modèle d'actif au fichier, mais ne soumettez pas de demande de création ou de mise à jour du modèle d'actif. Dans cette section, vous ajoutez une définition d'alarme aux détails du modèle d'actif dans le `asset-model-payload.json` fichier.
   - Pour plus d'informations sur la création d'un modèle d'actifs, consultezCréation d'un modèle d'actifs (AWS CLI).
   - Pour plus d'informations sur la mise à jour d'un modèle d'actif existant, consultezMettre à jour un modèle d'actif ou de composant (AWS CLI).

   > **Note**
   >
   > Votre modèle d'actif doit définir au moins une propriété d'actif, y compris la propriété d'actif à surveiller avec l'alarme.

2. Ajoutez un modèle composite d'alarme (`assetModelCompositeModels`) au modèle d'actif. Un modèle composite AWS IoT Events d'alarme indique le `IOT_EVENTS` type et spécifie une propriété de source d'alarme. Vous ajoutez la propriété source d'alarme après avoir créé le modèle d'alarme dans AWS IoT Events.

   > **Important**
   >
   > Le modèle composite d'alarme doit porter le même nom que le modèle AWS IoT Events d'alarme que vous créerez ultérieurement. Les noms des modèles d'alarme ne peuvent contenir que des caractères alphanumériques. Spécifiez un nom alphanumérique unique afin de pouvoir utiliser le même nom pour le modèle d'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. Ajoutez un attribut de seuil d'alarme au modèle d'actif. Spécifiez la valeur par défaut à utiliser pour ce seuil. Vous pouvez remplacer cette valeur par défaut pour chaque actif en fonction de ce modèle.

> **Note**
>
> L'attribut du seuil d'alarme doit être a `INTEGER` ou `DOUBLE` a.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "Temperature Max Threshold",
      "dataType": "DOUBLE",
      "type": {
        "attribute": {
          "defaultValue": "105.0"
        }
      }
```

```
    }
  ]
}
```

4. (Facultatif) Ajoutez des attributs de notification d'alarme au modèle d'actif. Ces attributs indiquent le destinataire du centre d'identité IAM et les autres entrées AWS IoT Events utilisées pour envoyer des notifications lorsque l'alarme change d'état. Vous pouvez remplacer ces valeurs par défaut pour chaque actif en fonction de ce modèle.

   > **Important**
   >
   > Vous pouvez envoyer des notifications d'alarme aux AWS IAM Identity Center utilisateurs. Pour utiliser cette fonctionnalité, vous devez activer IAM Identity Center. Vous ne pouvez activer IAM Identity Center que dans une seule AWS région à la fois. Cela signifie que vous ne pouvez définir des notifications d'alarme que dans la région où vous activez IAM Identity Center. Pour plus d'informations, consultez Démarrer dans le Guide de l'utilisateur AWS IAM Identity Center .

   Procédez comme suit :

   a. Ajoutez un attribut qui spécifie l'ID de votre banque d'identités IAM Identity Center. Vous pouvez utiliser l'opération d'ListInstancesAPI IAM Identity Center pour répertorier vos magasins d'identités. Cette opération ne fonctionne que dans la région où vous activez IAM Identity Center.

      ```
      aws sso-admin list-instances
      ```

      Spécifiez ensuite l'ID du magasin d'identités (par exemple,`d-123EXAMPLE`) comme valeur par défaut pour l'attribut.

      ```
      {
        ...
        "assetModelProperties": [
          ...
          {
            "name": "identityStoreId",
            "dataType": "STRING",
            "type": {
      ```

```
        "attribute": {
          "defaultValue": "d-123EXAMPLE"
        }
      }
    }
  ]
}
```

b. Ajoutez un attribut qui spécifie l'ID de l'utilisateur IAM Identity Center qui reçoit les notifications. Pour définir un destinataire de notification par défaut, ajoutez un ID utilisateur IAM Identity Center comme valeur par défaut. Procédez de l'une des manières suivantes pour obtenir un ID utilisateur IAM Identity Center :

   i. Vous pouvez utiliser l'ListUsersAPI IAM Identity Center pour obtenir l'identifiant d'un utilisateur dont vous connaissez le nom d'utilisateur. Remplacez *D-123Example par* l'ID de votre banque d'identités et remplacez *Name* par le nom d'utilisateur de l'utilisateur.

   ```
   aws identitystore list-users \
     --identity-store-id d-123EXAMPLE \
     --filters AttributePath=UserName,AttributeValue=Name
   ```

   ii. Utilisez la console IAM Identity Center pour parcourir vos utilisateurs et trouver un ID utilisateur.

   Spécifiez ensuite l'ID utilisateur (par exemple,`123EXAMPLE-a1b2c3d4-5678-90ab-cdef-33333EXAMPLE`) comme valeur par défaut pour l'attribut, ou définissez l'attribut sans valeur par défaut.

   ```
   {
     ...
     "assetModelProperties": [
       ...
       {
         "name": "userId",
         "dataType": "STRING",
         "type": {
           "attribute": {
             "defaultValue": "123EXAMPLE-a1b2c3d4-5678-90ab-cdef-33333EXAMPLE"
           }
         }
   ```

```
    }
  ]
}
```

c. (Facultatif) Ajoutez un attribut qui spécifie l'ID d'expéditeur par défaut pour les notifications par SMS (texte). L'identifiant de l'expéditeur s'affiche en tant qu'expéditeur des messages envoyés par Amazon Simple Notification Service (Amazon SNS). Pour plus d'informations, consultez la section Demande d'identifiants d'expéditeur pour les messages SMS avec Amazon SNS dans le guide du développeur Amazon Simple Notification Service.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "senderId",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "MyFactory"
        }
      }
    }
  ]
}
```

d. (Facultatif) Ajoutez un attribut qui spécifie l'adresse e-mail par défaut à utiliser comme adresse d'expéditeur dans les notifications par e-mail.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "fromAddress",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "my.factory@example.com"
        }
      }
    }
```

```
  ]
}
```

e. (Facultatif) Ajoutez un attribut qui indique le sujet par défaut à utiliser dans les notifications par e-mail.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "emailSubject",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "[ALERT] High boiler temperature"
        }
      }
    }
  ]
}
```

f. (Facultatif) Ajoutez un attribut qui spécifie un message supplémentaire à inclure dans les notifications. Par défaut, les messages de notification incluent des informations sur l'alarme. Vous pouvez également inclure un message supplémentaire fournissant plus d'informations à l'utilisateur.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "additionalMessage",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "Turn off the power before you check the alarm."
        }
      }
    }
  ]
}
```

5. Créez le modèle d'actif ou mettez à jour le modèle d'actif existant. Effectuez l'une des actions suivantes :

   - Pour créer le modèle d'actif, exécutez la commande suivante.

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

   - Pour mettre à jour le modèle d'actif existant, exécutez la commande suivante. Remplacez *asset-model-id* par l'ID du modèle de ressource.

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

   Après avoir exécuté la commande, notez le `assetModelId` dans la réponse.

Exemple : modèle d'actif de chaudière

Le modèle d'actif suivant représente une chaudière qui fournit des données de température. Ce modèle d'équipement définit une alarme qui détecte la surchauffe de la chaudière.

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

Étape 2 : Définition d'un modèle AWS IoT Events d'alarme

Créez le modèle d'alarme dans AWS IoT Events. Dans AWS IoT Events, vous utilisez des expressions pour spécifier des valeurs dans les modèles d'alarme. Vous pouvez utiliser des expressions pour spécifier des valeurs de AWS IoT SiteWise à évaluer et à utiliser comme entrées pour l'alarme. Lorsque les valeurs des propriétés de l'actif sont AWS IoT SiteWise envoyées au modèle d'alarme, il AWS IoT Events évalue l'expression pour obtenir la valeur de la propriété ou l'ID de l'actif. Vous pouvez utiliser les expressions suivantes dans le modèle d'alarme :

- Valeurs des propriétés des actifs

  Pour obtenir la valeur d'une propriété d'actif, utilisez l'expression suivante. Remplacez *`assetModelId`* par l'ID du modèle d'actif et remplacez *`propertyID`* par l'ID de la propriété.

  ```
  $sitewise.assetModel.`assetModelId`.`propertyId`.propertyValue.value
  ```

- Identifiants des actifs

  Pour obtenir l'ID de la ressource, utilisez l'expression suivante. Remplacez *`asset ModelId`* par l'ID du modèle d'actif et remplacez *`propertyID`* par l'ID de la propriété.

  ```
  $sitewise.assetModel.`assetModelId`.`propertyId`.assetId
  ```

> **Note**
>
> Lorsque vous créez le modèle d'alarme, vous pouvez définir des littéraux plutôt que des expressions dont l'évaluation est basée sur des AWS IoT SiteWise valeurs. Cela peut réduire le nombre d'attributs que vous définissez dans votre modèle d'actifs. Toutefois, si vous définissez une valeur au sens littéral, vous ne pouvez pas personnaliser cette valeur sur les actifs en fonction du modèle d'actif. Vos AWS IoT SiteWise Monitor utilisateurs ne peuvent pas non plus personnaliser l'alarme, car ils ne peuvent configurer les paramètres d'alarme que sur les actifs.

Pour créer un modèle AWS IoT Events d'alarme (CLI)

1. Lorsque vous créez le modèle d'alarme dans AWS IoT Events, vous devez spécifier l'ID de chaque propriété utilisée par l'alarme, notamment les éléments suivants :

- La propriété d'état d'alarme dans le modèle d'actif composite
- La propriété surveillée par l'alarme
- L'attribut de seuil
- (Facultatif) L'attribut ID de la banque d'identités IAM Identity Center
- (Facultatif) L'attribut d'ID utilisateur IAM Identity Center
- (Facultatif) L'attribut ID de l'expéditeur du SMS
- (Facultatif) L'attribut d'adresse e-mail
- (Facultatif) L'attribut d'objet de l'e-mail
- (Facultatif) L'attribut de message supplémentaire

Exécutez la commande suivante pour récupérer les identifiants de ces propriétés sur le modèle d'actif. Remplacez *asset-model-id* par l'ID du modèle d'actif de l'étape précédente.

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

L'opération renvoie une réponse qui contient les détails du modèle de ressource. Notez l'ID de chaque propriété utilisée par l'alarme. Vous utiliserez ces identifiants lorsque vous créerez le modèle AWS IoT Events d'alarme à l'étape suivante.

2. Créez le modèle d'alarme dans AWS IoT Events. Procédez comme suit :

   a. Créez un fichier, appelé `alarm-model-payload.json`.

   b. Copiez l'objet JSON suivant dans le fichier.

   c. Entrez le nom (`alarmModelName`), la description (`alarmModelDescription`) et la gravité (`severity`) de votre alarme. Pour ce qui est de la gravité, spécifiez un entier qui reflète les niveaux de gravité de votre entreprise.

> **Important**
>
> Le modèle d'alarme doit porter le même nom que le modèle composite d'alarme que vous avez défini précédemment dans votre modèle d'équipement.
> Les noms des modèles d'alarme ne peuvent contenir que des caractères alphanumériques.

```
{
  "alarmModelName": "BoilerTemperatureHighAlarm",
  "alarmModelDescription": "Detects when the boiler temperature is high.",
  "severity": 3
}
```

d. Ajoutez la règle de comparaison (`alarmRule`) à l'alarme. Cette règle définit la propriété à surveiller (`inputProperty`), la valeur de seuil à comparer (`threshold`) et l'opérateur de comparaison à utiliser (`comparisonOperator`).

- Remplacez ModelId l'*`actif`* par l'ID du modèle d'actif.
- Remplacez l'*`alarme PropertyId`* par l'identifiant de la propriété surveillée par l'alarme.
- Remplacez *`threshold AttributeId`* par l'ID de la propriété de l'attribut threshold.
- Remplacez *`GREATER`* par l'opérateur à utiliser pour comparer les valeurs des propriétés avec le seuil. Sélectionnez parmi les options suivantes :
  - `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. Ajoutez une action (`alarmEventActions`) pour envoyer l'état de l'alarme au AWS IoT SiteWise moment où l'alarme change d'état.

> **Note**
>
> Pour une configuration avancée, vous pouvez définir des actions supplémentaires à effectuer lorsque l'alarme change d'état. Par exemple, vous pouvez appeler une AWS Lambda fonction ou publier sur un sujet MQTT. Pour plus d'informations, consultez la section Utilisation d'autres AWS services dans le Guide du AWS IoT Events développeur.

- Remplacez ModelId l'*`actif`* par l'ID du modèle d'actif.
- Remplacez l'*`alarme PropertyId`* par l'identifiant de la propriété surveillée par l'alarme.
- Remplacez l'*`StatePropertyID d'alarme`* par l'ID de la propriété d'état de l'alarme dans le modèle composite d'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. (Facultatif) Configurez les paramètres de notification d'alarme. L'action de notification d'alarme utilise une fonction Lambda de votre compte pour envoyer des notifications d'alarme. Pour plus d'informations, consultez Exigences relatives aux notifications d'alarme. Dans les paramètres de notification d'alarme, vous pouvez configurer les notifications par SMS et e-mail à envoyer aux utilisateurs d'IAM Identity Center. Procédez comme suit :

   i. Ajoutez la configuration de notification d'alarme (`alarmNotification`) à la charge utile dans`alarm-model-payload.json`.

      - Remplacez l'*`NotificationFunctionARN de l'alarme`* par l'ARN de la fonction Lambda qui gère les notifications d'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. (Facultatif) Configurez les notifications par SMS (`smsConfigurations`) à envoyer à un utilisateur du IAM Identity Center lorsque l'alarme change d'état.

- Remplacez l'*identité StoreId AttributeId* par l'ID de l'attribut qui contient l'ID de la banque d'identités IAM Identity Center.
- Remplacez *l'IdAttributeID utilisateur* par l'ID de l'attribut qui contient l'ID de l'utilisateur IAM Identity Center.
- Remplacez *l'IdAttributeidentifiant de l'expéditeur* par l'ID de l'attribut contenant l'identifiant de l'expéditeur Amazon SNS, ou supprimez-le `senderId` de la charge utile.
- Remplacez l'*MessageAttributeID supplémentaire* par l'ID de l'attribut qui contient le message supplémentaire, ou supprimez-le `additionalMessage` de la charge utile.

```
{
  "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. (Facultatif) Configurez les notifications par e-mail (`emailConfigurations`) à envoyer à un utilisateur du IAM Identity Center lorsque l'alarme change d'état.

- Remplacez *l'identité StoreId AttributeId* par l'ID de la propriété d'attribut ID de la banque d'identités IAM Identity Center.
- Remplacez *l'IdAttributeID utilisateur* par l'ID de la propriété d'attribut ID utilisateur d'IAM Identity Center.
- Remplacez *from AddressAttribute Id* par l'ID de la propriété d'attribut d'adresse « from », ou supprimez-le `from` de la charge utile.
- Remplacez l'*SubjectAttributeID de l'e-mail par* l'ID de la propriété de l'attribut de l'objet de l'e-mail, ou `subject` supprimez-le de la charge utile.
- Remplacez l'*MessageAttributeID supplémentaire* par l'ID de la propriété d'attribut de message supplémentaire, ou supprimez-le `additionalMessage` de la charge utile.

```
{
  "alarmModelName": "BoilerTemperatureHighAlarm",
  "alarmModelDescription": "Detects when the boiler temperature is high.",
  "severity": 3,
  "alarmRule": {
    "simpleRule": {
      "inputProperty":
 "$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.propertyValue.value",
      "comparisonOperator": "GREATER",
      "threshold":
 "$sitewise.assetModel.`assetModelId`.`thresholdAttributeId`.propertyValue.value"
    }
  },
  "alarmEventActions": {
    "alarmActions": [
      {
        "iotSiteWise": {
          "assetId":
 "$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.assetId",
          "propertyId": "'alarmStatePropertyId'"
        }
      }
    ]
  },
  "alarmNotification": {
    "notificationActions": [
      {
```

```
        "action": {
          "lambdaAction": {
            "functionArn": "alarmNotificationFunctionArn"
          }
        },
        "smsConfigurations": [
          {
            "recipients": [
              {
                "ssoIdentity": {
                  "identityStoreId":
"$sitewise.assetModel.`assetModelId`.`identityStoreIdAttributeId`.propertyValue.va
                  "userId":
"$sitewise.assetModel.`assetModelId`.`userIdAttributeId`.propertyValue.value"
                }
              }
            ],
            "senderId":
"$sitewise.assetModel.`assetModelId`.`senderIdAttributeId`.propertyValue.value",
            "additionalMessage":
"$sitewise.assetModel.`assetModelId`.`additionalMessageAttributeId`.propertyValue.
          }
        ],
        "emailConfigurations": [
          {
            "from":
"$sitewise.assetModel.`assetModelId`.`fromAddressAttributeId`.propertyValue.value"
            "recipients": {
              "to": [
                {
                  "ssoIdentity": {
                    "identityStoreId":
"$sitewise.assetModel.`assetModelId`.`identityStoreIdAttributeId`.propertyValue.va
                    "userId":
"$sitewise.assetModel.`assetModelId`.`userIdAttributeId`.propertyValue.value"
                  }
                }
              ]
            },
            "content": {
              "subject":
"$sitewise.assetModel.`assetModelId`.`emailSubjectAttributeId`.propertyValue.value
              "additionalMessage":
"$sitewise.assetModel.`assetModelId`.`additionalMessageAttributeId`.propertyValue.
```

```
            }
          }
        ]
      }
    ]
  }
}
```

g. (Facultatif) Ajoutez les capacités d'alarme (`alarmCapabilities`) à la charge utile. `alarm-model-payload.json` Dans cet objet, vous pouvez spécifier si le flux d'accusé de réception est activé et l'état d'activation par défaut pour les actifs en fonction du modèle d'actif. Pour plus d'informations sur le flux d'accusé de réception, consultezÉtats d'alarme.

```
{
  "alarmModelName": "BoilerTemperatureHighAlarm",
  "alarmModelDescription": "Detects when the boiler temperature is high.",
  "severity": 3,
  "alarmRule": {
    "simpleRule": {
      "inputProperty":
 "$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.propertyValue.value",
      "comparisonOperator": "GREATER",
      "threshold":
 "$sitewise.assetModel.`assetModelId`.`thresholdAttributeId`.propertyValue.value"
    }
  },
  "alarmEventActions": {
    "alarmActions": [
      {
        "iotSiteWise": {
          "assetId":
 "$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.assetId",
          "propertyId": "'alarmStatePropertyId'"
        }
      }
    ]
  },
  "alarmNotification": {
    "notificationActions": [
      {
        "action": {
          "lambdaAction": {
            "functionArn": "alarmNotificationFunctionArn"
```

```
          }
        },
        "smsConfigurations": [
          {
            "recipients": [
              {
                "ssoIdentity": {
                  "identityStoreId":
"$sitewise.assetModel.`assetModelId`.`identityStoreIdAttributeId`.propertyValue.value"
                  "userId":
"$sitewise.assetModel.`assetModelId`.`userIdAttributeId`.propertyValue.value"
                }
              }
            ],
            "senderId":
"$sitewise.assetModel.`assetModelId`.`senderIdAttributeId`.propertyValue.value",
            "additionalMessage":
"$sitewise.assetModel.`assetModelId`.`additionalMessageAttributeId`.propertyValue.valu
          }
        ],
        "emailConfigurations": [
          {
            "from":
"$sitewise.assetModel.`assetModelId`.`fromAddressAttributeId`.propertyValue.value",
            "recipients": {
              "to": [
                {
                  "ssoIdentity": {
                    "identityStoreId":
"$sitewise.assetModel.`assetModelId`.`identityStoreIdAttributeId`.propertyValue.value"
                    "userId":
"$sitewise.assetModel.`assetModelId`.`userIdAttributeId`.propertyValue.value"
                  }
                }
              ]
            },
            "content": {
              "subject":
"$sitewise.assetModel.`assetModelId`.`emailSubjectAttributeId`.propertyValue.value",
              "additionalMessage":
"$sitewise.assetModel.`assetModelId`.`additionalMessageAttributeId`.propertyValue.valu
            }
          }
        ]
```

```
      }
    ]
  },
  "alarmCapabilities": {
    "initializationConfiguration": {
      "disabledOnInitialization": false
    },
    "acknowledgeFlow": {
      "enabled": true
    }
  }
}
```

h. Ajoutez le rôle de service IAM (`roleArn`) qui AWS IoT Events peut assumer d'envoyer des données à AWS IoT SiteWise. Ce rôle nécessite l'`iotsitewise:BatchPutAssetPropertyValue`autorisation et une relation de confiance qui permettent `iotevents.amazonaws.com` d'assumer le rôle. Pour envoyer des notifications, ce rôle nécessite également les `sso-directory:DescribeUser` autorisations `lambda:InvokeFunction` et. Pour plus d'informations, consultez la section Rôles du service Alarm dans le guide du AWS IoT Events développeur.

- Remplacez le `roleArn` par l'ARN du rôle qui AWS IoT Events peut assumer ces actions.

```
{
  "alarmModelName": "BoilerTemperatureHighAlarm",
  "alarmModelDescription": "Detects when the boiler temperature is high.",
  "severity": 3,
  "alarmRule": {
    "simpleRule": {
      "inputProperty":
 "$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.propertyValue.value",
      "comparisonOperator": "GREATER",
      "threshold":
 "$sitewise.assetModel.`assetModelId`.`thresholdAttributeId`.propertyValue.value"
    }
  },
  "alarmEventActions": {
    "alarmActions": [
      {
        "iotSiteWise": {
```

```
          "assetId":
"$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.assetId",
          "propertyId": "'alarmStatePropertyId'"
        }
      }
    ]
  },
  "alarmNotification": {
    "notificationActions": [
      {
        "action": {
          "lambdaAction": {
            "functionArn": "alarmNotificationFunctionArn"
          }
        },
        "smsConfigurations": [
          {
            "recipients": [
              {
                "ssoIdentity": {
                  "identityStoreId":
"$sitewise.assetModel.`assetModelId`.`identityStoreIdAttributeId`.propertyValue.value"
                  "userId":
"$sitewise.assetModel.`assetModelId`.`userIdAttributeId`.propertyValue.value"
                }
              }
            ],
            "senderId":
"$sitewise.assetModel.`assetModelId`.`senderIdAttributeId`.propertyValue.value",
            "additionalMessage":
"$sitewise.assetModel.`assetModelId`.`additionalMessageAttributeId`.propertyValue.valu
          }
        ],
        "emailConfigurations": [
          {
            "from":
"$sitewise.assetModel.`assetModelId`.`fromAddressAttributeId`.propertyValue.value",
            "recipients": {
              "to": [
                {
                  "ssoIdentity": {
                    "identityStoreId":
"$sitewise.assetModel.`assetModelId`.`identityStoreIdAttributeId`.propertyValue.value"
```

```
                    "userId":
 "$sitewise.assetModel.`assetModelId`.`userIdAttributeId`.propertyValue.value"
                  }
                }
              ]
            },
            "content": {
              "subject":
 "$sitewise.assetModel.`assetModelId`.`emailSubjectAttributeId`.propertyValue.value",
              "additionalMessage":
 "$sitewise.assetModel.`assetModelId`.`additionalMessageAttributeId`.propertyValue.valu
            }
          }
        ]
      }
    ]
  },
  "alarmCapabilities": {
    "initializationConfiguration": {
      "disabledOnInitialization": false
    },
    "acknowledgeFlow": {
      "enabled": false
    }
  },
  "roleArn": "arn:aws:iam::123456789012:role/MyIoTEventsAlarmRole"
}
```

i. Exécutez la commande suivante pour créer le modèle AWS IoT Events d'alarme à partir de la charge utile. `alarm-model-payload.json`

```
aws iotevents create-alarm-model --cli-input-json file://alarm-model-
payload.json
```

j. L'opération renvoie une réponse qui inclut l'ARN du modèle d'alarme,`alarmModelArn`. Copiez cet ARN pour définir la définition de l'alarme sur votre modèle d'actif à l'étape suivante.

Étape 3 : Activation du flux de données entre AWS IoT SiteWise et AWS IoT Events

Après avoir créé les ressources requises dans AWS IoT SiteWise et AWS IoT Events, vous pouvez activer le flux de données entre les ressources pour activer votre alarme. Dans cette section, vous

allez mettre à jour la définition d'alarme dans le modèle d'actif pour utiliser le modèle d'alarme que vous avez créé à l'étape précédente.

Pour activer le flux de données entre AWS IoT SiteWise et AWS IoT Events (CLI)

- Définissez le modèle d'alarme comme source de l'alarme dans le modèle d'actif. Procédez comme suit :

  a. Exécutez la commande suivante pour récupérer la définition de modèle de ressource existante. Remplacez *asset-model-id* par l'ID du modèle de ressource.

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

  L'opération renvoie une réponse qui contient les détails du modèle de ressource.

  b. Créez un fichier appelé `update-asset-model-payload.json` et copiez la réponse de la commande précédente dans le fichier.

  c. Supprimez les paires clé-valeur suivantes du `update-asset-model-payload.json` fichier :

  - `assetModelId`
  - `assetModelArn`
  - `assetModelCreationDate`
  - `assetModelLastUpdateDate`
  - `assetModelStatus`

  d. Ajoutez la propriété de source d'alarme (`AWS/ALARM_SOURCE`) au modèle composite d'alarme que vous avez défini précédemment. Remplacez l'*alarme ModelArn* par l'ARN du modèle d'alarme, qui définit la valeur de la propriété de la source d'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. Exécutez la commande suivante pour mettre à jour le modèle d'actif avec la définition stockée dans le `update-asset-model-payload.json` fichier. Remplacez *asset-model-id* par l'ID du modèle de ressource.

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

Votre modèle d'équipement définit désormais une alarme qui détecte AWS IoT Events. L'alarme surveille la propriété cible dans tous les actifs sur la base de ce modèle d'actif. Vous pouvez

configurer l'alarme sur chaque actif afin de personnaliser les propriétés telles que le seuil ou le destinataire du IAM Identity Center pour chaque actif. Pour plus d'informations, consultez Configuration des alarmes sur les actifs.

Définition des alarmes externes

Les alarmes externes contiennent l'état d'une alarme que vous détectez à l'extérieur AWS IoT SiteWise.

Définition d'une alarme externe (console)

Vous pouvez utiliser la AWS IoT SiteWise console pour définir une alarme externe sur un modèle d'actif existant. Pour définir une alarme externe sur un nouveau modèle d'actif, créez le modèle d'actif, puis procédez comme suit. Pour plus d'informations, consultez Création de modèles de ressources.

Pour définir une alarme sur un modèle d'actif

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Models (Modèles).
3. Choisissez le modèle d'actif pour lequel vous souhaitez définir une alarme.
4. Choisissez l'onglet Définitions des alarmes.
5. Choisissez Ajouter une alarme.
6. Dans les options de type d'alarme, choisissez Alarme externe.
7. Saisissez un nom pour votre alarme.
8. (Facultatif) Entrez une description pour votre alarme.
9. Choisissez Ajouter une alarme.

Définition d'une alarme externe (CLI)

Vous pouvez utiliser le AWS CLI pour définir une alarme externe sur un modèle d'actif nouveau ou existant.

Pour ajouter une alarme externe à un modèle d'actif, vous devez ajouter un modèle composite d'alarme au modèle d'actif. Un modèle composite d'alarme externe spécifie le `EXTERNAL` type et ne spécifie aucune propriété de source d'alarme. L'exemple d'alarme composite suivant définit une alarme de température externe.

```
{
  ...
  "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": {}
          }
        }
      ]
    }
  ]
}
```

Pour plus d'informations sur la façon d'ajouter un modèle composite à un modèle d'actif nouveau ou existant, consultez ce qui suit :

- Création d'un modèle d'actifs (AWS CLI)
- Mettre à jour un modèle d'actif ou de composant (AWS CLI)

Après avoir défini l'alarme externe, vous pouvez intégrer l'état de l'alarme aux actifs en fonction du modèle d'actif. Pour plus d'informations, consultez Ingestion de l'état d'alarme externe.

Configuration des alarmes sur les actifs

Après avoir défini une AWS IoT Events alarme sur un modèle d'actif, vous pouvez configurer l'alarme pour chaque actif en fonction du modèle d'actif. Vous pouvez modifier la valeur du seuil et les paramètres de notification de l'alarme. Chacune de ces valeurs est un attribut de la ressource. Vous pouvez donc mettre à jour la valeur par défaut de l'attribut pour configurer ces valeurs.

> **Note**
>
> Vous pouvez configurer ces valeurs pour les AWS IoT Events alarmes, mais pas pour les alarmes externes.

Rubriques

- Configuration d'une valeur de seuil (console)
- Configuration d'une valeur de seuil (AWS CLI)
- Configuration des paramètres de notification (console)
- Configuration des paramètres de notification (CLI)

Configuration d'une valeur de seuil (console)

Vous pouvez utiliser la AWS IoT SiteWise console pour mettre à jour la valeur de l'attribut qui indique le seuil d'une alarme.

Pour mettre à jour la valeur seuil d'une alarme (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Ressources.
3. Choisissez l'actif pour lequel vous souhaitez mettre à jour une valeur de seuil d'alarme.

   > **Tip**
   >
   > Vous pouvez cliquer sur l'icône en forme de flèche pour développer une hiérarchie de ressources afin de trouver votre ressource.

4. Choisissez Modifier.

5. Recherchez l'attribut que l'alarme utilise pour sa valeur de seuil, puis entrez sa nouvelle valeur.
6. Choisissez Enregistrer.

Configuration d'une valeur de seuil (AWS CLI)

Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour mettre à jour la valeur de l'attribut qui indique le seuil d'une alarme.

Vous devez connaître l'`assetId` de votre ressource et le `propertyId`de la propriété pour effectuer cette procédure. Vous pouvez également utiliser l'identifiant externe. Si vous avez créé un actif et que vous ne le connaissez pas`assetId`, utilisez l'ListAssetsAPI pour répertorier tous les actifs d'un modèle spécifique. Utilisez cette DescribeAssetopération pour afficher les propriétés de votre actif, y compris les identifiants de propriété.

Utilisez l'opération BatchPutAssetPropertyValue pour attribuer des valeurs d'attribut à votre actif. Vous pouvez utiliser cette opération pour définir plusieurs attributs à la fois. La charge utile de cette opération contient une liste d'entrées, chacune contenant l'ID de ressource, l'ID de propriété et la valeur d'attribut.

Pour mettre à jour la valeur d'un attribut (AWS CLI)

1. Créez un fichier nommé `batch-put-payload.json` et copiez l'objet JSON suivant dans le fichier. Cet exemple de charge utile montre comment définir la latitude et la longitude d'une éolienne. Mettez à jour les ID, les valeurs et les horodatages pour modifier la charge utile de votre cas d'utilisation.

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

- Chaque entrée de la charge utile contient un `entryId` que vous pouvez définir sous la forme d'une chaîne unique. Si des entrées de demande échouent, chaque erreur contiendra l'`entryId` de la demande correspondante afin que vous sachiez quelles demandes réessayer.
- Pour définir une valeur d'attribut, vous pouvez inclure une structure timestamp-quality-value (TQV) dans la liste de chaque propriété `propertyValues` d'attribut. Cette structure doit contenir le nouveau `value` et le `timestamp` actuel.
  - `value`— Structure contenant l'un des champs suivants, selon le type de propriété définie :
    - `booleanValue`
    - `doubleValue`
    - `integerValue`
    - `stringValue`
  - `timestamp`— Une structure qui contient l'heure actuelle d'Unix en secondes,. `timeInSeconds` AWS IoT SiteWise rejette tous les points de données dont l'horodatage existait depuis plus de 7 jours ou moins de 5 minutes dans le futur.

Pour plus d'informations sur la préparation d'une charge utile pour BatchPutAssetPropertyValue, consultezIngestion de données à l'aide de l'API AWS IoT SiteWise.

2. Exécutez la commande suivante pour envoyer les valeurs d'attribut à AWS IoT SiteWise :

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

Configuration des paramètres de notification (console)

Vous pouvez utiliser la AWS IoT SiteWise console pour mettre à jour la valeur des attributs qui spécifient les paramètres de notification d'une alarme.

Pour mettre à jour les paramètres de notification d'une alarme (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Ressources.
3. Choisissez l'actif pour lequel vous souhaitez mettre à jour les paramètres d'alarme.
4. Choisissez Modifier.
5. Recherchez l'attribut utilisé par l'alarme pour le paramètre de notification que vous souhaitez modifier, puis entrez sa nouvelle valeur.
6. Choisissez Enregistrer.

Configuration des paramètres de notification (CLI)

Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour mettre à jour la valeur de l'attribut qui spécifie les paramètres de notification pour une alarme.

Vous devez connaître l'`assetId` de votre ressource et le `propertyId`de la propriété pour effectuer cette procédure. Vous pouvez également utiliser l'identifiant externe. Si vous avez créé un actif et que vous ne le connaissez pas`assetId`, utilisez l'ListAssetsAPI pour répertorier tous les actifs d'un modèle spécifique. Utilisez cette DescribeAssetopération pour afficher les propriétés de votre actif, y compris les identifiants de propriété.

Utilisez l'opération BatchPutAssetPropertyValue pour attribuer des valeurs d'attribut à votre actif. Vous pouvez utiliser cette opération pour définir plusieurs attributs à la fois. La charge utile de cette opération contient une liste d'entrées, chacune contenant l'ID de ressource, l'ID de propriété et la valeur d'attribut.

Pour mettre à jour la valeur d'un attribut (AWS CLI)

1. Créez un fichier nommé `batch-put-payload.json` et copiez l'objet JSON suivant dans le fichier. Cet exemple de charge utile montre comment définir la latitude et la longitude d'une éolienne. Mettez à jour les ID, les valeurs et les horodatages pour modifier la charge utile de votre cas d'utilisation.

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

- Chaque entrée de la charge utile contient un `entryId` que vous pouvez définir sous la forme d'une chaîne unique. Si des entrées de demande échouent, chaque erreur contiendra l'`entryId` de la demande correspondante afin que vous sachiez quelles demandes réessayer.
- Pour définir une valeur d'attribut, vous pouvez inclure une structure timestamp-quality-value (TQV) dans la liste de chaque propriété `propertyValues` d'attribut. Cette structure doit contenir le nouveau `value` et le `timestamp` actuel.
  - `value`— Structure contenant l'un des champs suivants, selon le type de propriété définie :
    - `booleanValue`
    - `doubleValue`
    - `integerValue`
    - `stringValue`
  - `timestamp`— Une structure qui contient l'heure actuelle d'Unix en secondes,. `timeInSeconds` AWS IoT SiteWise rejette tous les points de données dont l'horodatage existait depuis plus de 7 jours ou moins de 5 minutes dans le futur.

  Pour plus d'informations sur la préparation d'une charge utile pour BatchPutAssetPropertyValue, consultezIngestion de données à l'aide de l'API AWS IoT SiteWise.

2. Exécutez la commande suivante pour envoyer les valeurs d'attribut à AWS IoT SiteWise :

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

Répondre aux alarmes

Lorsqu'une AWS IoT Events alarme change d'état, vous pouvez effectuer les opérations suivantes pour y répondre :

- Accusez réception d'une alarme pour indiquer que vous êtes en train de résoudre le problème.
- Suspendez une alarme pour la désactiver temporairement.
- Désactivez une alarme pour la désactiver définitivement jusqu'à ce que vous la réactiviez.
- Activez une alarme désactivée pour détecter l'état de l'alarme.
- Réinitialisez une alarme pour effacer son état et sa dernière valeur.

Vous pouvez utiliser la AWS IoT SiteWise console ou l' AWS IoT Events API pour répondre à une alarme.

> **Note**
>
> Vous pouvez répondre aux AWS IoT Events alarmes, mais pas aux alarmes externes.

Rubriques

- Répondre à une alarme (console)
- Répondre à une alarme (API)

Répondre à une alarme (console)

Vous pouvez utiliser la AWS IoT SiteWise console pour accuser réception, suspendre, désactiver ou activer une alarme.

Rubriques

- Confirmer une alarme (console)
- Suspendez une alarme (console)
- Désactiver une alarme (console)
- Activer une alarme (console)
- Réinitialiser une alarme (console)

Confirmer une alarme (console)

Vous pouvez accuser réception d'une alarme pour indiquer que vous êtes en train de résoudre le problème.

> **Note**
>
> Vous devez activer le flux d'accusé de réception de l'alarme afin de pouvoir accuser réception de l'alarme. Cette option est activée par défaut si vous définissez l'alarme depuis la AWS IoT SiteWise console.

Pour accuser réception d'une alarme (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Ressources.
3. Choisissez la ressource pour laquelle vous souhaitez accuser réception d'une alarme.

> **Tip**
>
> Vous pouvez cliquer sur l'icône en forme de flèche pour développer une hiérarchie de ressources afin de trouver votre ressource.

4. Choisissez l'onglet Alarmes.
5. Sélectionnez l'alarme pour accuser réception, puis choisissez Actions pour ouvrir le menu des actions de réponse.
6. Sélectionnez I acknowledge (Je confirme). L'état de l'alarme passe à Accusé.

Suspendez une alarme (console)

Vous pouvez suspendre une alarme pour la désactiver temporairement. Spécifiez la durée pendant laquelle l'alarme doit être interrompue.

Pour suspendre une alarme (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Ressources.
3. Choisissez la ressource pour laquelle vous souhaitez suspendre une alarme.

> **Tip**
>
> Vous pouvez cliquer sur l'icône en forme de flèche pour développer une hiérarchie de ressources afin de trouver votre ressource.

4. Choisissez l'onglet Alarmes.
5. Sélectionnez l'alarme à suspendre, puis choisissez Actions pour ouvrir le menu des actions de réponse.
6. Choisissez Snooze. Un modèle s'ouvre dans lequel vous spécifiez la durée de la pause.

7. Choisissez la durée du rappel ou entrez une durée de rappel personnalisée.
8. Choisissez Enregistrer. L'état de l'alarme passe à Snoozed.

Désactiver une alarme (console)

Vous pouvez désactiver une alarme pour qu'elle ne soit plus détectée. Après avoir désactivé l'alarme, vous devez la réactiver si vous souhaitez qu'elle soit détectée.

Pour désactiver une alarme (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Ressources.
3. Choisissez l'actif pour lequel vous souhaitez désactiver une alarme.

> **Tip**
>
> Vous pouvez cliquer sur l'icône en forme de flèche pour développer une hiérarchie de ressources afin de trouver votre ressource.

4. Choisissez l'onglet Alarmes.
5. Sélectionnez l'alarme à désactiver, puis choisissez Actions pour ouvrir le menu des actions de réponse.
6. Choisissez Désactiver. L'état de l'alarme passe à Désactivé.

Activer une alarme (console)

Vous pouvez activer une alarme pour qu'elle soit à nouveau détectée après l'avoir désactivée ou mise en pause.

Pour activer une alarme (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Ressources.
3. Choisissez la ressource pour laquelle vous souhaitez activer une alarme.

> **Tip**
>
> Vous pouvez cliquer sur l'icône en forme de flèche pour développer une hiérarchie de ressources afin de trouver votre ressource.

4. Choisissez l'onglet Alarmes.
5. Sélectionnez l'alarme à activer, puis choisissez Actions pour ouvrir le menu des actions de réponse.
6. Sélectionnez Activer. L'état de l'alarme passe à Normal.

Réinitialiser une alarme (console)

Vous pouvez réinitialiser une alarme pour effacer son état et sa dernière valeur.

Pour réinitialiser une alarme (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Ressources.
3. Choisissez l'actif pour lequel vous souhaitez réinitialiser une alarme.

> **Tip**
>
> Vous pouvez cliquer sur l'icône en forme de flèche pour développer une hiérarchie de ressources afin de trouver votre ressource.

4. Choisissez l'onglet Alarmes.
5. Sélectionnez l'alarme à activer, puis choisissez Actions pour ouvrir le menu des actions de réponse.
6. Choisissez Réinitialiser. L'état de l'alarme passe à Normal.

Répondre à une alarme (API)

Vous pouvez utiliser l' AWS IoT Events API pour accuser réception, suspendre, désactiver, activer ou réinitialiser une alarme. Pour plus d'informations, consultez les opérations suivantes dans le manuel de référence des AWS IoT Events API :

- BatchAcknowledgeAlarme
- BatchSnoozeAlarme
- BatchDisableAlarme
- BatchEnableAlarme
- BatchResetAlarme

Pour plus d'informations, consultez la section Répondre aux alarmes dans le guide du AWS IoT Events développeur.

Ingestion de l'état d'alarme externe

Les alarmes externes sont des alarmes que vous évaluez en dehors de celles-ci AWS IoT SiteWise. Vous pouvez utiliser des alarmes externes lorsqu'une source de données indique l'état des alarmes que vous souhaitez ingérer AWS IoT SiteWise.

Les propriétés d'état d'alarme nécessitent un format spécifique pour les valeurs des données d'état d'alarme. Chaque valeur de données doit être un objet JSON sérialisé sous forme de chaîne. Ensuite, vous ingérez la chaîne sérialisée sous forme de valeur de chaîne. Pour plus d'informations, consultez Propriétés de l'état de l'alarme.

Example Exemple de valeur de données d'état d'alarme (non sérialisée)

```
{
  "stateName": "Active"
}
```

Example Exemple de valeur de données d'état d'alarme (sérialisée)

```
{\"stateName\":\"Active\"}
```

> **Note**
>
> Si votre source de données ne peut pas fournir de données dans ce format, ou si vous ne pouvez pas convertir vos données dans ce format avant de les ingérer, vous pouvez choisir de ne pas utiliser de propriété d'alarme. Au lieu de cela, vous pouvez ingérer les données en tant que propriété de mesure avec le type de données chaîne, par exemple. Pour

plus d'informations, consultez Définition des flux de données provenant des équipements (mesures) et Ingestion de données pour AWS IoT SiteWise.

Cartographie des flux d'état d'alarme externes

Vous pouvez définir des alias de propriété pour mapper vos flux de données aux propriétés de l'état de votre alarme. Cela vous permet d'identifier facilement une propriété d'état d'alarme lorsque vous ingérez ou récupérez des données. Pour plus d'informations sur les alias de propriété, consultezMappage des flux de données industrielles avec des propriétés de ressources.

Rubriques

- Cartographie des flux d'état des alarmes externes (console)
- Cartographie des flux d'état d'alarme externes (AWS CLI)

Cartographie des flux d'état des alarmes externes (console)

Vous pouvez définir des alias de propriété pour mapper vos flux de données aux propriétés de l'état de votre alarme. Cela vous permet d'identifier facilement une propriété d'état d'alarme lorsque vous ingérez ou récupérez des données. Pour plus d'informations sur les alias de propriété, consultezMappage des flux de données industrielles avec des propriétés de ressources.

Vous pouvez utiliser la AWS IoT SiteWise console pour définir un alias pour une propriété d'état d'alarme.

Pour définir un alias de propriété pour une propriété d'état d'alarme (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Ressources.
3. Choisissez la ressource pour laquelle vous souhaitez définir un alias de propriété.

   > **Tip**
   >
   > Vous pouvez cliquer sur l'icône en forme de flèche pour développer une hiérarchie de ressources afin de trouver votre ressource.

4. Choisissez Modifier.

5. Faites défiler la page jusqu'à Alarmes et développez la section.
6. Sous Alarmes externes, entrez l'alias dans Alias de propriété — facultatif.
7. Choisissez Enregistrer.

Cartographie des flux d'état d'alarme externes (AWS CLI)

Vous pouvez définir des alias de propriété pour mapper vos flux de données aux propriétés de l'état de votre alarme. Cela vous permet d'identifier facilement une propriété d'état d'alarme lorsque vous ingérez ou récupérez des données. Pour plus d'informations sur les alias de propriété, consultezMappage des flux de données industrielles avec des propriétés de ressources.

Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour définir un alias pour une propriété d'état d'alarme.

Vous devez connaître l'`assetId` de votre ressource et le `propertyId`de la propriété pour effectuer cette procédure. Vous pouvez également utiliser l'identifiant externe. Si vous avez créé un actif et que vous ne le connaissez pas`assetId`, utilisez l'ListAssetsAPI pour répertorier tous les actifs d'un modèle spécifique. Utilisez cette DescribeAssetopération pour afficher les propriétés de votre actif, y compris les identifiants de propriété.

> **Note**
>
> La DescribeAssetréponse inclut la liste des modèles d'actifs composites pour l'actif. Chaque alarme est un modèle composite. Pour trouver le`propertyId`, recherchez le modèle composite de l'alarme, puis recherchez la `AWS/ALARM_STATE` propriété dans ce modèle composite.

Pour plus d'informations sur la définition de l'alias de propriété, consultezDéfinition d'un alias de propriété (AWS CLI).

Ingestion des données d'état des alarmes

Les propriétés d'état d'alarme prévoient un état d'alarme sous forme de chaîne JSON sérialisée. Pour intégrer l'état d'alarme à une alarme externe AWS IoT SiteWise, vous devez ingérer cette chaîne sérialisée sous forme de valeur de chaîne horodatée. L'exemple suivant montre une valeur de données d'état pour une alarme active.

```
{\"stateName\":\"Active\"}
```

Pour identifier une propriété d'état d'alarme, vous pouvez spécifier l'une des options suivantes :

- La `assetId` fin `propertyId` de la propriété d'alarme à laquelle vous envoyez des données.
- Le`propertyAlias`, qui est un alias de flux de données (par exemple,`/company/windfarm/3/turbine/7/temperature/high`). Pour utiliser cette option, vous devez d'abord définir l'alias de la propriété de votre alarme. Pour savoir comment définir des alias de propriété pour les propriétés d'état des alarmes, consultezCartographie des flux d'état d'alarme externes.

L'exemple de charge utile de l'API BatchPutAssetPropertyValue suivant montre comment formater l'état d'une alarme externe. Cette alarme externe signale lorsque le nombre de rotations par minute (RPM) d'une éolienne est trop élevé.

Example Exemple de BatchPutAssetPropertyValue charge utile pour les données d'état des alarmes

```
{
    "entries": [
      {
        "entryId": "unique entry ID",
        "propertyAlias": "/company/windfarm/3/turbine/7/temperature/high",
        "propertyValues": [
          {
            "value": {
              "stringValue": "{\"stateName\":\"Active\"}"
            },
            "timestamp": {
              "timeInSeconds": 1607550262
            }
          }
        ]
      }
    ]
  }
```

Pour plus d'informations sur l'utilisation de l'`BatchPutAssetPropertyValue`API pour ingérer des données, consultezIngestion de données à l'aide de l'API AWS IoT SiteWise.

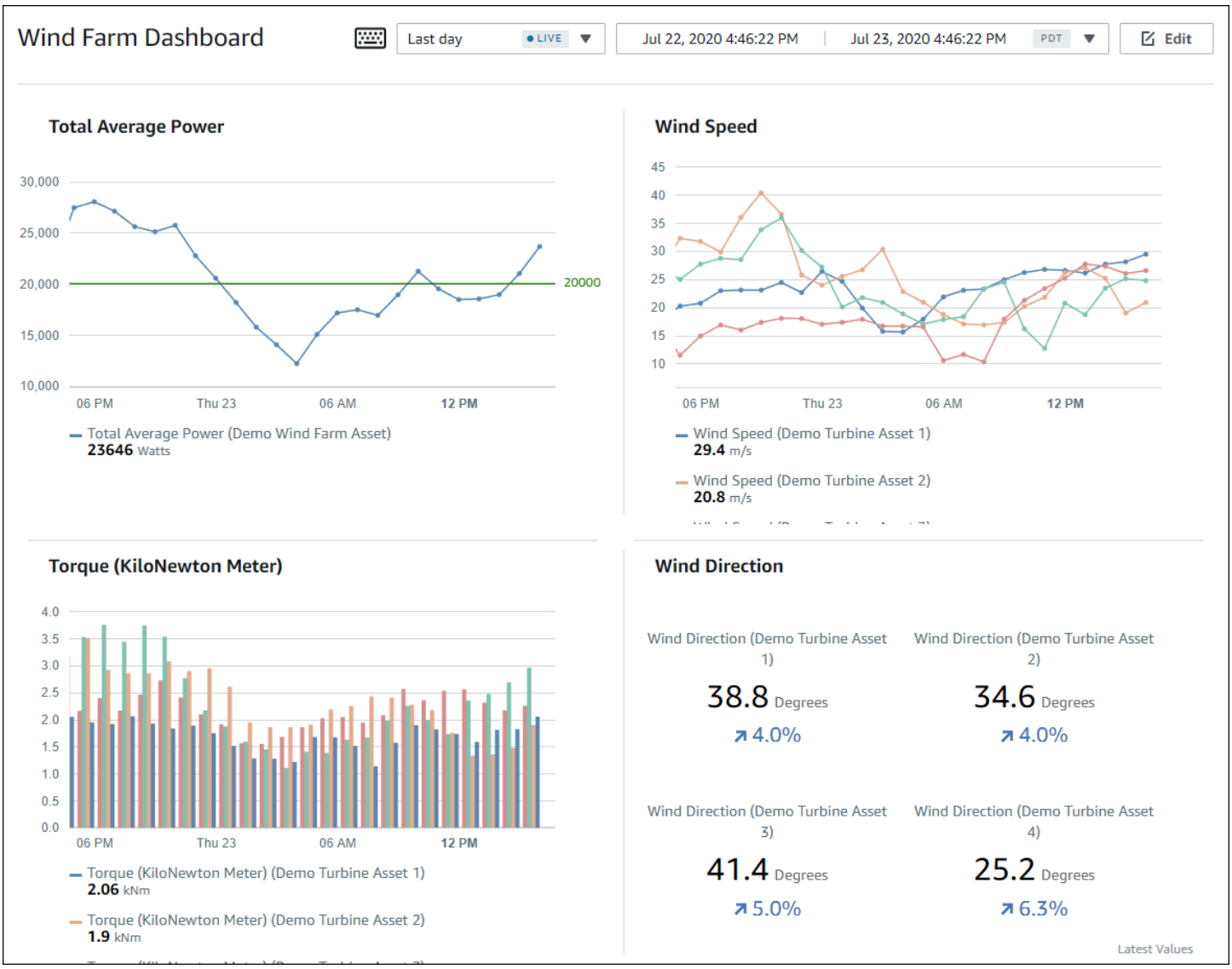
Pour plus d'informations sur les autres méthodes d'ingestion de données, consultezIngestion de données pour AWS IoT SiteWise.

Surveillance des données avec AWS IoT SiteWise Monitor

Vous pouvez l'utiliser AWS IoT SiteWise pour surveiller les données de vos processus, appareils et équipements en créant des portails Web SiteWise Monitor. SiteWise Monitor est une fonctionnalité AWS IoT SiteWise que vous pouvez utiliser pour créer des portails sous la forme d'une application Web gérée. Vous pouvez ensuite utiliser ces portails pour afficher et partager vos données opérationnelles. Vous pouvez créer des projets avec des tableaux de bord pour visualiser les données de vos processus, périphériques et équipements connectés à AWS IoT.

Les experts de domaine, tels que les ingénieurs de processus, peuvent utiliser ces portails pour obtenir rapidement des informations sur leurs données opérationnelles afin de comprendre le comportement des appareils et des équipements.

Voici un exemple de tableau de bord qui affiche les données d'un parc éolien.



Comme il AWS IoT SiteWise capture les données au fil du temps, vous pouvez utiliser SiteWise Monitor pour visualiser les données opérationnelles au fil du temps ou les dernières valeurs signalées à des moments spécifiques. Cela vous permet de découvrir des informations qui sont généralement difficiles à trouver.

SiteWise Contrôler les rôles

Quatre rôles interagissent avec SiteWise Monitor :

AWS administrateur

L' AWS administrateur utilise la AWS IoT SiteWise console pour créer des portails. L'administrateur AWS peut également affecter des administrateurs de portail et ajouter des

utilisateurs de portail. Les administrateurs du portail attribueront ultérieurement des utilisateurs du portail à des projets en tant que propriétaires ou utilisateurs standard. L' AWS administrateur travaille exclusivement dans la AWS console.

Administrateur du portail

Chaque portail SiteWise Monitor possède un ou plusieurs administrateurs de portail. Les administrateurs du portail utilisent ce dernier pour créer des projets contenant des collections de ressources et de tableaux de bord. Ils attribuent ensuite des ressources et des propriétaires à chaque projet. En contrôlant l'accès au projet, les administrateurs de portail spécifient les ressources que les propriétaires et les utilisateurs de projet peuvent voir.

Propriétaire du projet

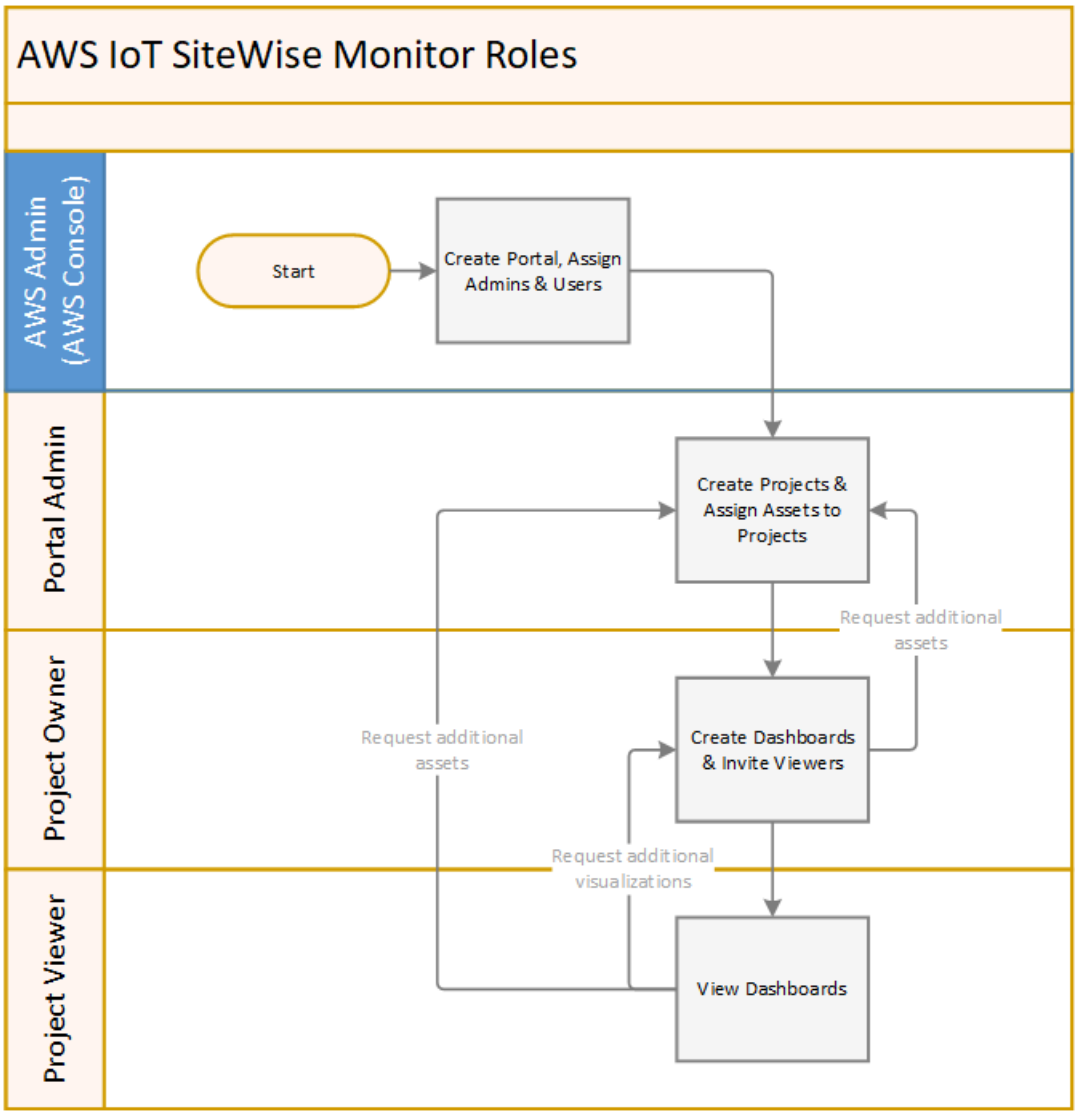
Chaque projet SiteWise Monitor a des propriétaires. Ces propriétaires créent des visualisations sous la forme de tableaux de bord afin de représenter les données opérationnelles de manière cohérente. Lorsque les tableaux de bord sont prêts à être partagés, tout propriétaire du projet peut inviter des utilisateurs. Les propriétaires de projet peuvent également affecter d'autres propriétaires au projet. Les propriétaires de projets peuvent configurer des seuils et des paramètres de notification pour les alarmes.

Utilisateur de projet

Chaque projet SiteWise Monitor possède des spectateurs. Les utilisateurs de projet peuvent se connecter au portail pour consulter les tableaux de bord créés par les propriétaires de projet. Dans chaque tableau de bord, les utilisateurs du projet peuvent ajuster la plage de temps pour mieux comprendre les données opérationnelles. Les utilisateurs de projet ne peuvent afficher que les tableaux de bord des projets auxquels ils ont accès. Les spectateurs du projet peuvent accuser réception des alarmes et les suspendre.

Selon votre organisation, la même personne peut jouer plusieurs rôles.

L'image suivante montre comment ces quatre rôles interagissent dans le portail SiteWise Monitor.



Vous pouvez gérer qui a accès à vos données en utilisant AWS IAM Identity Center ou IAM. Les utilisateurs de vos données peuvent se connecter à SiteWise Monitor depuis un navigateur de bureau ou mobile à l'aide de leurs informations d'identification IAM Identity Center ou IAM.

Fédération SAML

IAM Identity Center et IAM prennent en charge la fédération des identités avec le langage SAML (Security Assertion Markup Language) 2.0. SAML 2.0 est un standard ouvert que de nombreux fournisseurs d'identité externes (IdPs) utilisent pour authentifier les utilisateurs et transmettre leur identité et leurs informations de sécurité aux fournisseurs de services (SP). Les SP sont généralement des applications ou des services. La fédération SAML permet aux administrateurs et aux utilisateurs de votre portail SiteWise Monitor de se connecter aux portails qui leur sont assignés à

l'aide d'informations d'identification externes, telles que le nom d'utilisateur et le mot de passe de leur entreprise.

Vous pouvez configurer IAM Identity Center et IAM pour utiliser la fédération basée sur SAML pour accéder à vos portails Monitor. SiteWise

IAM Identity Center

Les administrateurs et les utilisateurs de votre portail peuvent se connecter au portail d' AWS accès à l'aide de leur nom d'utilisateur et de leur mot de passe d'entreprise. Ils peuvent ensuite accéder aux portails de SiteWise surveillance qui leur sont assignés. IAM Identity Center utilise des certificats pour établir une relation de confiance SAML entre votre fournisseur d'identité et. AWS Pour plus d'informations, le profil SCIM et l'implémentation de SAML 2.0 sont disponibles dans le guide de l'AWS IAM Identity Center utilisateur.

IAM

Les administrateurs et utilisateurs de votre portail peuvent demander des informations d'identification de sécurité temporaires pour accéder aux portails SiteWise Monitor qui leur sont assignés. Vous créez une identité de fournisseur d'identité SAML dans IAM pour établir une relation de confiance entre votre fournisseur d'identité et. AWS Pour plus d'informations, consultez la section Utilisation de la fédération basée sur SAML pour l'accès à l'API dans le AWS guide de l'utilisateur IAM.

Les administrateurs et utilisateurs de votre portail peuvent se connecter au portail de votre entreprise et sélectionner l'option permettant d'accéder à la console AWS de gestion. Ils peuvent ensuite accéder aux portails de SiteWise surveillance qui leur sont assignés. Le portail de votre entreprise gère l'échange de confiance entre votre fournisseur d'identité et AWS. Pour plus d'informations, consultez la section Permettre aux utilisateurs fédérés SAML 2.0 d'accéder à la console de AWS gestion dans le guide de l'utilisateur IAM.

> **Note**
>
> Lorsque vous ajoutez des utilisateurs ou des administrateurs au portail, évitez de créer des politiques IAM qui limitent les autorisations des utilisateurs, telles qu'une adresse IP limitée. Les politiques associées avec des autorisations restreintes ne pourront pas se connecter au AWS IoT SiteWise portail.

SiteWise Concepts de surveillance

Pour utiliser SiteWise Monitor, vous devez connaître les concepts suivants :

Portal

Un AWS IoT SiteWise Monitor portail est une application Web que vous pouvez utiliser pour visualiser et partager vos AWS IoT SiteWise données. Un portail compte un ou plusieurs administrateurs et contient zéro ou plusieurs projets.

Projet

Chaque portail SiteWise Monitor contient un ensemble de projets. Chaque projet est associé à un sous-ensemble de vos ressources AWS IoT SiteWise . Les propriétaires de projet créent un ou plusieurs tableaux de bord pour fournir un moyen cohérent de visualiser les données liées à ces ressources. Ils peuvent inviter des utilisateurs standard dans le projet pour leur permettre d'en consulter les ressources et les tableaux de bord. Le projet est l'unité de base du partage au sein de SiteWise Monitor. Les propriétaires de projets peuvent inviter les utilisateurs auxquels l' AWS administrateur a donné accès au portail. Tout utilisateur doit avoir accès à un portail avant qu'un projet de ce portail puisse être partagé avec lui.

Ressource

Lorsque des données sont ingérées AWS IoT SiteWise depuis votre équipement industriel, vos appareils, équipements et processus sont chacun représentés comme des actifs. Chaque actif possède des propriétés et des alarmes qui lui sont associées. L'administrateur du portail affecte des ensembles de ressources à chaque projet.

Propriété

Les propriétés sont des séries chronologiques associées à des actifs. Par exemple, une pièce d'équipement peut avoir un numéro de série, un emplacement, une marque et un modèle, ainsi qu'une date d'installation. Elle peut également comporter des valeurs de séries chronologiques pour la disponibilité, les performances, la qualité, la température, la pression, etc.

alerte

Les alarmes surveillent les propriétés pour identifier lorsque l'équipement se trouve en dehors de sa plage de fonctionnement. Chaque alarme définit un seuil et une propriété à surveiller. Lorsque la propriété dépasse le seuil, l'alarme s'active et indique que vous ou un membre de votre équipe devez régler le problème. Les propriétaires de projets peuvent personnaliser les seuils

et les paramètres de notification pour les alarmes. Les spectateurs du projet peuvent accuser réception des alarmes et les suspendre, et ils peuvent laisser un message contenant des détails sur l'alarme ou sur les mesures prises pour y remédier.

Tableau de bord

Chaque projet contient un ensemble de tableaux de bord. Les tableaux de bord fournissent un ensemble de visualisations pour les valeurs d'un ensemble de ressources. Les propriétaires de projet créent les tableaux de bord et les visualisations qu'il contient. Lorsqu'un propriétaire de projet est prêt à partager l'ensemble de tableaux de bord, il peut inviter des utilisateurs dans le projet, ce qui leur donne accès à tous les tableaux de bord correspondants. Si vous souhaitez affecter différents groupes d'utilisateurs à différents tableaux de bord, vous devez diviser les tableaux de bord entre plusieurs projets. Lorsque les utilisateurs consultent les tableaux de bord, ils peuvent personnaliser la plage horaire pour examiner des données spécifiques.

Visualisation

Dans chaque tableau de bord, les propriétaires de projet décident comment afficher les propriétés et les alarmes des actifs associés au projet. La disponibilité peut être représentée sous forme de graphique linéaire, tandis que d'autres valeurs peuvent être affichées sous forme de diagrammes à barres ou d'indicateurs de performance clés (KPI). Il est préférable d'afficher les alarmes sous forme de grilles d'état et de chronologies d'état. Les propriétaires de projet personnalisent chaque visualisation pour fournir une compréhension optimale des données de la ressource concernée.

Commencer avec AWS IoT SiteWise Monitor

Si vous êtes l' AWS administrateur de votre organisation, vous créez des portails à partir de la AWS IoT SiteWise console. Procédez comme suit pour créer un portail afin que les membres de votre organisation puissent consulter vos AWS IoT SiteWise données :

1. Configurer et créer un portail
2. Ajouter des administrateurs de portail et envoyer des e-mails d'invitation
3. Ajouter des utilisateurs de portail

Après avoir créé un portail, l'administrateur du portail peut consulter vos AWS IoT SiteWise actifs et les affecter à des projets sur le portail. Les propriétaires de projet peuvent ensuite créer des tableaux de bord pour visualiser les propriétés des ressources qui aident les utilisateurs de projet à comprendre les performances de vos appareils, processus et équipement.

> **Note**
>
> Lorsque vous ajoutez des utilisateurs ou des administrateurs au portail, évitez de créer des politiques AWS Identity and Access Management (IAM) qui limitent les autorisations des utilisateurs, telles qu'une adresse IP limitée. Les politiques associées avec des autorisations restreintes ne pourront pas se connecter au AWS IoT SiteWise portail.

Vous pouvez suivre un didacticiel qui décrit les étapes requises pour configurer un portail avec un projet, des tableaux de bord et plusieurs utilisateurs pour un scénario spécifique à l'aide de données de parc éolien. Pour plus d'informations, consultez Visualisation et partage des données des parcs éoliens dans Monitor SiteWise .

Rubriques

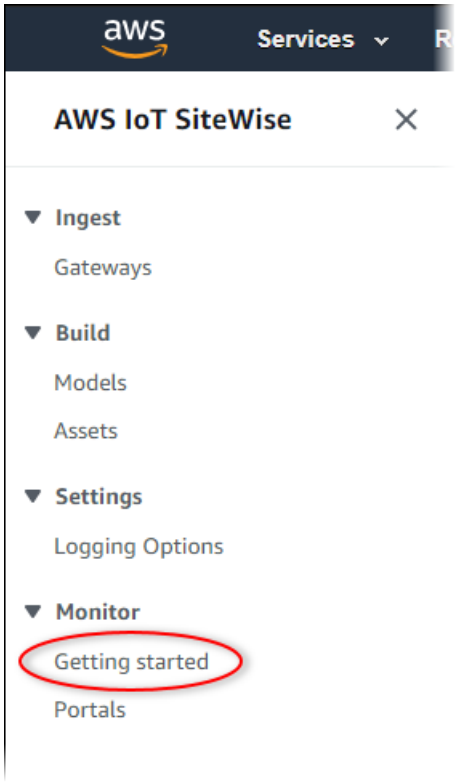
- Création d'un portail
- Configuration de votre portail
- Invitation des administrateurs
- Ajout d'utilisateurs du portail

Création d'un portail

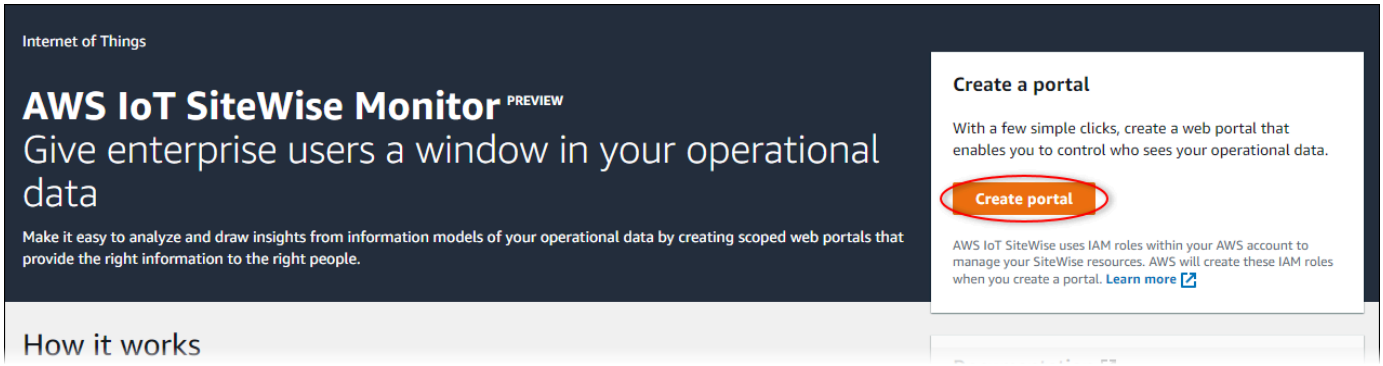
Vous créez un portail SiteWise Monitor dans la AWS IoT SiteWise console.

Pour créer un portail

1. Connectez-vous à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Moniteur, Mise en route.



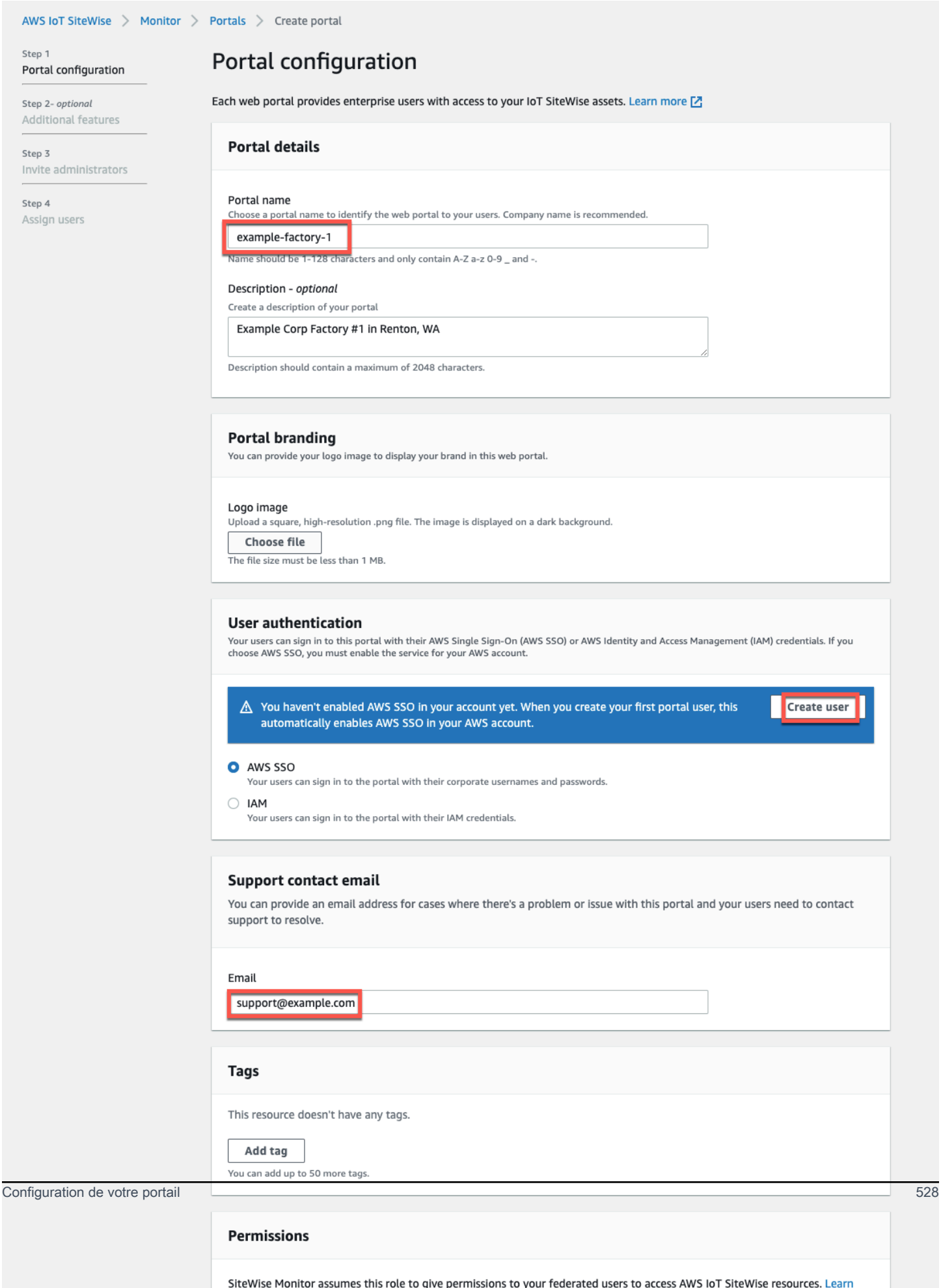
3. Choisissez Créer un portail.



Ensuite, vous devez fournir quelques informations de base pour configurer votre portail.

Configuration de votre portail

Les utilisateurs utilisent des portails pour afficher vos données. Vous pouvez personnaliser le nom, la description, l'image de marque, l'authentification des utilisateurs, l'e-mail de contact du service d'assistance et les autorisations d'un portail.


AWS IoT SiteWise > Monitor > Portals > Create portal
Step 1
Portal configuration
Step 2- optional
Additional features
Step 3
Invite administrators
Step 4
Assign users
Portal configuration
Each web portal provides enterprise users with access to your IoT SiteWise assets. Learn more
Portal details
Portal name
Choose a portal name to identify the web portal to your users. Company name is recommended.
example-factory-1
Name should be 1-128 characters and only contain A-Z a-z 0-9 _ and -.
Description - optional
Create a description of your portal
Example Corp Factory #1 in Renton, WA
Description should contain a maximum of 2048 characters.
Portal branding
You can provide your logo image to display your brand in this web portal.
Logo image
Upload a square, high-resolution .png file. The image is displayed on a dark background.
Choose file
The file size must be less than 1 MB.
User authentication
Your users can sign in to this portal with their AWS Single Sign-On (AWS SSO) or AWS Identity and Access Management (IAM) credentials. If you choose AWS SSO, you must enable the service for your AWS account.
You haven't enabled AWS SSO in your account yet. When you create your first portal user, this automatically enables AWS SSO in your AWS account.
Create user
AWS SSO
Your users can sign in to the portal with their corporate usernames and passwords.
IAM
Your users can sign in to the portal with their IAM credentials.
Support contact email
You can provide an email address for cases where there's a problem or issue with this portal and your users need to contact support to resolve.
Email
support@example.com
Tags
This resource doesn't have any tags.
Add tag
You can add up to 50 more tags.
Permissions
SiteWise Monitor assumes this role to give permissions to your federated users to access AWS IoT SiteWise resources. Learn

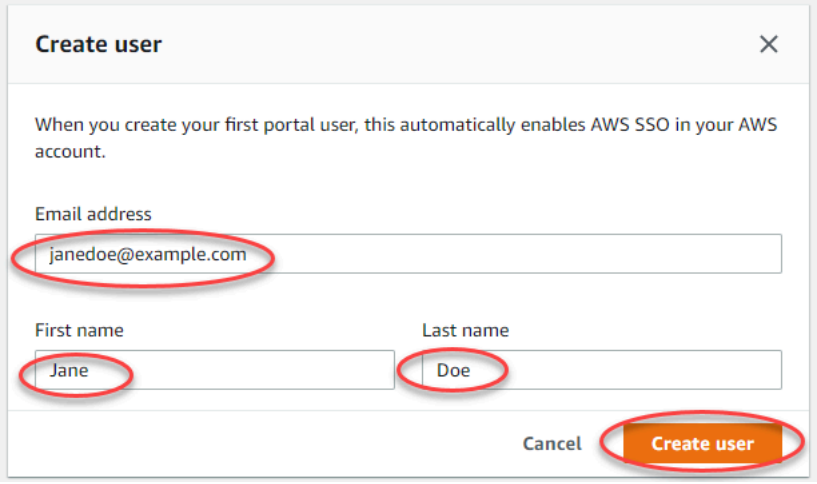
Pour configurer un portail

1. Entrez un nom pour votre portail.
2. (Facultatif) Saisissez une description pour votre portail. Si vous avez plusieurs portails, utilisez des descriptions significatives pour vous aider à suivre ce que contient chaque portail.
3. (Facultatif) Chargez une image pour afficher votre marque dans le portail. Choisissez une image PNG carrée. Si vous chargez une image qui n'est pas carrée, le portail réduit l'image à un carré.
4. Choisissez l'une des options suivantes :
   - Choisissez IAM Identity Center si les utilisateurs de votre portail se connectent à ce portail avec leur nom d'utilisateur et leur mot de passe d'entreprise.

     Si vous n'avez pas activé IAM Identity Center dans votre compte, procédez comme suit :

     a. Choisissez Create user (Créer un utilisateur).

     b. Sur la page Créer un utilisateur, pour créer le premier portail, entrez l'adresse e-mail, le prénom et le nom de famille de l'utilisateur, puis choisissez Créer un utilisateur.



> **Note**
>
> - AWS active automatiquement IAM Identity Center dans votre compte lorsque vous créez le premier utilisateur du portail.
> - Vous ne pouvez configurer IAM Identity Center que dans une seule région à la fois. SiteWise Monitor se connecte à la région que vous avez configurée pour IAM Identity Center. Cela signifie que vous utilisez une région pour

accéder à l'IAM Identity Center, mais que vous pouvez créer des portails dans n'importe quelle région.

- Choisissez IAM si les utilisateurs de votre portail se connectent à ce portail avec leurs informations d'identification IAM.

> **Important**
>
> Les utilisateurs ou les rôles doivent être autorisés à se connecter au portail. `iotsitewise:DescribePortal`

5. Entrez une adresse e-mail que les utilisateurs du portail peuvent contacter lorsqu'ils ont un problème avec le portail et ont besoin d'aide pour le résoudre.
6. (Facultatif) Ajoutez des balises pour votre portail. Pour plus d'informations, consultez Marquer vos ressources AWS IoT SiteWise.
7. Choisissez l'une des options suivantes :
   - Choisissez Créer et utilisez un nouveau rôle de service. Par défaut, SiteWise Monitor crée automatiquement un rôle de service pour chaque portail. Ce rôle permet aux utilisateurs de votre portail d'accéder à vos AWS IoT SiteWise ressources. Pour plus d'informations, consultez Utilisation des rôles de service pour AWS IoT SiteWise Monitor.
   - Choisissez Utiliser un rôle de service existant, puis choisissez le rôle cible.
8. Choisissez Next (Suivant)
9. (Facultatif) Activez les alarmes pour votre portail. Pour plus d'informations, consultez Activation des alarmes pour vos portails.
10. Choisissez Create. AWS IoT SiteWise créera votre portail.

> **Note**
>
> Si vous fermez la console, vous pouvez terminer le processus d'installation en ajoutant des administrateurs et des utilisateurs. Pour plus d'informations, consultez Ajout ou suppression d'administrateurs du portail. Si vous ne souhaitez pas conserver ce portail, supprimez-le afin qu'il n'utilise pas de ressources. Pour plus d'informations, consultez Suppression d'un portail.

La colonne Status peut prendre l'une des valeurs suivantes.

- AWS IoT SiteWise CREATING - traite votre demande de création du portail. Ce processus peut prendre plusieurs minutes.
- MISE À JOUR - AWS IoT SiteWise traite votre demande de mise à jour du portail. Ce processus peut prendre plusieurs minutes.
- PENDING - AWS IoT SiteWise attend la fin de la propagation de l'enregistrement DNS. Ce processus peut prendre plusieurs minutes. Vous pouvez supprimer le portail lorsque le statut est EN ATTENTE.
- AWS IoT SiteWise DELETING - traite votre demande de suppression du portail. Ce processus peut prendre plusieurs minutes.
- ACTIF - Lorsque le portail devient actif, les utilisateurs de votre portail peuvent y accéder.
- ÉCHEC - AWS IoT SiteWise Impossible de traiter votre demande de création, de mise à jour ou de suppression du portail. Si vous avez activé AWS IoT SiteWise l'envoi de journaux vers Amazon CloudWatch Logs, vous pouvez utiliser ces journaux pour résoudre les problèmes. Pour plus d'informations, consultez la section Surveillance AWS IoT SiteWise à l'aide de CloudWatch journaux.

Un message s'affiche lors de la création de votre portail.

Ensuite, vous devez inviter un ou plusieurs administrateurs de portail dans le portail. Jusqu'à présent, vous avez créé un portail mais personne ne peut y accéder.

Invitation des administrateurs

Pour commencer, vous devez affecter un administrateur à votre nouveau portail. L'administrateur du portail crée des projets, choisit les propriétaires de projets et affecte des ressources aux projets. Les administrateurs du portail peuvent consulter tous vos AWS IoT SiteWise actifs.

En fonction du service d'authentification utilisateur, choisissez l'une des options suivantes :

IAM Identity Center

Si vous utilisez SiteWise Monitor pour la première fois, vous pouvez choisir l'utilisateur que vous avez créé précédemment comme administrateur du portail. Si vous souhaitez ajouter un autre

utilisateur en tant qu'administrateur du portail, vous pouvez créer un utilisateur IAM Identity Center à partir de cette page. Vous pouvez également connecter un fournisseur d'identité externe à IAM Identity Center. Pour plus d'informations, consultez le Guide de l'utilisateur AWS IAM Identity Center.

Pour inviter les administrateurs

1. Activez les cases à cocher pour les utilisateurs qui seront administrateurs de votre portail. Cela ajoute les utilisateurs à la liste des administrateurs du portail.

   > **Note**
   >
   > Si vous utilisez IAM Identity Center comme banque d'identités et que vous êtes connecté à votre compte de AWS Organizations gestion, vous pouvez choisir Create user pour créer un utilisateur IAM Identity Center. IAM Identity Center envoie un e-mail au nouvel utilisateur pour qu'il définisse son mot de passe. Vous pouvez ensuite affecter l'utilisateur au portail en tant qu'administrateur. Pour plus d'informations, consultez la rubrique Manage identities in IAM Identity Center.

2. (Facultatif) Choisissez Envoyer l'invitation aux utilisateurs sélectionnés. Votre client de messagerie s'ouvre et une invitation est renseignée dans le corps du message.

   Vous pouvez personnaliser l'e-mail avant de l'envoyer aux administrateurs de votre portail. Vous pouvez également envoyer l'e-mail aux administrateurs de votre portail ultérieurement. Si vous essayez SiteWise Monitor pour la première fois et que vous ajoutez votre nouvel utilisateur ou rôle IAM Identity Center ou IAM en tant qu'administrateur du portail, vous n'avez pas besoin de vous envoyer un e-mail.
3. Si vous ajoutez un utilisateur que vous ne souhaitez pas en tant qu'administrateur, désactivez la case à cocher correspondant à cet utilisateur.
4. Lorsque vous avez terminé d'inviter les administrateurs du portail, choisissez Suivant.

IAM

Vous pouvez choisir un utilisateur ou un rôle pour être l'administrateur du portail. Si vous souhaitez ajouter un autre utilisateur ou un autre rôle en tant qu'administrateur du portail, vous pouvez créer un utilisateur ou un rôle dans la console IAM. Pour plus d'informations, consultez les sections Création d'un utilisateur IAM dans votre AWS compte et Création de rôles IAM dans le Guide de l'utilisateur IAM.

Pour inviter les administrateurs

1. Procédez comme suit :
   - Choisissez les utilisateurs IAM pour ajouter un utilisateur IAM en tant qu'administrateur de votre portail.
   - Choisissez les rôles IAM pour ajouter un rôle IAM en tant qu'administrateur du portail.
2. Cochez les cases correspondant aux utilisateurs ou aux rôles que vous souhaitez utiliser en tant qu'administrateurs de votre portail. Cela ajoute les utilisateurs ou les rôles à la liste des administrateurs du portail.
3. Si vous ajoutez un utilisateur ou un rôle que vous ne souhaitez pas utiliser en tant qu'administrateur, décochez la case correspondant à cet utilisateur ou à ce rôle.
4. Lorsque vous avez terminé d'inviter les administrateurs du portail, choisissez Suivant.

> **Important**
>
> Les utilisateurs ou les rôles doivent être `iotsitewise:DescribePortal` autorisés à se connecter au portail.

> **Note**
>
> Si vous utilisez IAM Identity Center comme banque d'identités et que vous êtes connecté à votre compte de AWS Organizations gestion, vous pouvez choisir Create user pour créer un utilisateur IAM Identity Center. IAM Identity Center envoie un e-mail au nouvel utilisateur pour qu'il définisse son mot de passe. Vous pouvez ensuite affecter l'utilisateur au portail en tant qu'administrateur. Pour plus d'informations, consultez la rubrique Manage identities in IAM Identity Center.

Vous pouvez modifier la liste des administrateurs de portail ultérieurement. Pour plus d'informations, consultez Ajout ou suppression d'administrateurs du portail.

> **Note**
>
> Étant donné que seul un administrateur de portail peut créer des projets et leur attribuer des actifs, vous devez spécifier au moins un administrateur de portail.

La dernière étape consiste à ajouter des utilisateurs qui peuvent accéder à votre nouveau portail.

Ajout d'utilisateurs du portail

Vous contrôlez les utilisateurs qui ont accès à vos portails. Dans chaque portail, les administrateurs du portail créent un ou plusieurs projets et attribuent des utilisateurs du portail en tant que propriétaires ou utilisateurs standard pour chaque projet. Chaque propriétaire de projet peut inviter d'autres utilisateurs de portail à administrer ou à afficher le projet.

En fonction du service d'authentification utilisateur, choisissez l'une des options suivantes :

IAM Identity Center

Si vous souhaitez ajouter un utilisateur à la liste des utilisateurs, procédez comme suit.

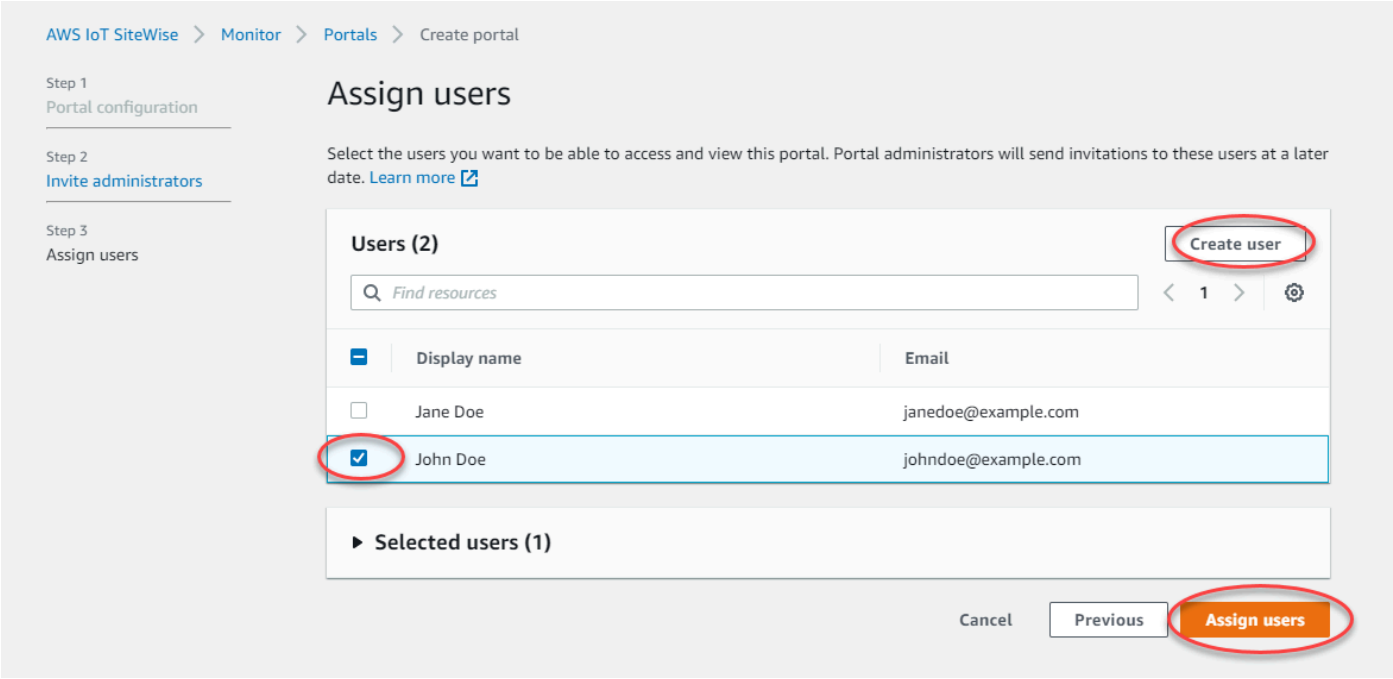
Pour ajouter des utilisateurs du portail

1. Dans la liste Utilisateurs, sélectionnez les utilisateurs à ajouter au portail. Cela ajoute les utilisateurs à la liste des utilisateurs du portail. Si vous utilisez SiteWise Monitor pour la première fois, il n'est pas nécessaire d'ajouter l'administrateur de votre portail en tant qu'utilisateur du portail.

   > **Note**
   >
   > Si vous utilisez IAM Identity Center comme banque d'identités et que vous êtes connecté à votre compte de AWS Organizations gestion, vous pouvez choisir Create user pour créer un utilisateur IAM Identity Center. IAM Identity Center envoie un e-mail au nouvel utilisateur pour qu'il définisse son mot de passe. Vous pouvez ensuite affecter l'utilisateur au portail en tant qu'utilisateur. Pour plus d'informations, consultez la rubrique Manage identities in IAM Identity Center.

2. Si vous ajoutez un utilisateur qui ne doit pas avoir accès au portail, désactivez la case à cocher correspondant à cet utilisateur.

3. Lorsque vous avez terminé de sélectionner des utilisateurs, choisissez Attribuer des utilisateurs.



IAM

Si vous voyez l'utilisateur ou le rôle que vous souhaitez ajouter dans la liste des utilisateurs ou des rôles IAM, procédez comme suit.

Pour ajouter des utilisateurs du portail

1. Utilisez les options suivantes :

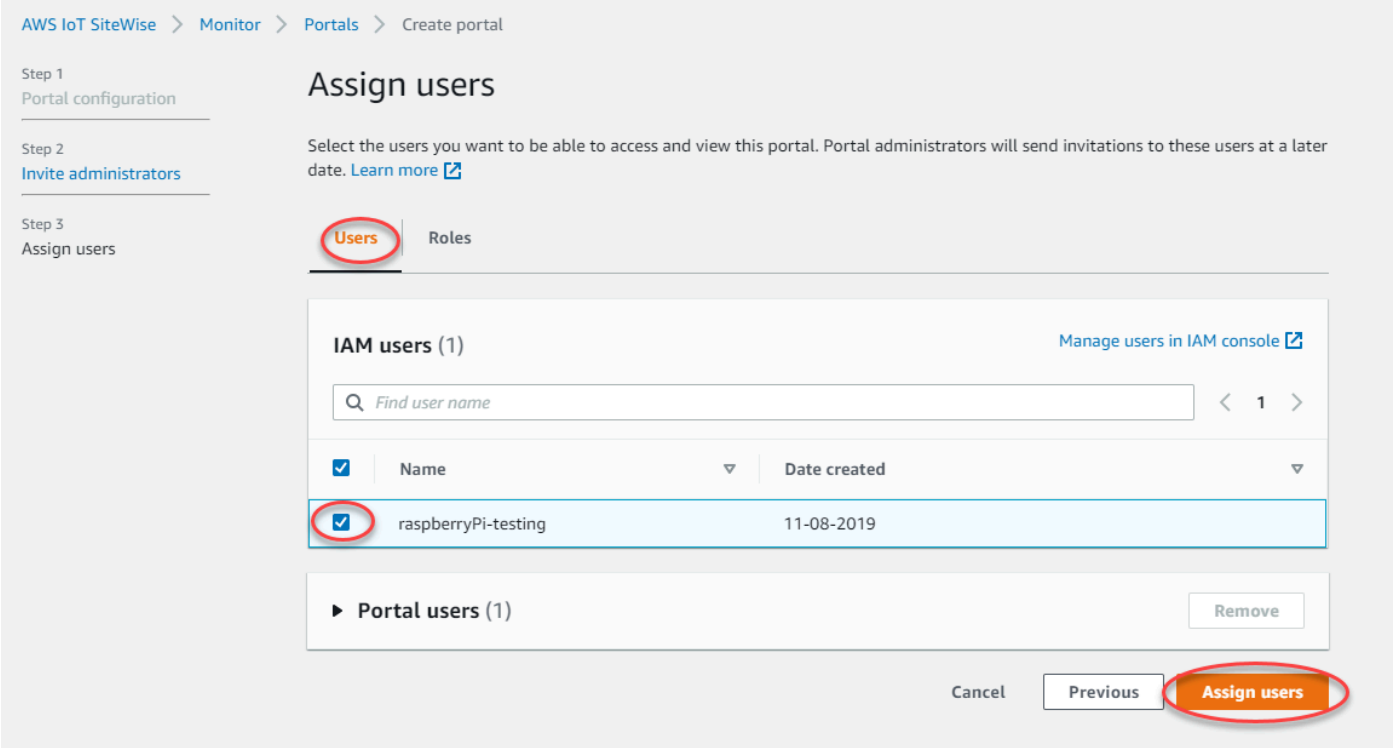
   - Choisissez les utilisateurs IAM pour ajouter un utilisateur IAM en tant qu'utilisateur du portail.
   - Choisissez les rôles IAM pour ajouter un rôle IAM en tant qu'utilisateur du portail.

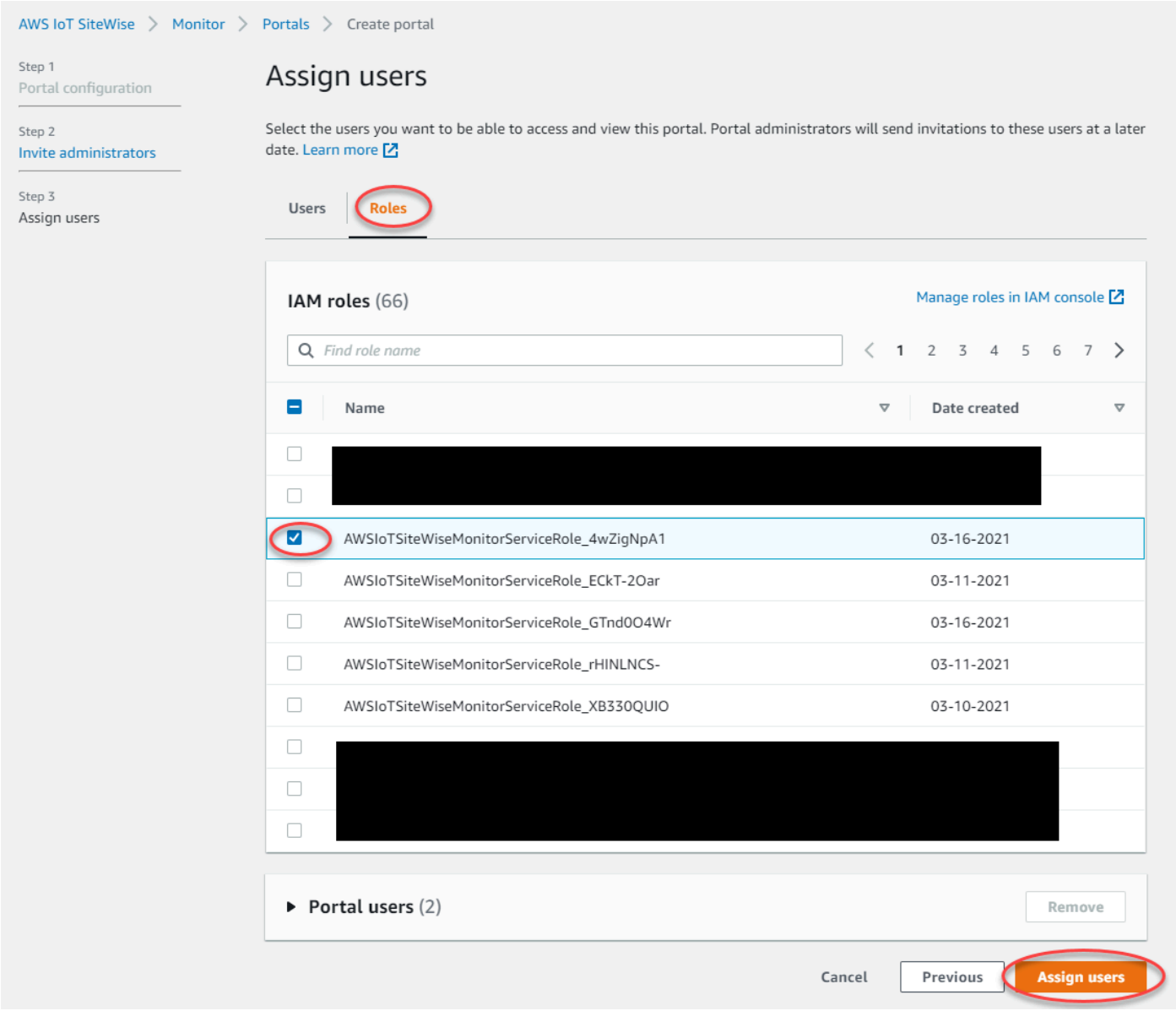
   Si vous utilisez SiteWise Monitor pour la première fois, il n'est pas nécessaire d'ajouter l'administrateur de votre portail en tant qu'utilisateur du portail.

2. Cochez les cases correspondant aux utilisateurs ou aux rôles que vous souhaitez utiliser en tant qu'utilisateurs du portail. Cela ajoute les utilisateurs ou les rôles à la liste des utilisateurs du portail.

3. Si vous ajoutez un utilisateur qui ne doit pas avoir accès au portail, désactivez la case à cocher correspondant à cet utilisateur.
4. Lorsque vous avez terminé de sélectionner des utilisateurs, choisissez Attribuer des utilisateurs.

> **Important**
>
> Les utilisateurs ou les rôles doivent être `iotsitewise:DescribePortal` autorisés à se connecter au portail.





Félicitations ! Vous avez créé avec succès un portail, affecté des administrateurs de portail et affecté des utilisateurs qui peuvent utiliser ce portail lorsqu'ils sont invités à le faire. Les administrateurs de votre portail peuvent désormais créer des projets et y ajouter des ressources. Ensuite, les propriétaires de votre projet pourront créer des tableaux de bord pour visualiser les données correspondant aux ressources de chaque projet.

Vous pourrez modifier la liste des utilisateurs du portail ultérieurement. Pour plus d'informations, consultez Ajout ou suppression d'utilisateurs du portail.

Si vous devez apporter des modifications au portail, reportez-vous à la section Administration de vos portails SiteWise Monitor.

Pour commencer à utiliser le portail, reportez-vous à la section Getting started du Guide de l'application SiteWise Monitor.

Création de tableaux de bord (AWS Command Line Interface)

Lorsque vous définissez des visualisations (ou des widgets) dans des tableaux de bord à l'aide de AWS CLI, vous devez spécifier les informations suivantes dans le document JSON `dashboardDefinition`. Cette définition est un paramètre des UpdateDashboardopérations CreateDashboardet.

`widgets`

Liste des structures de définition de widget contenant chacune les informations suivantes :

`type`

Type de widget. AWS IoT SiteWise fournit les types de widget suivants :

- `sc-line-chart`— Un graphique linéaire. Pour plus d'informations, voir les diagrammes linéaires dans le guide AWS IoT SiteWise Monitor d'application.
- `sc-scatter-chart`— Un diagramme de points. Pour plus d'informations, reportez-vous à la section Graphiques de points dans le guide AWS IoT SiteWise Monitor d'application.
- `sc-bar-chart`— Un graphique à barres. Pour plus d'informations, voir les diagrammes à barres dans le guide AWS IoT SiteWise Monitor d'application.
- `sc-status-grid`— Un widget d'état qui affiche la dernière valeur des propriétés des actifs sous forme de grille. Pour plus d'informations, consultez la section Widgets d'état dans le guide de AWS IoT SiteWise Monitor candidature.
- `sc-status-timeline`— Un widget d'état qui affiche les valeurs historiques des propriétés des actifs sous forme de chronologie. Pour plus d'informations, consultez la section Widgets d'état dans le guide de AWS IoT SiteWise Monitor candidature.
- `sc-kpi`— Une visualisation des indicateurs de performance clés (KPI). Pour plus d'informations, consultez la section Widgets KPI dans le guide de AWS IoT SiteWise Monitor l'application.
- `sc-table`— Un widget de tableau. Pour plus d'informations, consultez la section Widgets de tableau dans le guide de AWS IoT SiteWise Monitor l'application.

`title`

Le titre du widget.

`x`

Position horizontale du widget, à partir de la gauche de la grille. Cette valeur fait référence à la position du widget dans la grille du tableau de bord.

`y`

Position verticale du widget, à partir du haut de la grille. Cette valeur fait référence à la position du widget dans la grille du tableau de bord.

`width`

Largeur du widget, exprimée en nombre d'espaces sur la grille du tableau de bord.

`height`

Hauteur du widget, exprimée en nombre d'espaces sur la grille du tableau de bord.

`metrics`

Liste des structures de métrique qui définissent chacune un flux de données pour ce widget. Chaque structure de la liste doit contenir les informations suivantes :

`label`

Étiquette à afficher pour cette métrique.

`type`

Type de source de données pour cette mesure. AWS IoT SiteWise fournit les types de métriques suivants :

- `iotsitewise`— Le tableau de bord récupère les données d'une propriété d'actif dansAWS IoT SiteWise. Si vous choisissez cette option, vous devez définir `assetId` et `propertyId` pour cette métrique.

`assetId`

(Facultatif) ID d'une ressource dans AWS IoT SiteWise.

Ce champ est obligatoire si vous choisissez `iotsitewise` pour `type` cette métrique.

`propertyId`

(Facultatif) ID d'une propriété d'actif dans AWS IoT SiteWise.

Ce champ est obligatoire si vous choisissez `iotsitewise` pour `type` cette métrique.

`analysis`

(Facultatif) Structure qui définit l'analyse, telle que les courbes de tendance, à afficher pour le widget. Pour plus d'informations, consultez la section Configuration des courbes de tendance dans le Guide de AWS IoT SiteWise Monitor l'application. Vous pouvez ajouter une courbe de tendance de chaque type par propriété dans le widget. La structure d'analyse contient les informations suivantes :

`trends`

(Facultatif) Une liste de structures de tendance qui définissent chacune une analyse des tendances pour ce widget. Chaque structure de la liste contient les informations suivantes :

`type`

Type de ligne de tendance. Choisissez l'option suivante :

- `linear-regression`— Affiche une droite de régression linéaire. SiteWise Monitor utilise la méthode des moindres carrés pour calculer la régression linéaire.

`annotations`

(Facultatif) Une structure d'annotations qui définit les seuils pour le widget. Pour plus d'informations, consultez la section Configuration des seuils dans le Guide de AWS IoT SiteWise Monitor l'application. Vous pouvez ajouter jusqu'à six annotations par widget. La structure des annotations contient les informations suivantes :

`y`

(Facultatif) Liste des structures d'annotation qui définissent chacune un seuil horizontal pour ce widget. Chaque structure de la liste contient les informations suivantes :

`comparisonOperator`

L'opérateur de comparaison pour le seuil. Sélectionnez l'une des méthodes suivantes :

- `LT`— Mettez en évidence les propriétés dont au moins un point de données est inférieur à`value`.

- `GT`— Mettez en évidence les propriétés dont au moins un point de données est supérieur à`value`.
- `LTE`— Mettez en évidence les propriétés dont au moins un point de données est inférieur ou égal à`value`.
- `GTE`— Mettez en évidence les propriétés dont au moins un point de données est supérieur ou égal à`value`.
- `EQ`— Mettez en évidence les propriétés dont au moins un point de données est égal à`value`.

`value`

La valeur de seuil pour comparer les points de données avec`comparisonOperator`.

`color`

(Facultatif) Le code hexadécimal à 6 chiffres de la couleur du seuil. La visualisation affiche les légendes des propriétés dans cette couleur pour les propriétés dont au moins un point de données répond à la règle du seuil. La valeur par défaut est black (`#000000`).

`showValue`

(Facultatif) Indique s'il faut afficher ou non la valeur du seuil dans les marges du widget. La valeur par défaut est `true`.

`properties`

(Facultatif) Un dictionnaire plat des propriétés du widget. Les membres de cette structure dépendent du contexte. AWS IoT SiteWisefournit les widgets suivants qui utilisent `properties` :

- Les graphiques linéaires, les graphiques en nuage de points et les graphiques à barres présentent les propriétés suivantes :

  `colorDataAcrossThresholds`

  (Facultatif) S'il faut ou non modifier la couleur des données qui dépassent les seuils dans ce widget. Lorsque vous activez cette option, les données qui franchissent un seuil apparaissent dans la couleur que vous choisissez. La valeur par défaut est `true`.

- Les grilles de statut ont les propriétés suivantes :

`labels`

(Facultatif) Structure qui définit les étiquettes à afficher sur la grille d'état. La structure des étiquettes contient les informations suivantes :

`showValue`

(Facultatif) Indique s'il faut afficher ou non l'unité et la valeur de chaque propriété d'actif dans ce widget. La valeur par défaut est `true`.

Example Exemple de définition de tableau de bord

L'exemple suivant définit un tableau de bord à partir d'une charge utile stockée dans un fichier JSON.

```
aws iotsitewise create-dashboard \
  --project-id a1b2c3d4-5678-90ab-cdef-eeeeeEXAMPLE \
  --dashboard-name "Wind Farm Dashboard" \
  --dashboard-definition file://dashboard-definition.json
```

L'exemple JSON suivant pour `dashboard-definition.json` définit un tableau de bord avec les widgets de visualisation suivants :

- Graphique linéaire qui visualise la puissance totale du parc éolien en haut à gauche du tableau de bord. Ce graphique linéaire inclut un seuil qui indique le moment où le parc éolien produit moins d'énergie que sa production minimale attendue. Ce graphique linéaire inclut également une courbe de tendance de régression linéaire.
- Diagramme à barres qui visualise la vitesse du vent pour quatre turbines en haut à droite du tableau de bord.

> **Note**
>
> Cet exemple représente des visualisations de graphiques linéaires et à barres sur un tableau de bord. Ce tableau de bord est similaire à l'exemple de tableau de bord de parc éolien.

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

Activation des alarmes pour vos portails

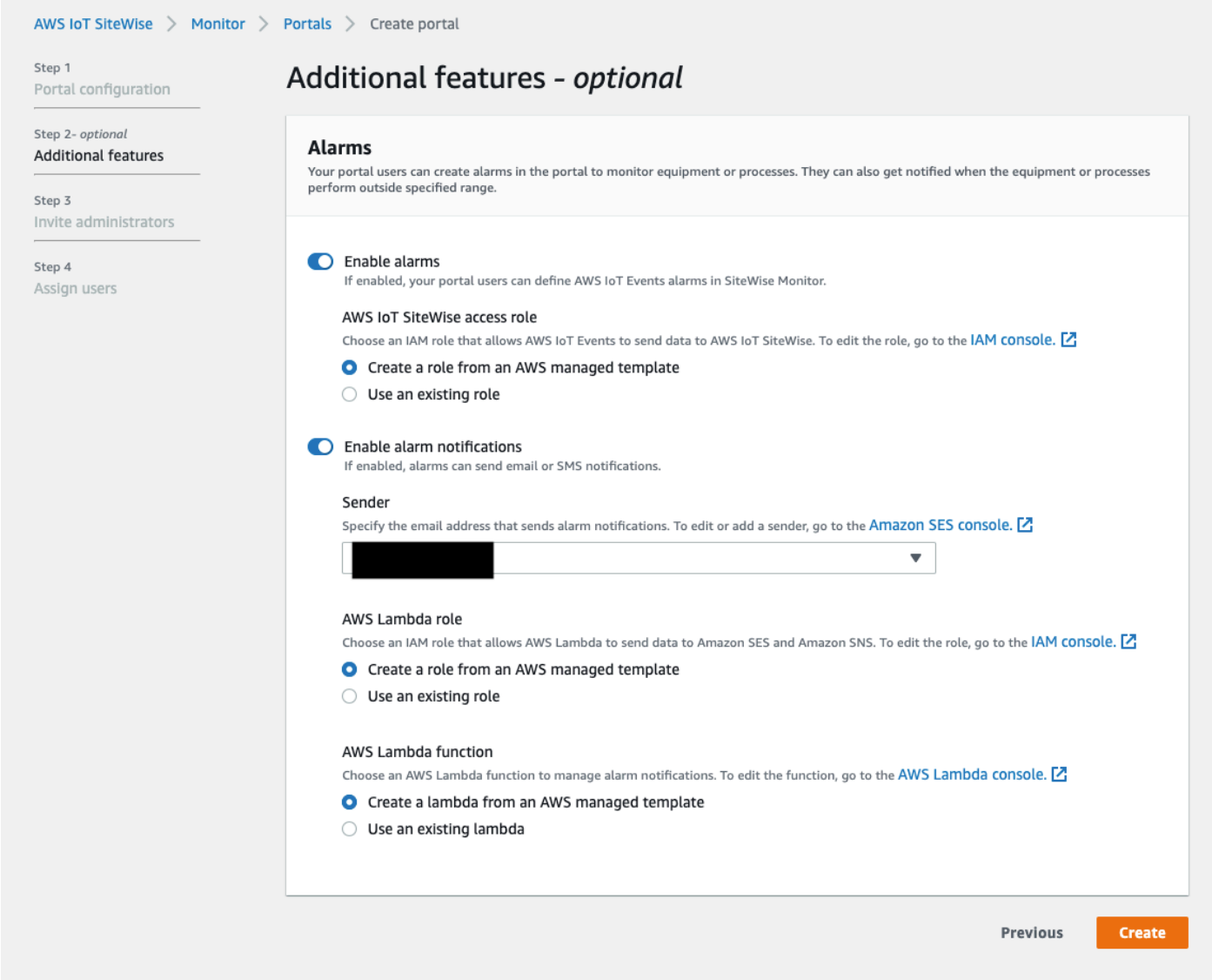
Vous pouvez activer la fonction d'alarmes prise en charge par AWS IoT Events for your portal afin que les administrateurs du portail puissent créer, modifier et supprimer des modèles AWS IoT Events d'alarme dans vos portails SiteWise Monitor. Les propriétaires de projets peuvent configurer des alarmes. Les spectateurs du projet peuvent consulter les détails des alarmes. Cette section explique comment utiliser la AWS IoT SiteWise console pour activer la fonction d'alarmes pour vos portails.

Important

- Vous ne pouvez pas créer d'alarmes externes dans vos portails.
- Si vous souhaitez envoyer des notifications d'alarme, vous devez choisir IAM Identity Center pour le service d'authentification des utilisateurs.
- La fonction de notification d'alarme n'est pas disponible en Chine (Pékin) Région AWS.

Lorsque vous configurez et créez un portail, vous pouvez activer les alarmes et les notifications d'alarme à l'étape 2 Fonctionnalités supplémentaires. En fonction du service d'authentification utilisateur, choisissez l'une des options suivantes :

IAM Identity Center



Pour activer les alarmes pour un portail

1. (Facultatif) Choisissez Activer les alarmes.

    - Pour le rôle d'AWS IoT SiteWise accès, utilisez un rôle existant ou créez un rôle avec les autorisations requises. Ce rôle nécessite l'`iotevents:BatchPutMessage`autorisation et une relation de confiance qui permettent `iot.amazonaws.com` et `iotevents.amazonaws.com` permettent d'assumer le rôle.

2. (Facultatif) Choisissez Activer les notifications d'alarme.

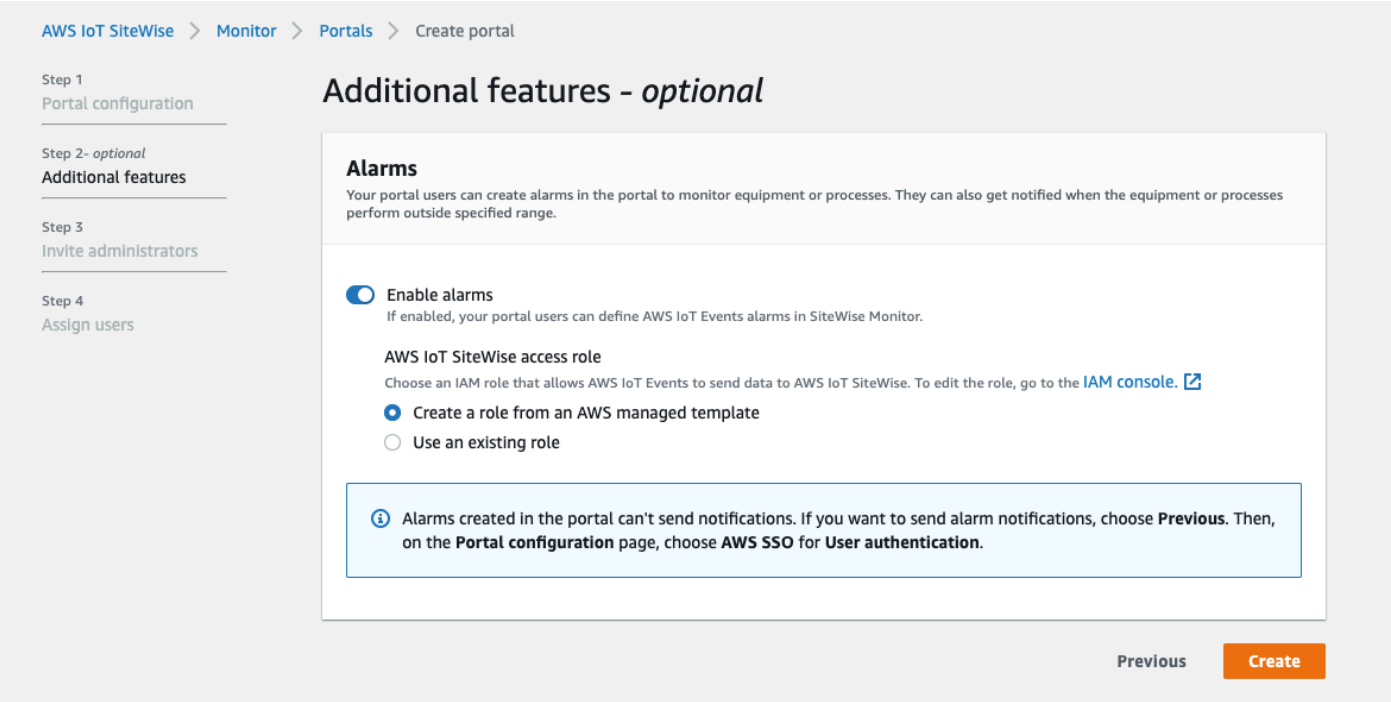
   a. Pour Expéditeur, choisissez l'expéditeur.

   > **Important**
   >
   > Vous devez vérifier l'adresse e-mail de l'expéditeur dans Amazon SES. Pour plus d'informations, consultez la section Vérification des adresses e-mail dans Amazon SES, dans le manuel Amazon Simple Email Service Developer Guide.

   b. Pour AWS Lambda le rôle, utilisez un rôle existant ou créez-en un avec les autorisations requises. Ce rôle nécessite les `sso-directory:DescribeUser` autorisations `lambda:InvokeFunction` et une relation de confiance qui permet `iotevents.amazonaws.com` et permet `lambda.amazonaws.com` d'assumer le rôle.

   c. Pour les AWS Lambda fonctions, choisissez une fonction Lambda existante ou créez une fonction qui gère les notifications d'alarme. Pour plus d'informations, consultez la section Gestion des notifications d'alarme dans le Guide du AWS IoT Events développeur.

IAM



Pour activer les alarmes pour un portail

- (Facultatif) Choisissez Activer les alarmes.
    - Pour le rôle d'AWS IoT SiteWise accès, utilisez un rôle existant ou créez un rôle avec les autorisations requises. Ce rôle nécessite l'`iotevents:BatchPutMessage`autorisation et une relation de confiance qui permettent `iot.amazonaws.com` et `iotevents.amazonaws.com` permettent d'assumer le rôle.

Pour plus d'informations sur les alarmes dans SiteWise Monitor, voir Surveillance à l'aide d'alarmes dans le guide AWS IoT SiteWise d'application.

Activation de votre portail à la périphérie

Une fois que vous avez activé votre portail en périphérie, celui-ci est disponible sur toutes les passerelles SiteWise Edge avec le pack de traitement des données activé dans votre compte.

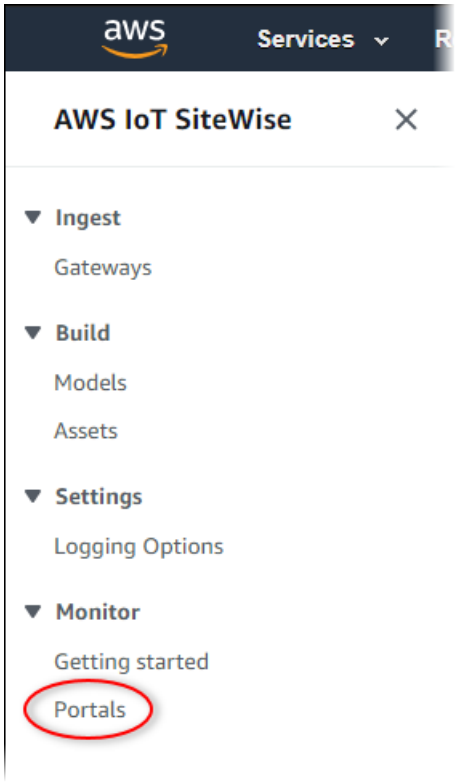
Pour activer le portail en périphérie

1. Dans la section Configuration Edge, activez Activer ce portail en périphérie.
2. Sélectionnez Create (Créer).

Administration de vos portails SiteWise Monitor

Vous devrez peut-être mettre à jour les détails du portail, modifier les administrateurs ou ajouter des utilisateurs à vos portails. Cette section explique comment effectuer ces tâches administratives de base pour vos portails SiteWise Monitor.

1. Connectez-vous à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Moniteur, Portails.



3. Choisissez le portail, puis choisissez View details (Afficher les détails) (ou choisissez le nom du portail).
4. Vous pouvez effectuer l'une des tâches administratives suivantes :

   - Modification du nom, de la description, de la personnalisation, de l'e-mail de support et des autorisations d'un portail
   - Ajout ou suppression d'administrateurs du portail
   - Envoi d'invitations par e-mail aux administrateurs du portail
   - Ajout ou suppression d'utilisateurs du portail
   - Suppression d'un portail

Pour obtenir des informations sur la façon de créer un portail, veuillez consulter Commencer avec AWS IoT SiteWise Monitor.

Rubriques

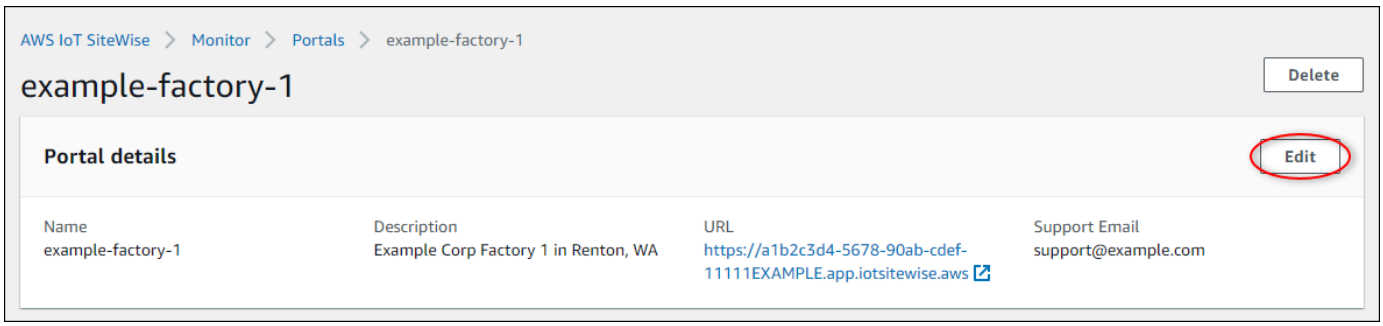
- Modification du nom, de la description, de la personnalisation, de l'e-mail de support et des autorisations d'un portail
- Ajout ou suppression d'administrateurs du portail

- Envoi d'invitations par e-mail aux administrateurs du portail
- Ajout ou suppression d'utilisateurs du portail
- Suppression d'un portail

Modification du nom, de la description, de la personnalisation, de l'e-mail de support et des autorisations d'un portail

Vous pouvez modifier le nom, la description, l'e-mail de support la personnalisation et les autorisations d'un portail.

1. Sur la page de détails du portail, dans la section Détails du portail choisissez Modifier.

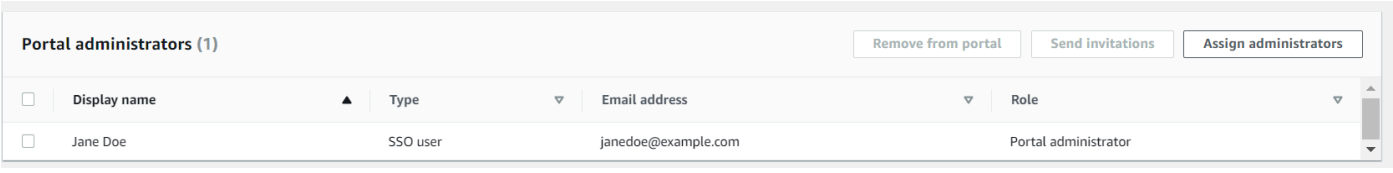


2. Mettez à jour les champs Nom, Description, Personnalisation du portail, E-mail de contact du support, ou Autorisations.
3. Lorsque vous avez terminé, sélectionnez Enregistrer.

Ajout ou suppression d'administrateurs du portail

En quelques étapes, vous pouvez ajouter ou supprimer des utilisateurs en tant qu'administrateurs d'un portail. En fonction du service d'authentification utilisateur, choisissez l'une des options suivantes.

IAM Identity Center

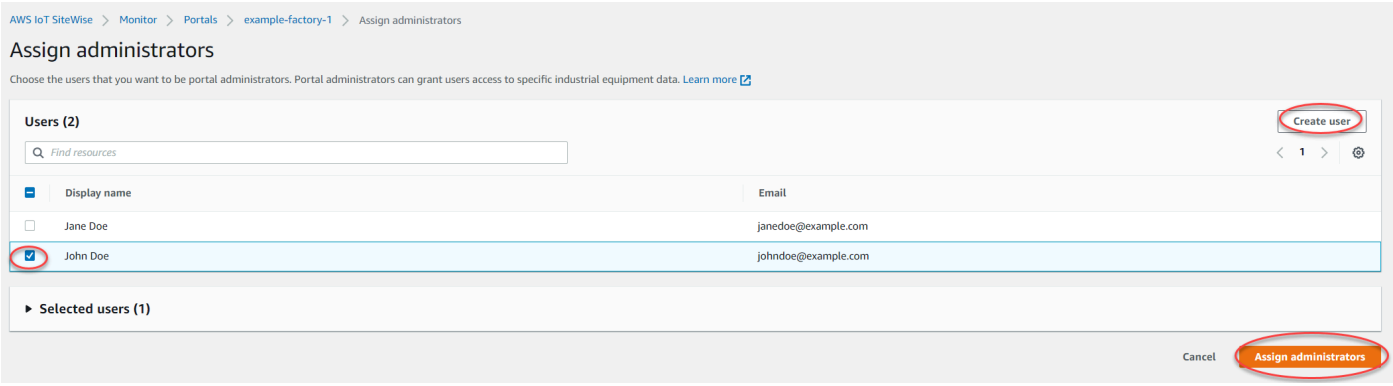


Pour ajouter des administrateurs de portail

1. Sur la page des détails du portail, dans la section Administrateurs du portail, sélectionnez Affecter des administrateurs.
2. Sur la page Affecter des administrateurs, cochez les cases correspondant aux utilisateurs à ajouter au portail en tant qu'administrateurs.

> **Note**
>
> Si vous utilisez IAM Identity Center comme banque d'identités et que vous êtes connecté à votre compte de AWS Organizations gestion, vous pouvez choisir Create user pour créer un utilisateur IAM Identity Center. IAM Identity Center envoie un e-mail au nouvel utilisateur pour qu'il définisse son mot de passe. Vous pouvez ensuite affecter l'utilisateur au portail en tant qu'administrateur. Pour plus d'informations, consultez la rubrique Manage identities in IAM Identity Center.

3. Choisissez Attribuer des administrateurs.

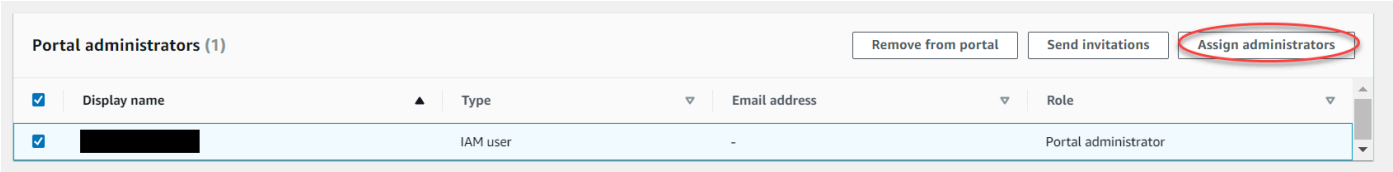


Pour supprimer des administrateurs de portail

- Dans la page de détails du portail, dans la section Portal administrators (Administrateurs du portail), cochez la case de chaque utilisateur à supprimer, puis choisissez Remove from portal (Supprimer du portail).

> **Note**
>
> Nous vous recommandons de sélectionner au moins un administrateur du portail.

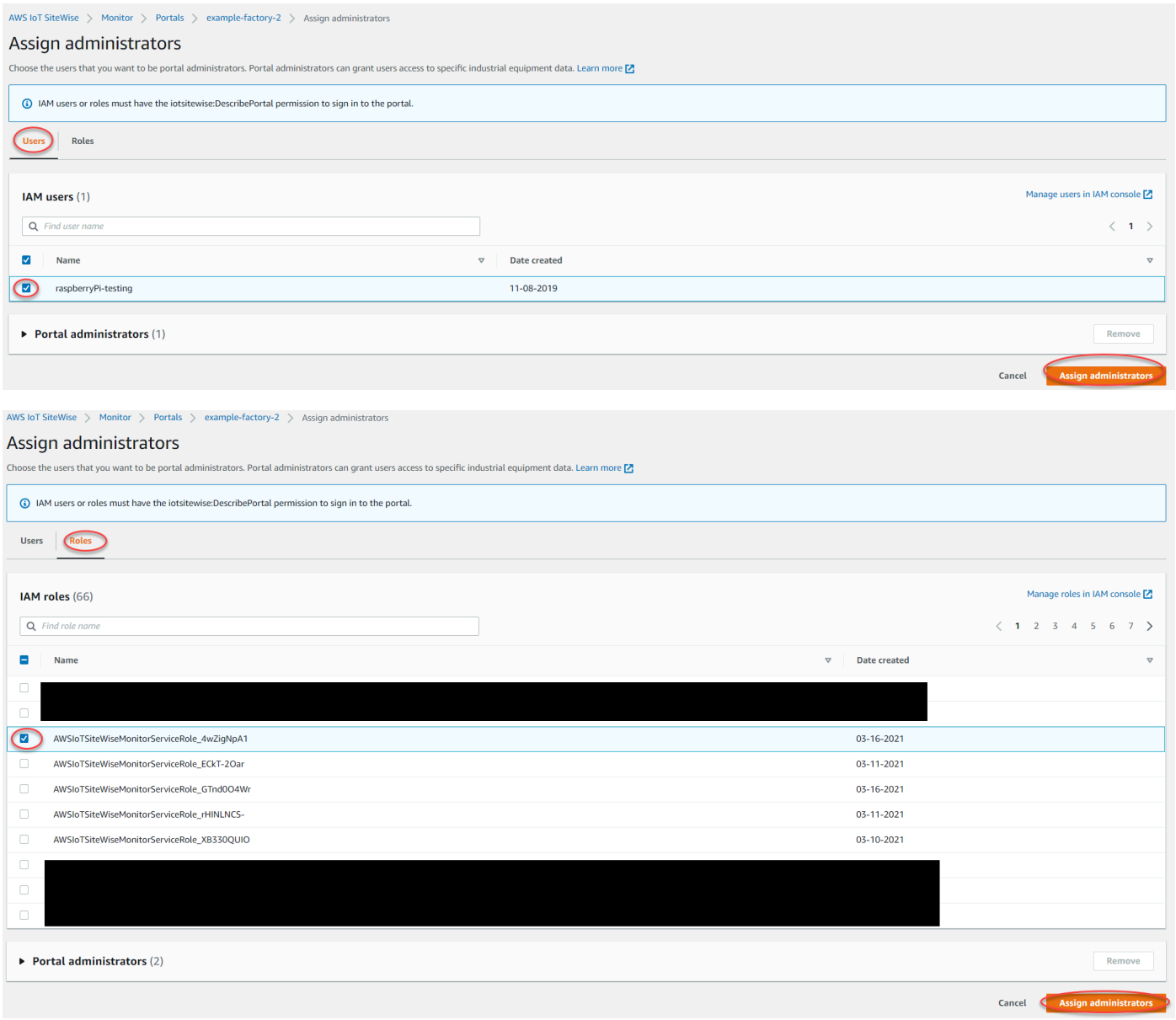
IAM



Pour ajouter des administrateurs de portail

1. Sur la page des détails du portail, dans la section Administrateurs du portail, sélectionnez Affecter des administrateurs.
2. Sur la page Affecter des administrateurs, procédez comme suit :
   - Choisissez Utilisateurs IAM si vous souhaitez ajouter un utilisateur IAM en tant qu'administrateur de votre portail.
   - Choisissez les rôles IAM si vous souhaitez ajouter un rôle IAM en tant qu'administrateur de portail.
3. Cochez les cases correspondant aux utilisateurs ou aux rôles que vous souhaitez utiliser en tant qu'administrateurs de votre portail. Cela ajoute les utilisateurs ou les rôles à la liste des administrateurs du portail.
4. Choisissez Attribuer des administrateurs.

> **Important**
>
> Les utilisateurs ou les rôles doivent être `iotsitewise:DescribePortal` autorisés à se connecter au portail.



Pour supprimer des administrateurs de portail

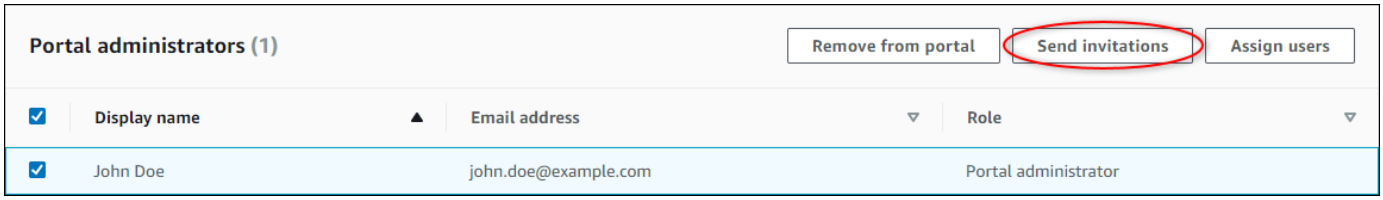
- Dans la page de détails du portail, dans la section Portal administrators (Administrateurs du portail), cochez la case de chaque utilisateur à supprimer, puis choisissez Remove from portal (Supprimer du portail).

> **Note**
>
> Il n'est pas recommandé de laisser un portail sans administrateur de portail.

Envoi d'invitations par e-mail aux administrateurs du portail

Vous pouvez envoyer des invitations par e-mail aux administrateurs du portail.

1. Sur la page de détails du portail, dans la section Portal administrators (Administrateurs du portail), activez les cases à cocher correspondant aux administrateurs du portail.



2. Choisissez Envoyer des invitations. Votre client de messagerie s'ouvre et une invitation est renseignée dans le corps du message.

   Vous pouvez personnaliser l'e-mail avant de l'envoyer aux administrateurs de votre portail.

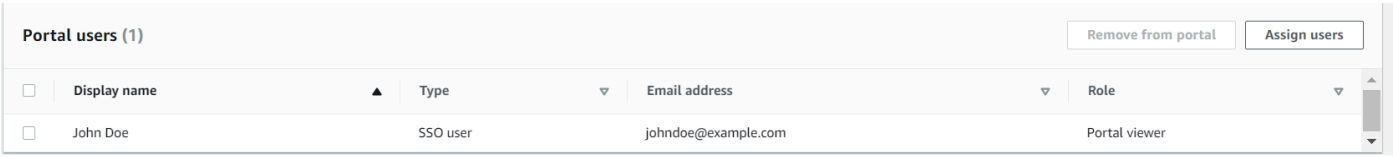
Ajout ou suppression d'utilisateurs du portail

Vous contrôlez les utilisateurs qui ont accès à votre portail. Les utilisateurs du portail apparaissent dans la liste des utilisateurs d'un portail SiteWise Monitor. Dans cette liste, les administrateurs du portail peuvent ajouter des propriétaires de projet, et les propriétaires de projet peuvent ajouter des utilisateurs de projet.

> **Note**
>
> Les administrateurs de votre portail et les utilisateurs du portail peuvent vous contacter via l'adresse e-mail de support d'un portail s'ils ont besoin que vous ajoutiez ou supprimez un utilisateur.

En fonction du service d'authentification utilisateur, choisissez l'une des options suivantes.

IAM Identity Center

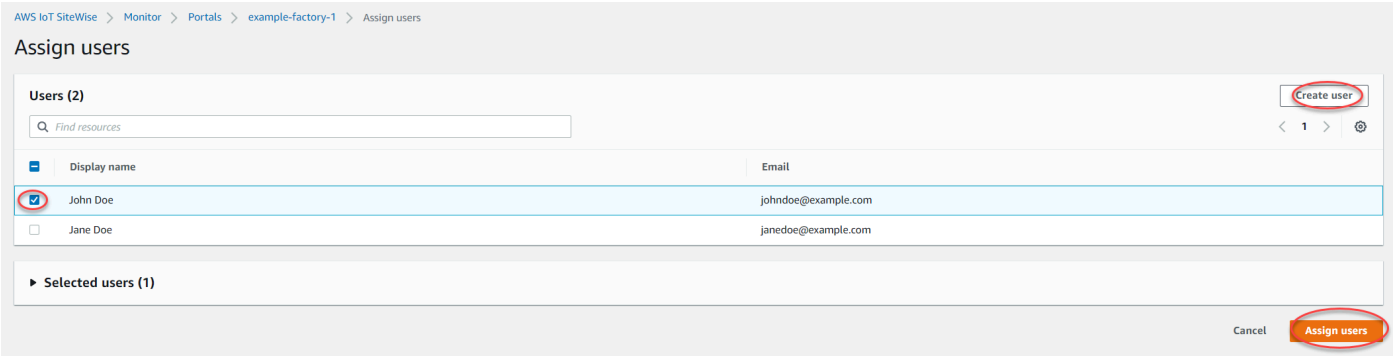


Pour ajouter des utilisateurs du portail

1. Sur la page de détails du portail, dans la section Portal users (Utilisateurs du portail), choisissez Assign users (Affecter des utilisateurs).
2. Sur la page Attribuer des utilisateurs, cochez la case correspondant aux utilisateurs à ajouter au portail.

> **Note**
>
> Si vous utilisez IAM Identity Center comme banque d'identités et que vous êtes connecté à votre compte de AWS Organizations gestion, vous pouvez choisir Create user pour créer un utilisateur IAM Identity Center. IAM Identity Center envoie un e-mail au nouvel utilisateur pour qu'il définisse son mot de passe. Vous pouvez ensuite affecter l'utilisateur au portail en tant qu'utilisateur. Pour plus d'informations, consultez la rubrique Manage identities in IAM Identity Center.

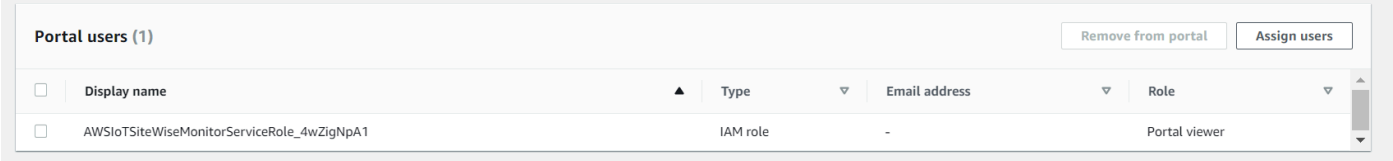
3. Choisissez Assign users (Affecter des utilisateurs).



Pour supprimer des utilisateurs du portail

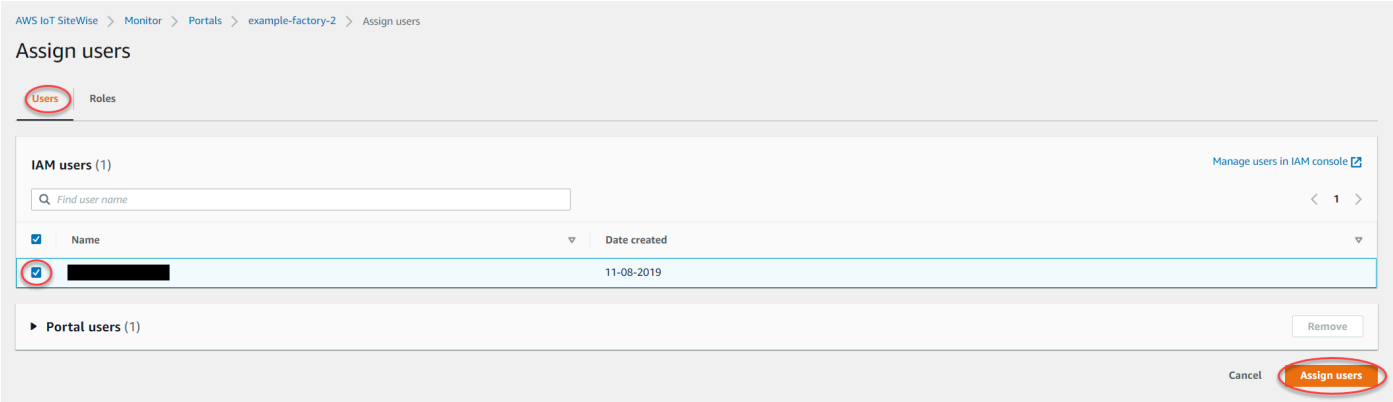
- Sur la page des détails du portail, dans la section Utilisateurs du portail, cochez la case correspondant aux utilisateurs à supprimer du portail, puis choisissez Supprimer du portail.

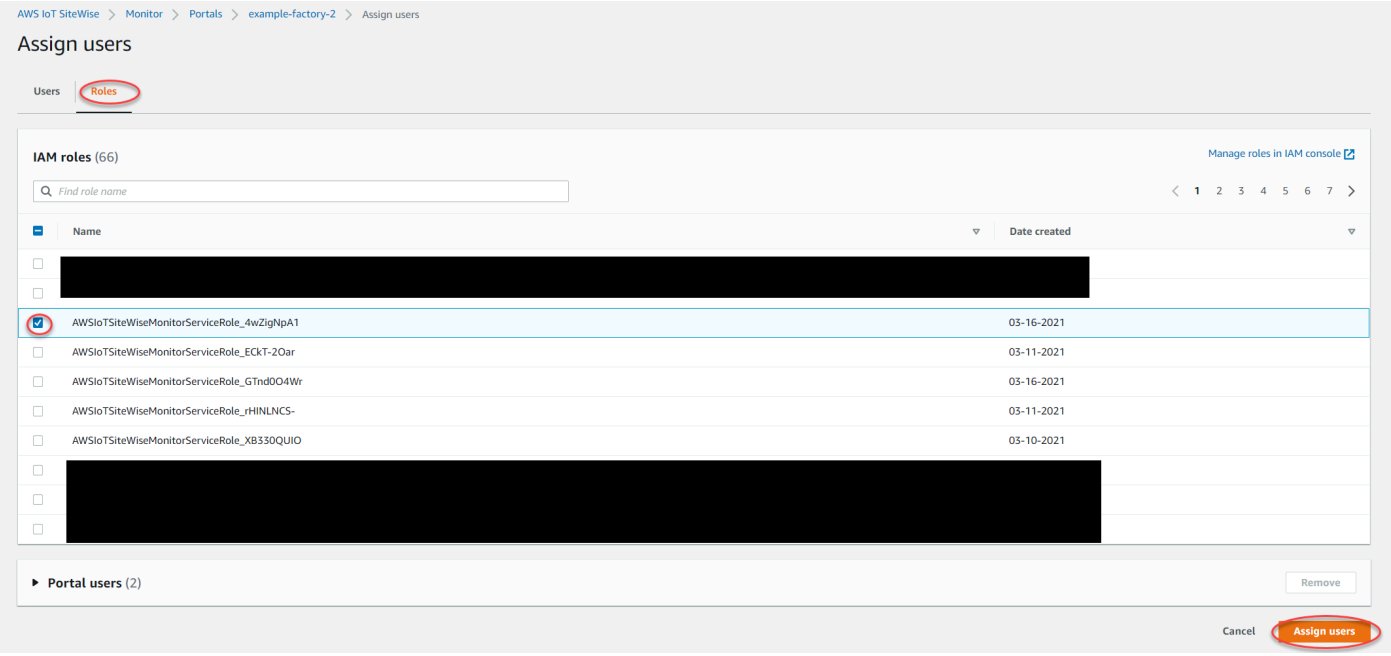
IAM



Pour ajouter des utilisateurs du portail

1. Sur la page de détails du portail, dans la section Portal users (Utilisateurs du portail), choisissez Assign users (Affecter des utilisateurs).
2. Sur la page Attribuer des utilisateurs, procédez comme suit :
   - Choisissez les utilisateurs IAM pour ajouter un utilisateur IAM en tant qu'utilisateur de votre portail.
   - Choisissez les rôles IAM pour ajouter un rôle IAM en tant qu'utilisateur de votre portail.
3. Cochez les cases correspondant aux utilisateurs ou aux rôles que vous souhaitez ajouter en tant qu'utilisateurs de votre portail. Cela ajoute les utilisateurs ou les rôles à la liste des utilisateurs du portail.
4. Choisissez Assign users (Affecter des utilisateurs).





Pour supprimer des utilisateurs du portail

- Sur la page des détails du portail, dans la section Utilisateurs du portail, cochez la case correspondant aux utilisateurs à supprimer du portail, puis choisissez Supprimer du portail.

> **Important**
>
> Les utilisateurs ou les rôles doivent être `iotsitewise:DescribePortal` autorisés à se connecter au portail.

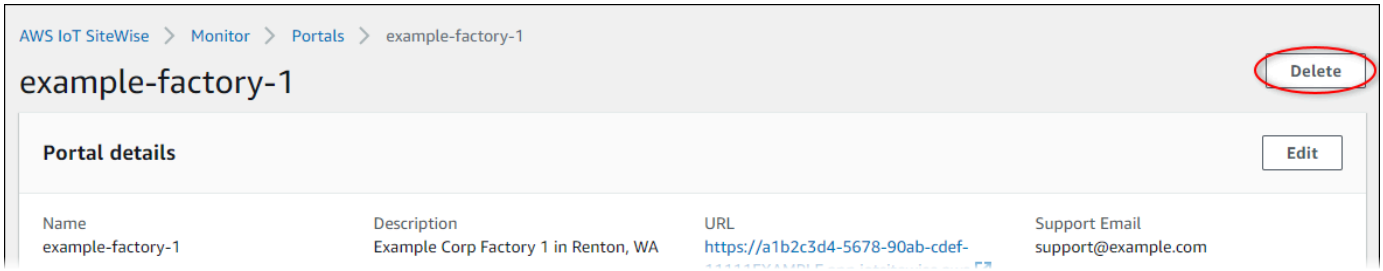
Suppression d'un portail

Vous pouvez supprimer un portail si vous l'avez créé à des fins de test ou en cas de doublon.

> **Note**
>
> Vous devez supprimer manuellement tous les tableaux de bord et projets du portail avant de pouvoir supprimer un portail. Pour plus d'informations, consultez les sections Suppression de projets et Suppression de tableaux de bord dans le Guide de l'application SiteWise Monitor.

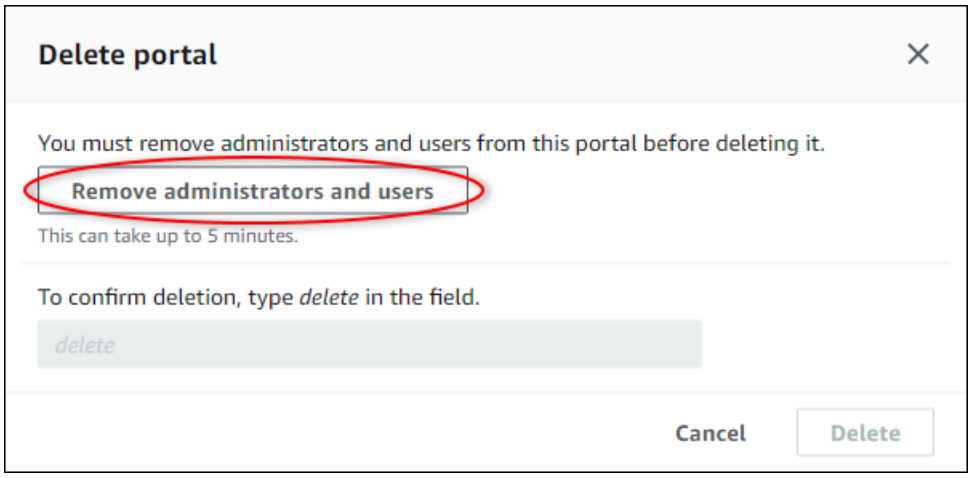
1. Sur la page de détails du portail, choisissez Supprimer.

> **Important**
>
> Lorsque vous supprimez un portail, vous perdez tous les projets qu'il contient et tous les tableaux de bord de chaque projet. Cette action ne peut pas être annulée. Les données de vos ressources ne sont pas affectées.

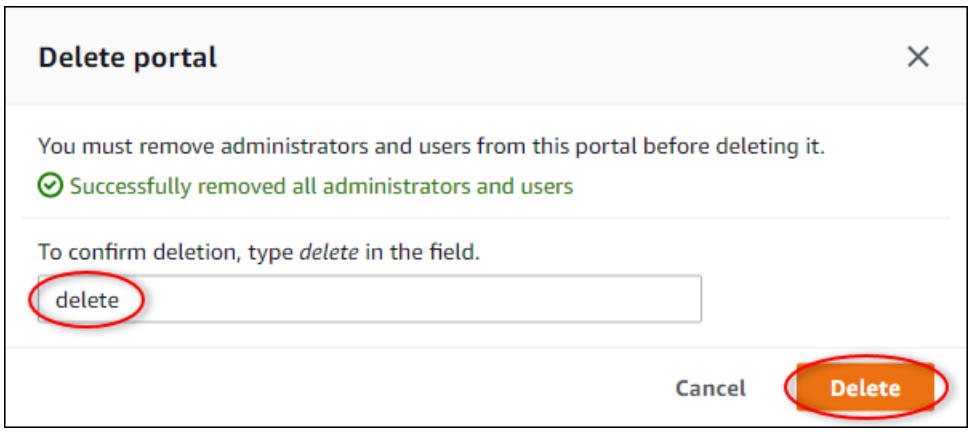


2. Dans la boîte de dialogue Supprimer les portails, choisissez Supprimer les administrateurs et les utilisateurs.

   Vous devez supprimer les administrateurs et les utilisateurs du portail avant de pouvoir supprimer ce dernier. Si votre portail ne dispose pas d'administrateurs ou d'utilisateurs, le bouton n'apparaît pas et vous pouvez passer à l'étape suivante.



3. Si vous êtes sûr de vouloir supprimer l'intégralité du portail, saisissez **`delete`** dans le champ pour confirmer la suppression.



4. Sélectionnez Supprimer.

Surveillance des données avec l'application de tableau de bord IoT

L'application de tableau de bord IoT est une application de tableau de bord open source dans laquelle vous pouvez visualiser et interagir avec les données opérationnelles. Vous pouvez utiliser l'application de tableau AWS Cloud Development Kit (AWS CDK) de bord pour déployer l'IoT.

Voici des exemples de fonctionnalités de visualisation de données personnalisables dans l'application de tableau de bord IoT :

- Support de plusieurs propriétés dans un graphique linéaire unique.
- Recherche améliorée d'actifs et de propriétés.

Les clients des secteurs de la fabrication, de la logistique, de l'énergie et d'autres secteurs peuvent utiliser l'application de tableau de bord IoT pour relever des défis spécifiques tels que le suivi des performances des équipements, l'optimisation de l'efficacité opérationnelle et les décisions basées sur les données. Pour plus d'informations, consultez le GitHub référentiel de l'application de tableau de bord IoT.

Interrogez les données de AWS IoT SiteWise

Vous pouvez utiliser les opérations de l' AWS IoT SiteWise API pour interroger les valeurs actuelles, les valeurs historiques et les agrégats des propriétés de vos actifs sur des intervalles de temps spécifiques.

Utilisez ces fonctionnalités pour mieux comprendre vos données. Par exemple, découvrez tous vos actifs avec une valeur de propriété donnée ou créez une représentation personnalisée de vos données. Vous pouvez également utiliser les opérations d'API pour développer des solutions logicielles qui s'intègrent aux données industrielles stockées dans vos AWS IoT SiteWise actifs. Vous pouvez également explorer les données de vos ressources en direct dans AWS IoT SiteWise Monitor. Pour savoir comment configurer le SiteWise moniteur, consultezSurveillance des données avec AWS IoT SiteWise Monitor.

Les opérations décrites dans cette section renvoient des objets contenant des valeurs de propriété contenant des structures d'horodatage, de qualité et de valeur (TQV) :

- `timestamp` contient l'heure d'époque Unix actuelle en secondes avec un décalage en nanosecondes.
- La métrique `quality` contient l'une des chaînes suivantes, qui indiquent la qualité du point de données :
  - `GOOD`— Les données ne sont affectées par aucun problème.
  - `BAD`— Les données sont affectées par un problème tel qu'une défaillance du capteur.
  - `UNCERTAIN`— Les données sont affectées par un problème tel que l'imprécision du capteur.
- `value` contient l'un des champs suivants, selon le type de la propriété :
  - `booleanValue`
  - `doubleValue`
  - `integerValue`
  - `stringValue`

Rubriques

- Interrogation des valeurs des propriétés actuelles de l'actif
- Interrogation des valeurs historiques de propriété de ressource
- Interrogation des agrégats de propriétés d'actif

- AWS IoT SiteWise langage de requête

Interrogation des valeurs des propriétés actuelles de l'actif

Ce didacticiel montre deux méthodes pour obtenir la valeur actuelle d'une propriété d'actif. Vous pouvez utiliser la AWS IoT SiteWise console ou utiliser l'API dans le AWS Command Line Interface (AWS CLI).

Rubriques

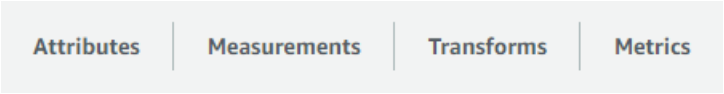
- Rechercher la valeur actuelle d'une propriété d'actif (console)
- Rechercher la valeur actuelle d'une propriété d'actif (AWS CLI)

Rechercher la valeur actuelle d'une propriété d'actif (console)

Vous pouvez utiliser la AWS IoT SiteWise console pour afficher la valeur actuelle d'une propriété d'actif.

Pour obtenir la valeur actuelle d'une propriété de ressource (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Ressources.
3. Choisissez la ressource avec la propriété à interroger.
4. Cliquez sur l'icône en forme de flèche pour développer une hiérarchie d'actifs afin de trouver votre actif.
5. Choisissez l'onglet correspondant au type de propriété. Par exemple, choisissez Mesures pour afficher la valeur actuelle d'une propriété de mesure.



6. Trouvez la propriété à afficher. La valeur actuelle apparaît dans la colonne Dernière valeur.

Rechercher la valeur actuelle d'une propriété d'actif (AWS CLI)

Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour rechercher la valeur actuelle d'une propriété d'actif.

Utilisez l'GetAssetPropertyValueopération pour interroger la valeur actuelle d'une propriété d'actif.

Pour identifier une propriété d'actif, spécifiez l'une des options suivantes :

- La `assetId` fin `propertyId` de la propriété de l'actif à laquelle les données sont envoyées.
- Le`propertyAlias`, qui est un alias de flux de données (par exemple,`/company/windfarm/3/turbine/7/temperature`). Pour utiliser cette option, vous devez d'abord définir l'alias de votre propriété de ressource. Pour définir des alias de propriété, consultezMappage des flux de données industrielles avec des propriétés de ressources.

Pour obtenir la valeur actuelle d'un actif (AWS CLI)

- Exécutez la commande suivante pour obtenir la valeur actuelle de la propriété de ressource. Remplacez *`asset-id`* par l'ID de la ressource et *`property-id`* par l'ID de la propriété.

```
aws iotsitewise get-asset-property-value \
  --asset-id asset-id \
  --property-id property-id
```

L'opération renvoie une réponse qui contient les données TQV actuelles de la propriété au format suivant.

```
{
  "propertyValue": {
    "value": {
      "booleanValue": Boolean,
      "doubleValue": Number,
      "integerValue": Number,
      "stringValue": "String"
    },
    "timestamp": {
      "timeInSeconds": Number,
      "offsetInNanos": Number
    },
    "quality": "String"
  }
}
```

Interrogation des valeurs historiques de propriété de ressource

Vous pouvez utiliser l'GetAssetPropertyValueHistoryopération AWS IoT SiteWise API pour interroger les valeurs historiques d'une propriété d'actif.

Pour identifier une propriété d'actif, spécifiez l'une des options suivantes :

- La `assetId` fin `propertyId` de la propriété de l'actif à laquelle les données sont envoyées.
- Le`propertyAlias`, qui est un alias de flux de données (par exemple,`/company/windfarm/3/turbine/7/temperature`). Pour utiliser cette option, vous devez d'abord définir l'alias de votre propriété de ressource. Pour définir des alias de propriété, consultezMappage des flux de données industrielles avec des propriétés de ressources.

Passez les paramètres suivants pour affiner vos résultats :

- `startDate`— Le début exclusif de la plage à partir de laquelle interroger les données historiques, exprimé en secondes à l'époque Unix.
- `endDate`— La fin de la plage inclusive à partir de laquelle interroger les données historiques, exprimée en secondes à l'époque Unix.
- `maxResults`— Le nombre maximum de résultats à renvoyer en une seule demande. Par défaut, ce sont les `20` résultats.
- `nextToken`— Un jeton de pagination renvoyé lors d'un précédent appel de cette opération.
- `timeOrdering`— La commande à appliquer aux valeurs renvoyées : `ASCENDING` ou`DESCENDING`.
- `qualities`— La qualité permettant de filtrer les résultats par : `GOODBAD`, ou`UNCERTAIN`.

Rubriques

- Rechercher l'historique des valeurs d'une propriété d'actif (AWS CLI)

Rechercher l'historique des valeurs d'une propriété d'actif (AWS CLI)

Pour consulter l'historique des valeurs d'une propriété d'actif (AWS CLI)

1. Exécutez la commande suivante pour obtenir l'historique des valeurs de la propriété de ressource. Cette commande interroge l'historique de la propriété sur un intervalle spécifique

de 10 minutes. Remplacez *asset-id* par l'ID de la ressource et *property-id* par l'ID de la propriété. Remplacez les paramètres de date par l'intervalle à interroger.

```
aws iotsitewise get-asset-property-value-history \
  --asset-id asset-id \
  --property-id property-id \
  --start-date 1575216000 \
  --end-date 1575216600
```

L'opération renvoie une réponse contenant les TQV historiques de la propriété au format suivant :

```
{
  "assetPropertyValueHistory": [
    {
      "value": {
        "booleanValue": Boolean,
        "doubleValue": Number,
        "integerValue": Number,
        "stringValue": "String"
      },
      "timestamp": {
        "timeInSeconds": Number,
        "offsetInNanos": Number
      },
      "quality": "String"
    }
  ],
  "nextToken": "String"
}
```

2. S'il existe d'autres entrées de valeur, vous pouvez transmettre le jeton de pagination du `nextToken` champ à un appel ultérieur à l'GetAssetPropertyValueHistoryopération.

Interrogation des agrégats de propriétés d'actif

AWS IoT SiteWise calcule automatiquement les valeurs agrégées des propriétés des actifs, qui sont un ensemble de mesures de base calculées sur plusieurs intervalles de temps. AWS IoT SiteWise calcule les agrégats suivants chaque minute, heure et jour pour les propriétés de vos actifs :

- average — La moyenne (moyenne) des valeurs d'une propriété sur un intervalle de temps.
- count — Le nombre de points de données pour une propriété sur un intervalle de temps.
- maximum — Le maximum des valeurs d'une propriété sur un intervalle de temps.
- minimum : valeur minimale d'une propriété sur un intervalle de temps.
- écart type : écart type des valeurs d'une propriété sur un intervalle de temps.
- sum — Somme des valeurs d'une propriété sur un intervalle de temps.

Pour les propriétés non numériques, telles que les chaînes et les booléens, AWS IoT SiteWise calcule uniquement le nombre agrégé.

Vous pouvez également calculer des métriques personnalisées pour vos données d'actif. Les propriétés des métriques vous permettent de définir des agrégations spécifiques à votre opération. Les propriétés métriques offrent des fonctions d'agrégation et des intervalles de temps supplémentaires qui ne sont pas précalculés pour l' AWS IoT SiteWise API. Pour plus d'informations, consultez Agrégation de données provenant de propriétés et d'autres actifs (métriques).

Rubriques

- Agrégats pour une propriété d'actif (API)
- Agrégats pour une propriété d'actif ()AWS CLI

Agrégats pour une propriété d'actif (API)

Vous pouvez utiliser l' AWS IoT SiteWise API pour obtenir des agrégats pour une propriété d'actif.

Utilisez l'GetAssetPropertyAggregatesopération pour interroger les agrégats d'une propriété d'actif.

Pour identifier une propriété d'actif, spécifiez l'une des options suivantes :

- La `assetId` fin `propertyId` de la propriété de l'actif à laquelle les données sont envoyées.
- Le`propertyAlias`, qui est un alias de flux de données (par exemple,`/company/windfarm/3/turbine/7/temperature`). Pour utiliser cette option, vous devez d'abord définir l'alias de votre propriété de ressource. Pour définir des alias de propriété, consultezMappage des flux de données industrielles avec des propriétés de ressources.

Vous devez également passer les paramètres obligatoires suivants :

- `aggregateTypes`— La liste des agrégats à récupérer. Vous pouvez spécifier n'importe quel élément : `AVERAGE`, `COUNT`, `MAXIMUM`, `MINIMUM`, `STANDARD_DEVIATION` et `SUM`.
- `resolution`— Intervalle de temps pendant lequel la métrique doit être `1m` récupérée : (1 minute), `1h` (1 heure) ou `1d` (1 jour).
- `startDate`— Le début exclusif de la plage à partir de laquelle interroger les données historiques, exprimé en secondes à l'époque Unix.
- `endDate`— La fin de la plage inclusive à partir de laquelle interroger les données historiques, exprimée en secondes à l'époque Unix.

Vous pouvez également passer l'un des paramètres suivants pour affiner vos résultats :

- `maxResults`— Le nombre maximum de résultats à renvoyer par requête. Par défaut, ce sont les `20` résultats.
- `nextToken`— Un jeton de pagination renvoyé lors d'un précédent appel de cette opération.
- `timeOrdering`— La commande à appliquer aux valeurs renvoyées : `ASCENDING` ou`DESCENDING`.
- `qualities`— La qualité permettant de filtrer les résultats par : `GOODBAD`, ou`UNCERTAIN`.

> **Note**
>
> L'GetAssetPropertyAggregatesopération renvoie un TQV avec un format différent de celui des autres opérations décrites dans cette section. La structure `value` contient un champ pour chacun des éléments `aggregateTypes` de la demande. Le `timestamp` contient l'heure à laquelle l'agrégation s'est produite, en secondes (heure UNIX Epoch).

Agrégats pour une propriété d'actif ()AWS CLI

Pour interroger des agrégats pour une propriété d'actif ()AWS CLI

1. Exécutez la commande suivante pour obtenir des agrégats pour la propriété de ressource. Cette commande interroge la moyenne et la somme avec une résolution d'1 heure pour un intervalle spécifique d'1 heure. Remplacez *`asset-id`* par l'ID de la ressource et *`property-id`* par l'ID de la propriété. Remplacez les paramètres par les agrégats et l'intervalle à interroger.

```
aws iotsitewise get-asset-property-aggregates \
  --asset-id asset-id \
  --property-id property-id \
  --start-date 1575216000 \
  --end-date 1575219600 \
  --aggregate-types AVERAGE SUM \
  --resolution 1h
```

L'opération renvoie une réponse qui contient les données TQV historiques de la propriété au format suivant. La réponse inclut uniquement les agrégats demandés.

```
{
  "aggregatedValues": [
    {
      "timestamp": Number,
      "quality": "String",
      "value": {
        "average": Number,
        "count": Number,
        "maximum": Number,
        "minimum": Number,
        "standardDeviation": Number,
        "sum": Number
      }
    }
  ],
  "nextToken": "String"
}
```

2. S'il existe d'autres entrées de valeur, vous pouvez transmettre le jeton de pagination du `nextToken` champ à un appel ultérieur à l'GetAssetPropertyAggregatesopération.

AWS IoT SiteWise langage de requête

Grâce à l'opération d'ExecuteQueryAPI de récupération de AWS IoT SiteWise données, vous pouvez récupérer des informations sur les définitions structurelles déclaratives et les données de séries chronologiques qui leur sont associées, à partir des informations suivantes :

- des modèles

- actifs
- mesures
- metrics
- transforme
- agrégats

Cela peut être fait avec des instructions de requête de type SQL, dans une seule requête d'API.

> **Note**
>
> Cette fonctionnalité est disponible dans toutes les régions où AWS IoT SiteWise les deux AWS IoT TwinMaker sont disponibles, sauf AWS GovCloud dans l'ouest des États-Unis.

Rubriques

- Prérequis
- Référence du langage de requête

Prérequis

AWS IoT SiteWise nécessite des autorisations d'intégration AWS IoT TwinMaker afin de pouvoir organiser et modéliser les données industrielles.

Avant de pouvoir récupérer des informations sur les modèles, les actifs, les mesures, les métriques, les transformations et les agrégats, assurez-vous que les conditions préalables suivantes sont remplies :

- Rôles liés au service pour les deux AWS IoT SiteWise et AWS IoT TwinMaker configurés dans votre. Compte AWS Pour plus d'informations sur l'utilisation des rôles liés à un service, consultez Utilisation des rôles liés à un service dans le Guide de l'utilisateur IAM.
- Une AWS IoT SiteWise intégration activée pour votre rôle IAM. Pour plus d'informations, consultez Intégration d'AWS IoT SiteWise et de AWS IoT TwinMaker.
- Un AWS IoT TwinMaker espace de travail avec un identifiant `IoTSiteWiseDefaultWorkspace` dans votre compte dans la région. Pour plus d'informations, consultez Utilisation d'IoTSiteWiseDefaultWorkspace dans le Guide de l'utilisateur AWS IoT TwinMaker .

- Les modes de tarification groupée standard ou échelonnés sont AWS IoT TwinMaker activés. Pour plus d'informations, consultez la section Changer de mode de AWS IoT TwinMaker tarification dans le guide de AWS IoT TwinMaker l'utilisateur.

Référence du langage de requête

AWS IoT SiteWise prend en charge un langage de requête riche pour travailler avec vos données. Les types de données, les opérateurs, les fonctions et les constructions disponibles sont décrits dans les rubriques suivantes.

Voir Exemples de requêtes pour écrire des requêtes avec le langage de AWS IoT SiteWise requête.

Rubriques

- Comprendre les points de vue
- Types de données pris en charge
- Récupérez des données avec une instruction SELECT
- Opérateurs logiques
- Opérateurs de comparaison
- Exemples de requêtes

Comprendre les points de vue

Cette section fournit des informations pour vous aider à comprendre les vues AWS IoT SiteWise, telles que les métadonnées de processus et les données de télémétrie.

Les tableaux suivants fournissent les noms et les descriptions des vues.

Modèle de données

Nom de la vue	Description de la vue
asset	Contient des informations sur l'actif et la dérivation du modèle.
propriété_actif	Contient des informations sur la structure de la propriété de l'actif.

Nom de la vue	Description de la vue
Série Raw_Time	Contient les données historiques de la série chronologique.
dernière_value_time_series	Contient la dernière valeur de la série chronologique.
agrégats_précalculés	Contient les valeurs agrégées des propriétés des actifs calculées automatiquement. Il s'agit d'un ensemble de mesures de base calculées sur plusieurs intervalles de temps.

Les vues suivantes répertorient les noms de colonnes pour les requêtes ainsi que des exemples de données.

Voir : actif

identifiant_actif	nom_actif	description_de l'actif	identifiant du modèle d'actif
88898498-0b8b-42b5-bf57-16180bc3d3a0	WindTurbine UN	WindTurbine Actif A	17847250-5bf0-4f74-b775-cc03f05e7cb8
17847250-5bf0-4f74-b775-cc03f05e7cb8	Modèle d'actifs d'éoliennes	Représente une turbine dans un parc éolien.	

Voir : asset_property

identifiant_propriété	identifiant_actif	nom_propriété	type_données_propriété	alias de propriété	asset_composite_model_id
b29be434-b000-4d74-b809-75287d83bcd6	88898498-0b8b-42b5-bf57-16180bc3d3a0	température du moteur	Double	`Rochester 2/44///Line-5/Bus-`	

identifiant_propriété	identifiant_actif	nom_propriété	type_données_propriété	alias de propriété	asset_composite_model_id
				2/Machine-5/Temperature	
3b458f00-24e7-458a-b4e8-c6026eff654a	88898498-0b8b-42b5-bf57-16180bc3d3a0	direction du vent	Double	/company/windfarm/3/turbine/7/winddirection	2f458n00-56e7-458h-b4e8-c6026eff985 g

Voir : RAW_TIME_SERIES

identifiant_actif	identifiant_propriété	alias de propriété	horodatage de l'événement	qualité	valeur_booléenne	int_value	valeur_double	valeur_chaîne
88898498-0b8b-42b5-bf57-16180bc3d3a	b29be434-b000-4d74-b809-75287d83bcd	Rochest 2/44/// Line-5/Bus-2/Machine-5/Temperature	1575219600	BON			115,0	
88898498-0b8b-42b5-bf57-16180bc3d3a	3b458f00-24e7-458a-b4e8-c6026eff654a	/company/windfarm/3/turbine	1575219377	BON			348,75	

identifiant_actif	identifiant_propriété	alias de propriété	horodatage de l'événement	qualité	valeur_booléenne	int_value	valeur_double	valeur_chaîne
		/7/winddirection						

> **Note**
>
> Vous devez inclure une clause de filtre dans la `event_timestamp` colonne pour interroger la `raw_time_series` vue. Il s'agit d'un filtre obligatoire, et la requête échouera sans ce filtre.
>
> Example query
>
> ```
> SELECT event_timestamp, double_value FROM raw_time_series WHERE event_timestamp
>  > 1234567890
> ```

Voir : LATEST_VALUE_TIME_SERIES

identifiant_actif	identifiant_propriété	alias de propriété	horodatage de l'événement	qualité	valeur_booléenne	int_value	valeur_double	valeur_chaîne
88898498-0b8b-42b5-bf57-16180bc3d3a	3b458f00-24e7-458a-b4e8-c6026eff654a	/company/windfarm/3/turbine/7/winddirection	1575219600	BON			355,39	

Voir : precomputed_aggregates

identifiant_actif	identifiant_propriété	alias de propriété	horodate de l'événement	resolution	valeur_somme	valeur_comptage	valeur_moyenne	valeur_maximale	valeur_minimale	stdev_value
888984 0b8b-42 - bf57-16 80bc3d	b29be4 b000-4c - b809-75 87d83b	Roches 2/44// Li ne-5/ Bus- 2/ Machin -5/ Temper ature	157521 0	15 min	1105,48	15	73,4	80,6	68	3,64

Types de données pris en charge

AWS IoT SiteWise le langage de requête prend en charge les types de données suivants.

Voir : actif

Type de données	Description
`STRING`	Chaîne d'une longueur maximale de 1024 octets.
`INTEGER`	Un entier signé de 32 bits dont la plage est comprise `-2,147,483,648 to 2,147,483,647` entre.
`DOUBLE`	Nombre à virgule flottante avec plage de `-10^100 to 10^100` valeurs et `IEEE 754` double précision.
`BOOLEAN`	`true` ou `false`.

> **Note**
>
> Les données de double précision ne sont pas exactes. Certaines valeurs ne sont pas converties exactement et ne représenteront pas tous les nombres réels en raison d'une précision limitée. Les données à virgule flottante de la requête peuvent ne pas avoir la même valeur que celle représentée en interne. La valeur est arrondie si la précision d'un nombre saisi est trop élevée.

Récupérez des données avec une instruction SELECT

L'`SELECT`instruction est utilisée pour récupérer des données à partir d'une ou de plusieurs vues. AWS IoT SiteWise soutient un point `JOIN` de vue implicite. Vous pouvez répertorier les vues à joindre (dans la `FROM` clause de l'`SELECT`instruction) en les séparant par des virgules.

Example

Utilisez l'`SELECT`énoncé suivant :

```
SELECT select_expr [, ...]
[ FROM from_item [, ...] ]
[ WHERE [LIKE condition ESCAPE condition] ]
```

Dans l'exemple précédent, la `LIKE` clause spécifie les conditions de recherche et de filtrage à l'aide de caractères génériques. AWS IoT SiteWise supporte en `percentage (%)` tant que caractère joker.

Example à utiliser `%` dans un état :

```
Prefix search: String%
Infix search: %String%
Suffix search: %String
```

Example pour rechercher un actif :

```
SELECT asset_name, asset_description FROM asset WHERE asset_name LIKE 'Wind%'
```

Example pour rechercher un actif à l'aide d'une condition ESCAPE :

```
SELECT asset_name, asset_description FROM asset WHERE asset_name LIKE 'room\%' ESCAPE
 '\'
```

Opérateurs logiques

AWS IoT SiteWise prend en charge les opérateurs logiques suivants.

Opérateurs logiques

Opérateur	Description	Exemple
AND	TRUEsi les deux valeurs sont vraies	un AND b

Si a ou b l'estFALSE, l'expression précédente est considérée comme fausse. Pour qu'un AND opérateur soit évalué comme vrai, a et b doivent tous deux être vrais.

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
```

Opérateurs de comparaison

AWS IoT SiteWise prend en charge les opérateurs de comparaison suivants.

Opérateurs logiques

Opérateur	Description
<	Inférieur à
>	Supérieure à
<=	Inférieur ou égal à

Opérateur	Description
>=	Supérieur ou égal à
=	Égal à
!=	Non égal à

Exemples de requêtes

Filtrage des métadonnées

L'exemple suivant concerne le filtrage des métadonnées à l'aide d'une `SELECT` instruction contenant le langage de AWS IoT SiteWise requête :

```
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%'
```

Filtrage des valeurs

Voici un exemple de filtrage de valeurs à l'aide d'une `SELECT` instruction utilisant le langage de AWS IoT SiteWise requête :

```
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
```

Interaction avec d'autres AWS services

AWS IoT SiteWise peut publier des données d'actifs sur le courtier de messages de publication/abonnement AWS IoT MQTT, afin que vous puissiez interagir avec les données de vos actifs provenant d'autres services. AWS AWS IoT SiteWise attribue à chaque propriété d'actif un sujet MQTT unique que vous pouvez utiliser pour acheminer les données de vos actifs vers d'autres AWS services à l'aide des règles de AWS IoT base. Par exemple, vous pouvez configurer les règles de AWS IoT base pour effectuer les tâches suivantes :

- Identifier les défaillances de l'équipement et aviser le personnel approprié en envoyant des données à AWS IoT Events.
- Historisez certaines données d'actifs à utiliser dans des solutions logicielles externes en envoyant des données à Amazon DynamoDB.
- Générez des rapports hebdomadaires en déclenchant une fonction AWS Lambda.

Vous pouvez suivre un didacticiel qui décrit les étapes nécessaires pour configurer une règle qui stocke les valeurs des propriétés dans DynamoDB. Pour plus d'informations, consultez Publication de mises à jour de la valeur des propriétés sur Amazon DynamoDB.

Pour plus d'informations sur la configuration d'une règle, consultez la section Règles du guide du AWS IoT développeur.

Vous pouvez également réutiliser les données d'autres AWS services dans AWS IoT SiteWise. Pour ingérer des données par le biais de l'action de la AWS IoT SiteWise règle, consultezIngestion de données à l'aide de règles AWS IoT Core.

Rubriques

- Présentation des rubriques MQTT des propriétés de ressource
- Utilisation des notifications relatives aux propriétés des actifs
- Exportez des données vers Amazon S3 avec des notifications relatives aux propriétés des actifs
- Intégration à Grafana
- Intégration d'AWS IoT SiteWise et de AWS IoT TwinMaker
- Détecter les anomalies des équipements avec Amazon Lookout for Equipment

Présentation des rubriques MQTT des propriétés de ressource

Chaque propriété de ressource possède un chemin d'accès de rubrique MQTT unique au format suivant.

```
$aws/sitewise/asset-models/assetModelId/assets/assetId/properties/propertyId
```

> **Note**
>
> AWS IoT SiteWise ne prend pas en charge le caractère générique du filtre de rubrique # (à plusieurs niveaux) dans le moteur de règles de AWS IoT base. Vous pouvez utiliser le caractère générique + (niveau unique). Par exemple, vous pouvez utiliser le filtre de rubrique suivant pour faire correspondre toutes les mises à jour d'un modèle de ressource particulier.
>
> ```
> $aws/sitewise/asset-models/assetModelId/assets/+/properties/+
> ```
>
> Pour en savoir plus sur les caractères génériques utilisés pour filtrer les rubriques, consultez la section Rubriques du Guide du développeur AWS IoT principal.

Utilisation des notifications relatives aux propriétés des actifs

Vous pouvez activer les notifications de propriété pour publier les mises à jour des données des actifs AWS IoT Core, puis exécuter des requêtes sur ces données. Avec les notifications relatives aux propriétés des actifs, AWS IoT SiteWise fournit un AWS CloudFormation modèle que vous pouvez utiliser pour exporter AWS IoT SiteWise des données vers Amazon S3.

> **Note**
>
> Les données relatives aux actifs sont envoyées à AWS IoT Core chaque fois qu'elles sont reçues AWS IoT SiteWise, que leur valeur ait changé ou non.

Rubriques

- Activation des notifications relatives aux propriétés de ressource (console)
- Activation des notifications relatives aux propriétés des actifs (AWS CLI)
- Interrogation des messages de notification de propriété de ressource

Activation des notifications relatives aux propriétés de ressource (console)

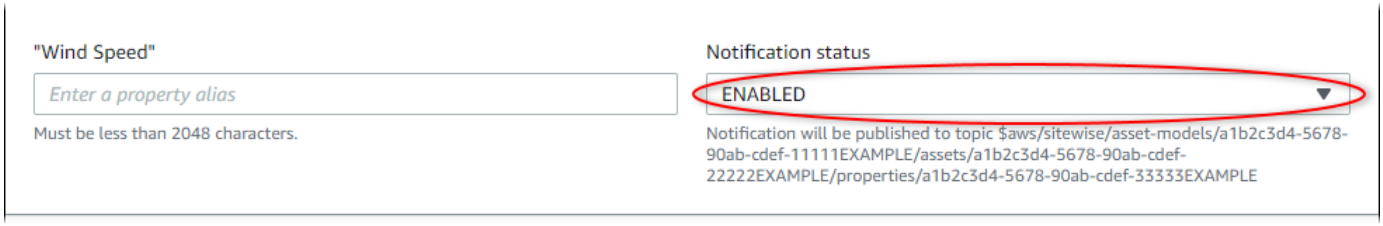
Par défaut, AWS IoT SiteWise ne publie pas les mises à jour de la valeur des propriétés. Vous pouvez utiliser la AWS IoT SiteWise console pour activer les notifications pour une propriété d'actif.

Pour activer ou désactiver les notifications pour une propriété de ressource (console)

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Ressources.
3. Choisissez la ressource pour activer les notifications d'une propriété.

> **Tip**
>
> Vous pouvez cliquer sur l'icône en forme de flèche pour développer une hiérarchie de ressources afin de trouver votre ressource.

4. Choisissez Modifier.
5. Pour le statut de notification de la propriété de ressource, choisissez ACTIVÉ.



Vous pouvez également choisir DÉSACTIVÉ pour désactiver les notifications pour la propriété de ressource.

6. Choisissez Enregistrer.

Activation des notifications relatives aux propriétés des actifs (AWS CLI)

Par défaut, AWS IoT SiteWise ne publie pas les mises à jour de la valeur des propriétés. Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour activer ou désactiver les notifications relatives à une propriété d'actif.

Vous devez connaître l'`assetId` de votre ressource et le `propertyId`de la propriété pour effectuer cette procédure. Vous pouvez également utiliser l'identifiant externe. Si vous avez créé un actif et que vous ne le connaissez pas`assetId`, utilisez l'ListAssetsAPI pour répertorier tous les actifs d'un

modèle spécifique. Utilisez cette DescribeAssetopération pour afficher les propriétés de votre actif, y compris les identifiants de propriété.

Utilisez cette UpdateAssetPropertyopération pour activer ou désactiver les notifications pour une propriété d'actif. Spécifiez les paramètres suivants :

- `assetId`— L'identifiant de l'actif.
- `propertyId`— L'ID de la propriété de l'actif.
- `propertyNotificationState`— État de notification de la valeur de la propriété : `ENABLED` ou`DISABLED`.
- `propertyAlias`— L'alias de la propriété. Spécifiez l'alias existant de la propriété lorsque vous mettez à jour l'état de notification. Si vous omettez ce paramètre, l'alias existant de la propriété est supprimé.

Pour activer ou désactiver les notifications pour une propriété de ressource (interface de ligne de commande)

1. Exécutez la commande suivante pour récupérer l'alias de la propriété de ressource. Remplacez *`asset-id`* par l'ID de la ressource et *`property-id`* par l'ID de la propriété.

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

   L'opération renvoie une réponse qui contient les informations de propriété de ressource au format suivant. L'alias de propriété se trouve dans `assetProperty.alias` dans l'objet JSON.

   ```
   {
     "assetId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
     "assetName": "Wind Turbine 7",
     "assetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
     "assetProperty": {
       "id": "a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
       "name": "Wind Speed",
       "alias": "/company/windfarm/3/turbine/7/windspeed",
       "notification": {
         "topic": "$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/
   assets/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE/properties/a1b2c3d4-5678-90ab-
   cdef-33333EXAMPLE",
   ```

```
      "state": "DISABLED"
    },
    "dataType": "DOUBLE",
    "unit": "m/s",
    "type": {
      "measurement": {}
    }
  }
}
```

2. Exécutez la commande suivante pour activer les notifications pour la propriété de ressource. Remplacez *property-alias* par l'alias de propriété de la réponse de la commande précédente ou omettez `--property-alias` pour mettre à jour la propriété sans alias.

```
aws iotsitewise update-asset-property \
  --asset-id asset-id \
  --property-id property-id \
  --property-notification-state ENABLED \
  --property-alias property-alias
```

   Vous pouvez également passer `--property-notification-state DISABLED` pour désactiver les notifications pour la propriété de ressource.

Interrogation des messages de notification de propriété de ressource

Pour interroger les notifications relatives aux propriétés des actifs, créez des AWS IoT Core règles composées d'instructions SQL.

AWS IoT SiteWise publie les mises à jour des données relatives aux propriétés des actifs dans AWS IoT Core au format suivant.

```
{
  "type": "PropertyValueUpdate",
  "payload": {
    "assetId": "String",
    "propertyId": "String",
    "values": [
      {
        "timestamp": {
          "timeInSeconds": Number,
          "offsetInNanos": Number
```

```
        },
        "quality": "String",
        "value": {
          "booleanValue": Boolean,
          "doubleValue": Number,
          "integerValue": Number,
          "stringValue": "String"
        }
      }
    ]
  }
}
```

Chaque structure de la `values` liste est une structure timestamp-quality-value (TQV).

- `timestamp` contient l'heure d'époque Unix actuelle en secondes avec un décalage en nanosecondes.
- La métrique `quality` contient l'une des chaînes suivantes, qui indiquent la qualité du point de données :
  - `GOOD`— Les données ne sont affectées par aucun problème.
  - `BAD`— Les données sont affectées par un problème tel qu'une défaillance du capteur.
  - `UNCERTAIN`— Les données sont affectées par un problème tel que l'imprécision du capteur.
- `value` contient l'un des champs suivants, selon le type de la propriété :
  - `booleanValue`
  - `doubleValue`
  - `integerValue`
  - `stringValue`

Pour analyser les valeurs sorties du tableau `values`, vous devez utiliser des requêtes d'objets imbriqués complexes dans les instructions SQL de vos règles. Pour plus d'informations, consultez la section Requêtes d'objets imbriqués dans le guide du AWS IoT développeur ou consultez le Publication de mises à jour de la valeur des propriétés sur Amazon DynamoDB didacticiel pour un exemple spécifique d'analyse des messages de notification relatifs aux propriétés des actifs.

Example Exemple d'interrogation pour extraire le tableau de valeurs

L'instruction suivante montre comment interroger le tableau de valeurs de propriété mises à jour pour une propriété de type double spécifique sur toutes les ressources avec cette propriété.

```
SELECT
  (SELECT VALUE (value.doubleValue) FROM payload.values) AS windspeed
FROM
  '$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/assets/+/
properties/a1b2c3d4-5678-90ab-cdef-33333EXAMPLE'
WHERE
  type = 'PropertyValueUpdate'
```

L'instruction d'interrogation de la règle précédente génère les données dans le format suivant.

```
{
  "windspeed": [
    26.32020195042838,
    26.282584572975477,
    26.352566977372508,
    26.283084346171442,
    26.571883739599322,
    26.60684140743005,
    26.628738636715045,
    26.273486932802125,
    26.436379105473964,
    26.600590095377303
  ]
}
```

Example Exemple d'interrogation pour extraire une valeur unique

L'instruction suivante montre comment interroger la première valeur du tableau de valeurs de propriété pour une propriété de type double spécifique sur tous les actifs avec cette propriété.

```
SELECT
  get((SELECT VALUE (value.doubleValue) FROM payload.values), 0) AS windspeed
FROM
  '$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/assets/+/
properties/a1b2c3d4-5678-90ab-cdef-33333EXAMPLE'
WHERE
  type = 'PropertyValueUpdate'
```

L'instruction d'interrogation de la règle précédente génère les données dans le format suivant.

```
{
```

```
  "windspeed": 26.32020195042838
}
```

> **Important**
>
> Cette instruction de requête de règle ignore les mises à jour de valeurs autres que la première dans chaque lot. Chaque lot peut contenir jusqu'à 10 valeurs. Si vous devez inclure les valeurs restantes, vous devez configurer une solution plus complexe pour générer des valeurs de propriété de ressources vers d'autres services. Par exemple, vous pouvez définir une règle avec une AWS Lambda action permettant de republier chaque valeur du tableau dans un autre sujet, et définir une autre règle pour interroger ce sujet et publier chaque valeur selon l'action de règle souhaitée.

Exportez des données vers Amazon S3 avec des notifications relatives aux propriétés des actifs

Vous pouvez exporter les données entrantes depuis AWS IoT SiteWise un compartiment Amazon S3 de votre compte. Vous pouvez sauvegarder vos données dans un format que vous pouvez utiliser pour créer des rapports historiques ou pour analyser vos données à l'aide de méthodes complexes.

> **Note**
>
> AWS IoT SiteWise prend également en charge le stockage à froid qui vous permet d'enregistrer des données dans un compartiment Amazon S3 géré par le client. Pour plus d'informations sur les niveaux de stockage pris en charge, consultezGestion du stockage des données.

AWS IoT SiteWise fournit cette fonctionnalité sous forme de AWS CloudFormation modèle. Lorsque vous créez une pile à partir du modèle, vous AWS CloudFormation créez les AWS ressources nécessaires pour diffuser les données entrantes AWS IoT SiteWise vers un compartiment S3.

Le compartiment S3 reçoit ensuite toutes les données de propriété de vos actifs envoyées à partir des messages de mise à jour de la valeur des AWS IoT SiteWise propriétés. Le compartiment S3 reçoit également vos métadonnées d'actif, qui incluent les noms des actifs et des propriétés et d'autres informations.

Pour plus d'informations sur la façon d'activer les messages de mise à jour de la valeur des propriétés pour les propriétés des actifs à exporter vers Amazon S3, consultezInteraction avec d'autres AWS services.

Cette fonctionnalité stocke les données de propriété et les métadonnées de vos actifs au format Apache Parquet dans Amazon S3. Parquet est un format de données en colonnes qui économise de l'espace et permet des requêtes plus rapides par rapport aux formats orientés ligne comme JSON.

> **Note**
>
> Lorsque cette fonctionnalité récupère les métadonnées des actifs, elle prend en charge jusqu'à environ 1 500 actifs. Cette limitation s'applique uniquement aux métadonnées des actifs. Cette limitation ne s'applique pas au nombre d'actifs pris en charge lorsque la fonctionnalité exporte les données de propriété des actifs.

Le nom de chaque ressource inclut un préfixe que vous pouvez personnaliser lorsque vous créez la pile. Il s'agit notamment des ressources suivantes :

- Un compartiment Amazon S3
- AWS Lambda fonctions
- Une AWS IoT Core règle
- AWS Identity and Access Management rôles
- Un stream Amazon Data Firehose
- Une AWS Glue base de données

Pour obtenir la liste complète, consultez Ressources créées à partir du modèle.

> **Important**
>
> Les ressources créées et consommées par ce AWS CloudFormation modèle vous seront facturées. Ces frais incluent le stockage et le transfert de données pour plusieurs AWS services.

Rubriques

- Créez la AWS CloudFormation pile

- Afficher vos données dans Amazon S3
- Analysez les données exportées avec Amazon Athena
- Ressources créées à partir du modèle

Créez la AWS CloudFormation pile

Vous devez créer un stack in AWS CloudFormation pour exporter les données de vos actifs vers Amazon S3.

Pour exporter des données vers Amazon S3

1. Ouvrez le modèle AWS CloudFormation et connectez-vous au AWS Management Console.
2. Dans la page Créer une pile, choisissez Suivant en bas de la page.
3. Sur la page Spécifier les détails de la pile, entrez un BucketNamepour le compartiment S3 créé par ce modèle afin de recevoir les données relatives aux actifs. Le nom de ce compartiment doit être globalement unique. Pour plus d'informations, consultez la section Règles relatives à l'attribution des noms de compartiments dans le Guide de l'utilisateur Amazon Simple Storage Service.
4. (Facultatif) Modifiez les autres paramètres du modèle :
   - GlobalResourcePrefix— Un préfixe pour les noms des ressources globales, telles que les rôles IAM, créés à partir de ce modèle.
   - LocalResourcePrefix— Un préfixe pour les noms des ressources créées à partir de ce modèle dans la région actuelle.

   > **Note**
   >
   > Si vous créez ce modèle plusieurs fois, vous devez modifier le nom du compartiment et les paramètres du préfixe de ressource afin d'éviter les conflits de noms de ressources.
5. Choisissez Next (Suivant).
6. Sur la page Configurer les options de pile, choisissez Suivant.
7. Au bas de la page, cochez la case indiquant que je reconnais que des ressources IAM AWS CloudFormation peuvent être créées.
8. Sélectionnez Créer la pile.

La création de la pile prend quelques minutes. Si la pile n'est pas créée, votre compte a peut-être des autorisations insuffisantes ou vous avez peut-être entré un nom de compartiment qui existe déjà. Procédez comme suit pour supprimer la pile et réessayez :

a. Choisissez Delete (Supprimer) dans le coin supérieur droit.

   La suppression de la pile prend quelques minutes.

   > **Note**
   >
   > AWS CloudFormation ne supprime pas les compartiments S3 ni les groupes de CloudWatch journaux. Vous pouvez supprimer ces ressources dans les consoles de ces services.

b. Si la pile n'a pas été supprimée, choisissez à nouveau Supprimer.

c. Si la pile ne parvient pas à être supprimée à nouveau, suivez les étapes de la AWS CloudFormation console pour ignorer les ressources qui n'ont pas pu être supprimées, puis réessayez.

9. Une fois la AWS CloudFormation pile créée avec succès, suivez la procédure suivante pour explorer les données relatives aux propriétés de vos actifs dans Amazon S3.

> **Important**
>
> Après avoir créé la pile, vous pouvez voir les nouvelles ressources dans votre AWS compte. La fonctionnalité peut cesser de fonctionner correctement si vous supprimez ou modifiez ces ressources. Nous vous recommandons de ne pas modifier ces ressources, sauf si vous souhaitez arrêter d'envoyer des données au compartiment ou personnaliser cette fonctionnalité.

Afficher vos données dans Amazon S3

Après avoir créé la fonctionnalité, vous pouvez consulter les données de propriété et les métadonnées de vos actifs dans Amazon S3.

> **Note**
>
> Les métadonnées des actifs sont mises à jour toutes les six heures. Vous devrez peut-être attendre jusqu'à six heures pour que les métadonnées des actifs apparaissent dans le compartiment S3.

Cette fonctionnalité stocke les données de propriété d'actif dans les colonnes suivantes, où chaque ligne contient un point de données :

- type — Type de notification de propriété (`PropertyValueUpdate`).
- asset_id — L'ID de la ressource qui a reçu un point de données.
- asset_property_id — L'ID de la propriété qui a reçu un point de données pour l'actif.
- time_in_seconds — Heure à laquelle les données ont été reçues, exprimée en secondes à l'époque Unix.
- offset_in_nanos — Le décalage en nanosecondes par rapport à. `timeInSeconds`
- asset_property_quality — Qualité du point de données :, ou. `GOOD` `UNCERTAIN` `BAD`
- asset_property_value — La valeur du point de données.
- asset_property_data_type — Type de données de la propriété de l'actif :,, ou. `boolean` `double` `integer` `string`

Cette fonctionnalité stocke les métadonnées des actifs dans les colonnes suivantes, où chaque ligne contient une propriété d'actif :

- asset_id — L'ID de l'actif.
- asset_name — Le nom de l'actif.
- asset_model_id — L'ID du modèle de l'actif.
- asset_property_id — L'ID de la propriété de l'actif.
- asset_property_name — Le nom de la propriété de l'actif.
- asset_property_data_type — Type de données de la propriété de l'actif :,, ou. `BOOLEAN` `DOUBLE` `INTEGER` `STRING`
- asset_property_unit — Unité de la propriété de l'actif.
- asset_property_alias — Alias de la propriété de l'actif.

Pour consulter vos AWS IoT SiteWise données dans Amazon S3

1. Accédez à la console Amazon S3.
2. Dans la liste des compartiments, choisissez le compartiment avec le nom que vous avez choisi lors de la création du modèle.
3. Dans le compartiment, choisissez l'un des dossiers suivants :
   - `asset-property-updates`— Ce dossier contient les données relatives aux propriétés des actifs exportées depuis AWS IoT SiteWise.
   - `asset-metadata`— Ce dossier contient les détails des actifs exportés depuis AWS IoT SiteWise.
4. Choisissez l'objet que vous souhaitez afficher.
5. Sur la page de l'objet, procédez comme suit :
   a. Choisissez l'onglet Sélectionner à partir.

      Dans ce panneau, vous pouvez prévisualiser les enregistrements des fichiers Parquet.
   b. Pour Format de fichier, choisissez Parquet.
   c. Pour afficher le contenu du fichier au format JSON, choisissez Afficher l'aperçu du fichier.

> **Note**
>
> Si de nouvelles données n'apparaissent pas dans le compartiment, vérifiez que vous avez activé les notifications de mise à jour des valeurs de propriété pour vos propriétés d'actif. Pour plus d'informations, consultez Interaction avec d'autres AWS services.

Pour de plus amples informations sur l'analyse des données de vos ressources stockées dans le compartiment S3, veuillez consulter Analysez les données exportées avec Amazon Athena.

Analysez les données exportées avec Amazon Athena

Une fois que vous avez enregistré les données relatives aux propriétés de vos actifs dans Amazon S3, vous pouvez utiliser plusieurs AWS services pour générer des rapports ou analyser et interroger vos données :

- Exécutez des requêtes SQL sur vos données à l'aide d'Amazon Athena.

- Réalisez des analyses de mégadonnées à l'aide d'Amazon EMR.
- Recherchez et analysez vos données à l'aide d'Amazon OpenSearch Service.

Vous trouverez d'autres AWS services susceptibles d'interagir avec vos données dans Amazon S3 dans la section Analytics du AWS Management Console.

> **Note**
>
> La pile crée une AWS Glue base de données pour formater les données des propriétés des actifs. Vous ne pouvez pas interroger cette base de données pour les données d'actif. Suivez les étapes décrites dans cette section pour créer une AWS Glue base de données que vous pouvez interroger.

Dans ce didacticiel, vous apprendrez comment configurer les conditions requises pour utiliser Amazon Athena et comment utiliser Athena pour exécuter des requêtes SQL sur les données de vos actifs exportées. AWS IoT SiteWise Pour interroger des données avec Athena, vous devez d'abord les renseigner AWS Glue Data Catalog avec les données de vos actifs. Le catalogue de données contient des bases de données et des tables, et Athena peut accéder aux données du catalogue de données. Vous pouvez créer un AWS Glue robot qui met régulièrement à jour le catalogue de données avec les données de vos actifs exportés.

Rubriques

- Configuration d'un analyseur pour renseigner le AWS Glue Data Catalog
- Interrogation de données avec Athena

Configuration d'un analyseur pour renseigner le AWS Glue Data Catalog

AWS Glue les robots explorent les magasins de données pour remplir les tables dans le. AWS Glue Data Catalog Dans cette procédure, vous créez et exécutez un AWS Glue robot d'exploration pour votre compartiment S3 qui contient les données d'actifs exportées. L'analyseur crée une table pour les mises à jour des propriétés des ressources et une table pour les métadonnées des ressources. Vous pouvez ensuite exécuter des requêtes SQL sur ces tables avec Athena. Pour plus d'informations, consultez la section Remplissage AWS Glue Data Catalog et définition des robots d'exploration dans le Guide du AWS Glue développeur.

Pour créer un AWS Glue crawler

1. Accédez à la console AWS Glue.
2. Dans le panneau de navigation, sélectionnez Crawlers. (Analyseurs)
3. Choisissez Add crawler (Ajouter un crawler).
4. Sur la page Ajouter un analyseur, procédez comme suit :

   a. Entrez un nom pour votre analyseur, par exemple **`IoTSiteWiseDataCrawler`**, puis choisissez Suivant.

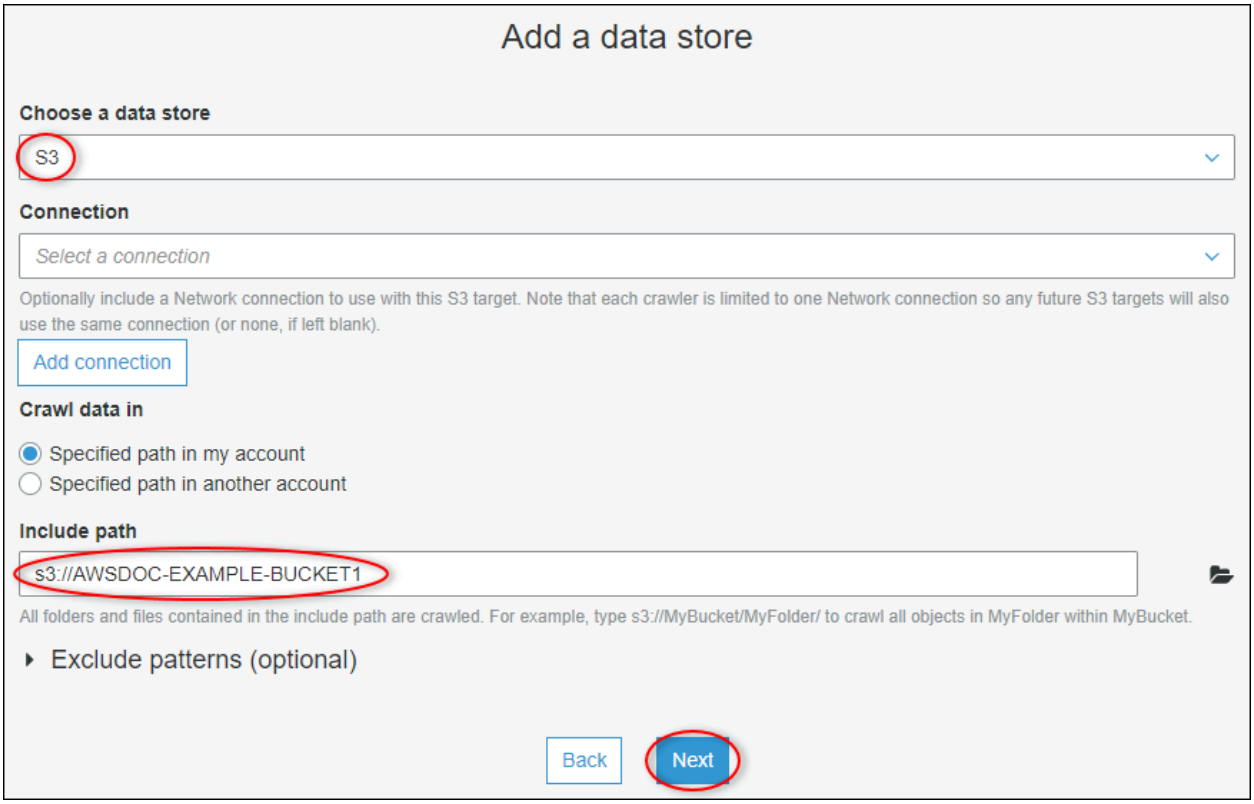
   b. Pour Type source d'analyseur, choisissez Magasins de données, puis Suivant.

   c. Sur la page Ajouter un magasin de données, procédez comme suit :

      i. Dans Choisir un magasin de données, choisissez S3.

      ii. Dans Inclure le chemin, entrez **`s3://DOC-EXAMPLE-BUCKET1`** pour ajouter votre compartiment de données de ressources en tant que magasin de données. Remplacez DOC-EXAMPLE-BUCKET1 par le nom du bucket que vous avez choisi lors de la création de la pile.

      iii. Choisissez Suivant.



   d. Sur la page Ajouter un autre magasin de données, choisissez Non, puis Suivant.

e. Sur la page Choisissez un rôle IAM, procédez comme suit :

   i. Pour créer un nouveau rôle de service permettant d' AWS Glue accéder au compartiment S3, choisissez Create an IAM role.

   ii. Entrez un suffixe pour le nom de votre rôle, par exemple **`IoTSiteWiseDataCrawler`**.

   iii. Choisissez Suivant.

f. Pour Fréquence, choisissez Toutes les heures, puis Suivant. L'analyseur met à jour les tables avec de nouvelles données chaque fois qu'il s'exécute. Vous pouvez donc choisir la fréquence qui correspond à votre cas d'utilisation.

g. Sur la page Configurer la sortie de l'analyseur, procédez comme suit :

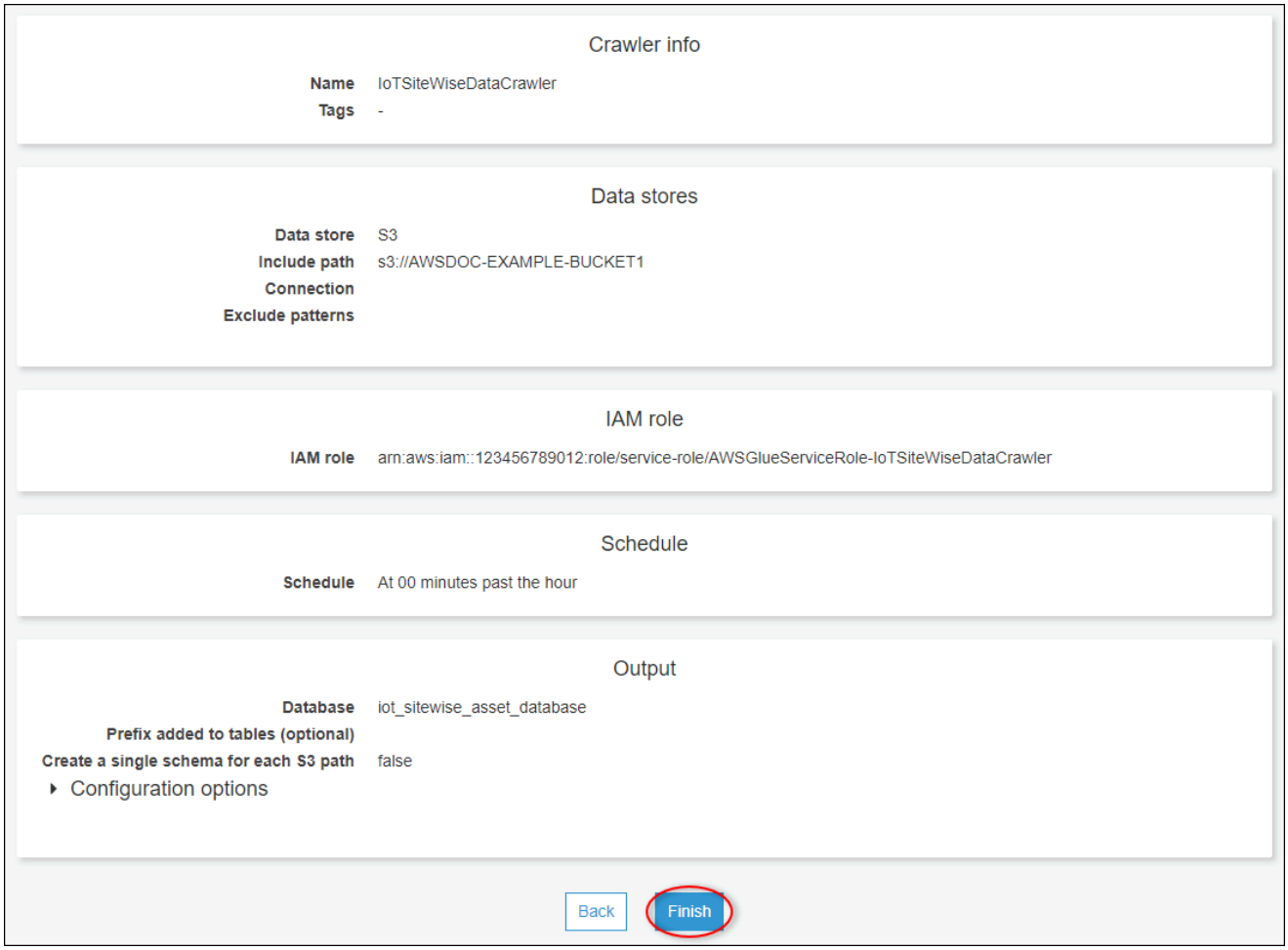
   i. Choisissez Ajouter une base de données pour créer une AWS Glue base de données pour les données de vos actifs.

   ii. Entrez un nom pour la base de données, par exemple **`iot_sitewise_asset_database`**.

   iii. Choisissez Créer.

   iv. Choisissez Suivant.

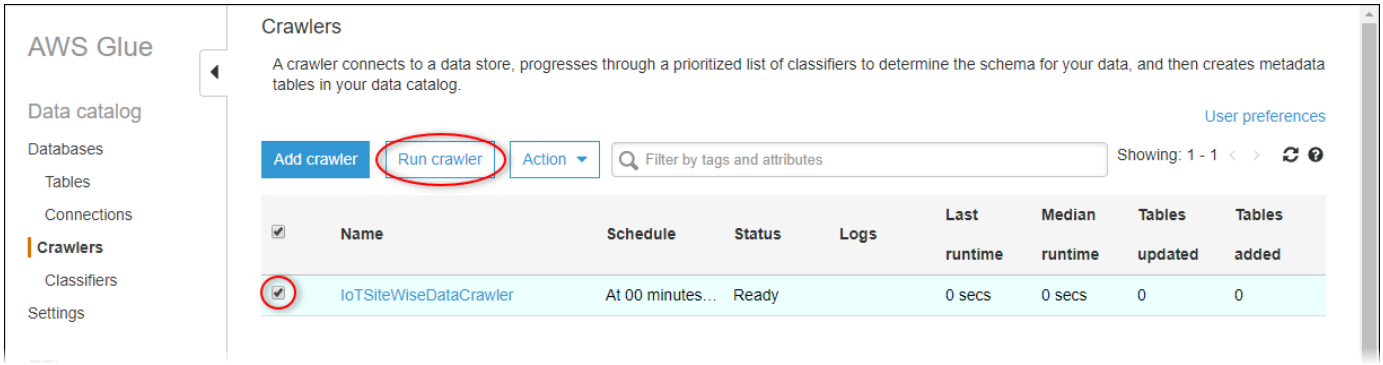
h. Passez en revue les détails de l'analyseur, puis choisissez Terminer.



Par défaut, votre nouvel analyseur ne s'exécute pas immédiatement. Vous devez l'exécuter manuellement ou attendre qu'il s'exécute selon la planification configurée.

Pour exécuter un analyseur

1. Sur la page Analyseurs, activez la case à cocher correspondant à votre nouvel analyseur, puis choisissez Exécuter un analyseur.



2. Attendez la fin de l'exécution de l'analyseur et l'affichage de l'état Prêt.

   L'exécution de l'analyseur peut prendre plusieurs minutes et son état se met automatiquement à jour.

3. Dans le volet de navigation, choisissez Tables.

   Deux nouvelles tables doivent s'afficher : asset_metadata et asset_property_updates.

Interrogation de données avec Athena

Athena découvre automatiquement les tableaux de données de vos actifs dans le. AWS Glue Data Catalog Pour effectuer des requêtes à l'intersection de ces tables, vous pouvez créer une vue sous la forme d'une table de données logique. Pour plus d'informations, consultez la section Utilisation des vues dans le guide de l'utilisateur d'Amazon Athena.

Une fois que vous avez créé une vue qui combine les données et les métadonnées de propriétés de ressources, vous pouvez exécuter des requêtes qui génèrent les valeurs de propriété avec des noms de ressources et de propriétés attachés. Pour plus d'informations, consultez la section Exécution de requêtes SQL à l'aide d'Amazon Athena dans le guide de l'utilisateur d'Amazon Athena.

Pour interroger les données des actifs avec Athena

1. Accédez à la console Athena.

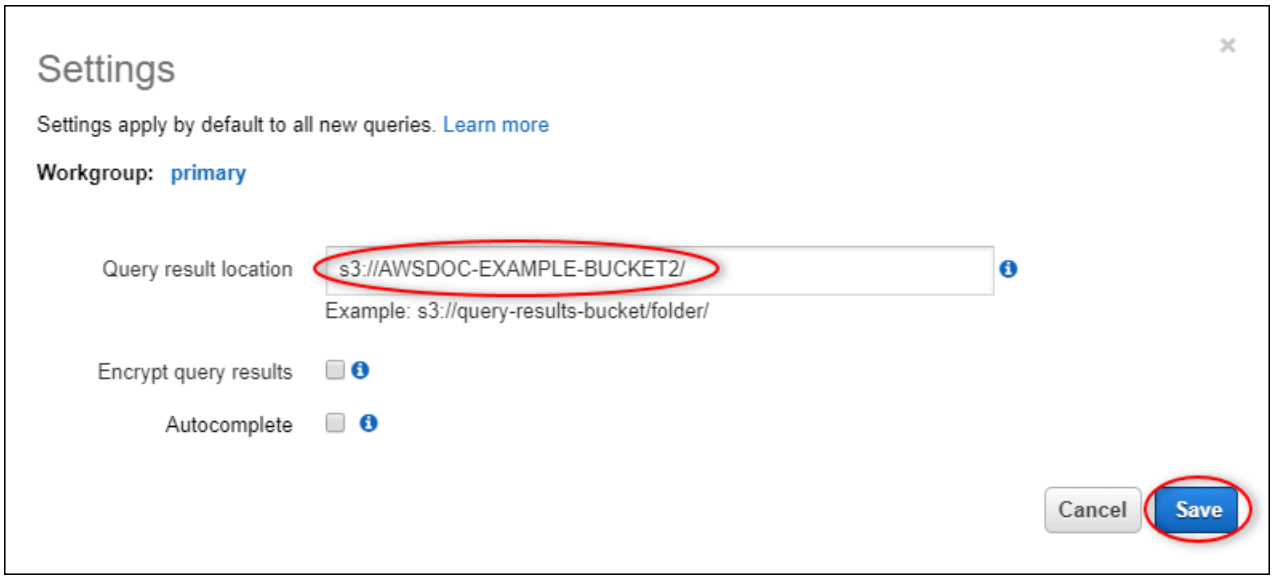
   Si la page Mise en route s'affiche, choisissez Démarrer.

2. Si vous utilisez Athena pour la première fois, suivez les étapes ci-dessous pour configurer un compartiment S3 pour les résultats des requêtes. Athena stocke les résultats de vos requêtes dans ce compartiment.

   > **Important**
   >
   > Utilisez un compartiment différent de celui de votre compartiment de données de ressources, afin que l'analyseur que vous avez créé précédemment n'analyse pas les résultats de la requête. Nous vous recommandons de créer un bucket à utiliser uniquement pour les résultats des requêtes Athena. Pour plus d'informations, consultez Comment créer un compartiment S3 ? dans le guide de l'utilisateur d'Amazon Simple Storage Service.

a. Sélectionnez Settings (Paramètres).

b. Dans Emplacement des résultats de la requête, entrez le compartiment S3 pour les résultats de la requête Athena. Le compartiment doit se terminer par /.

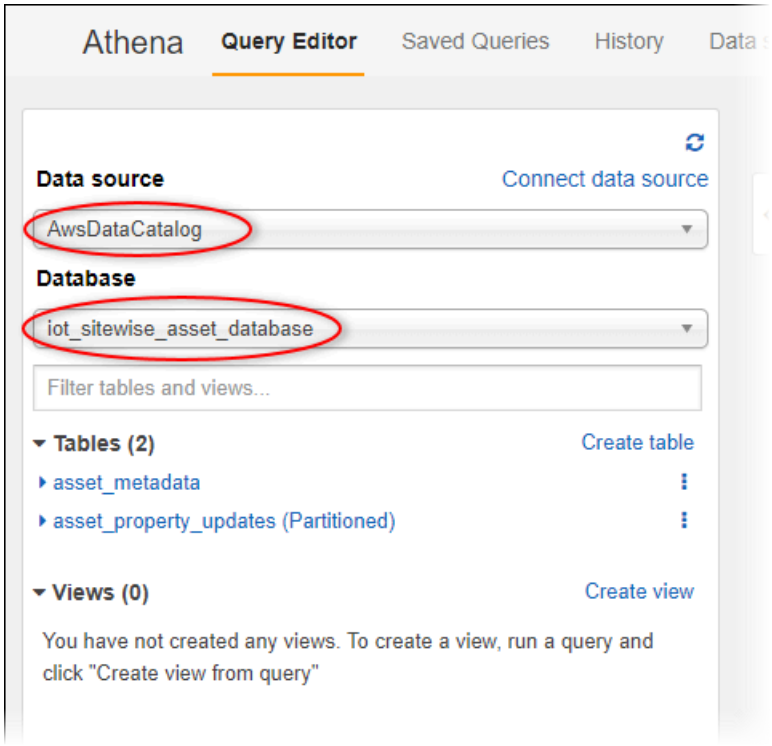


c. Choisissez Enregistrer.

3. Le panneau de gauche contient la source de données à interroger. Procédez comme suit :

a. Pour Source de données, choisissez AwsDataCatalogd'utiliser le AWS Glue Data Catalog.

b. Pour Base de données, choisissez la AWS Glue base de données que vous avez créée avec le robot d'exploration.



Vous devez voir deux tables : asset_metadata et asset_property_updates.

4. Pour créer une vue à partir de la combinaison de données et de métadonnées de propriétés de ressources, entrez la requête suivante, puis choisissez Exécuter la requête.

```
CREATE
        OR REPLACE VIEW iot_sitewise_asset_data AS
SELECT "from_unixtime"("time_in_seconds" + ("offset_in_nanos" / 1000000000))
 "timestamp",
         "metadata"."asset_name",
         "metadata"."asset_property_name",
         "data"."asset_property_value",
         "metadata"."asset_property_unit",
         "metadata"."asset_property_alias"
FROM ( "iot_sitewise_asset_database".asset_property_updates data
INNER JOIN "iot_sitewise_asset_database".asset_metadata metadata
    ON ( ("data"."asset_id" = "metadata"."asset_id")
        AND ("data"."asset_property_id" = "metadata"."asset_property_id") ) );
```

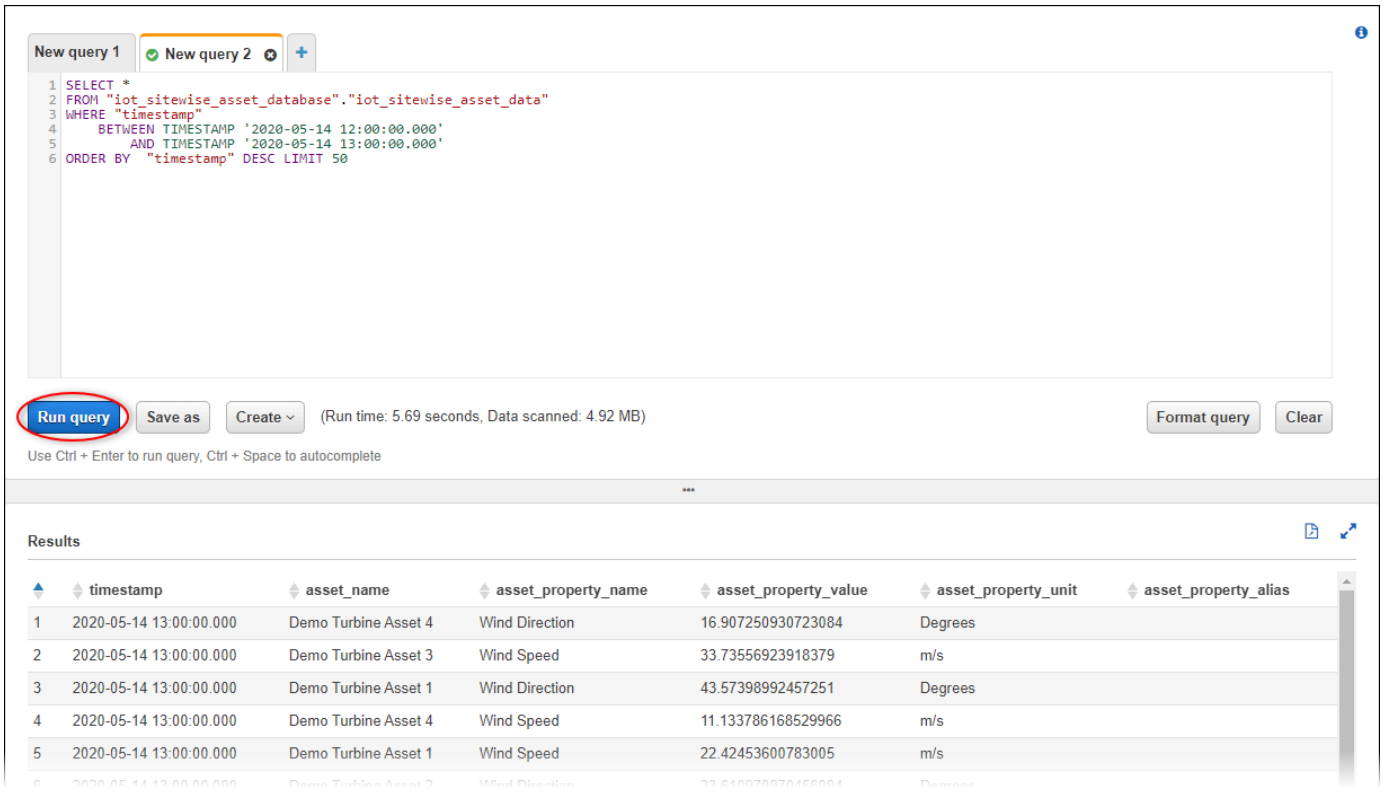
Cette requête joint les tables de données et de métadonnées de propriétés de ressources sur l'ID de ressource et l'ID de propriété pour créer une vue. Vous pouvez exécuter cette requête plusieurs fois, car elle remplace la vue existante, si elle existe déjà.

5. Pour ajouter une nouvelle requête, cliquez sur l'icône +.
6. Pour afficher un exemple de données de ressource, entrez la requête suivante, puis choisissez Exécuter la requête. Remplacez les horodatages par un intervalle pour lequel votre compartiment contient des données.

```
SELECT *
FROM "iot_sitewise_asset_database"."iot_sitewise_asset_data"
WHERE "timestamp"
    BETWEEN TIMESTAMP '2020-05-14 12:00:00.000'
        AND TIMESTAMP '2020-05-14 13:00:00.000'
ORDER BY  "timestamp" DESC LIMIT 50;
```

Cette requête génère jusqu'à 50 points de données entre deux horodatages. Les entrées les plus récentes sont affichées en premier.

Votre sortie de requête peut ressembler aux résultats suivants.



	timestamp	asset_name	asset_property_name	asset_property_value	asset_property_unit	asset_property_alias
1	2020-05-14 13:00:00.000	Demo Turbine Asset 4	Wind Direction	16.907250930723084	Degrees	
2	2020-05-14 13:00:00.000	Demo Turbine Asset 3	Wind Speed	33.73556923918379	m/s	
3	2020-05-14 13:00:00.000	Demo Turbine Asset 1	Wind Direction	43.57398992457251	Degrees	
4	2020-05-14 13:00:00.000	Demo Turbine Asset 4	Wind Speed	11.133786168529966	m/s	
5	2020-05-14 13:00:00.000	Demo Turbine Asset 1	Wind Speed	22.42453600783005	m/s	

Vous pouvez désormais exécuter des requêtes utiles à votre AWS IoT SiteWise application. Pour plus d'informations, consultez la référence SQL pour Amazon Athena dans le guide de l'utilisateur d'Amazon Athena.

Ressources créées à partir du modèle

Lorsque vous créez une pile à partir du modèle, AWS CloudFormation crée les ressources suivantes. Les noms de la plupart des ressources incluent un préfixe que vous pouvez personnaliser lorsque vous créez la pile.

Paramètres de nom de ressource

- `BucketName`— Le nom du compartiment S3 créé à partir de ce modèle qui reçoit les données des actifs.
- `GlobalResourcePrefix`— Préfixe pour les noms des ressources globales créées à partir de ce modèle. La valeur par défaut est `sitewise-export-to-s3`.
- `LocalResourcePrefix`— Un préfixe pour les noms des ressources créées à partir de ce modèle dans la région actuelle. La valeur par défaut est `sitewise_export_to_s3`.

Ressources créées par le AWS CloudFormation modèle

Ressource	Description	Nom
Compartiment S3 pour les données traitées	Ce compartiment contient deux dossiers. Un dossier reçoit les données aplaties et formatées du flux de diffusion Firehose, tandis que l'autre dossier reçoit les métadonné es des actifs.	`${BucketName}`
Base de données AWS Glue	Cette base de données contient la AWS Glue table créée par cette pile.	`${LocalResourcePre fix}_firehose_glue _database`
Tableau AWS Glue	Le flux de diffusion Firehose utilise ce tableau pour formater les données au format Parquet.	`${LocalResourcePre fix}_firehose_glue _table`

Ressource	Description	Nom
Fonction AWS Lambda qui transforme les données	Cette fonction aplanit le tableau de valeurs dans les messages de notification de valeur de propriété envoyés depuis. AWS IoT SiteWise	`${LocalResourcePrefix}_lambda_transform_function`
Rôle IAM pour la fonction Lambda de transformation	Ce rôle permet à Lambda de stocker les journaux d'exécution de la fonction de transformation.	`${GlobalResourcePrefix}-lambda-transform-role`
Politique IAM pour le rôle de la fonction Transform Lambda	Cette politique permet à Lambda de stocker les journaux d'exécution de la fonction de transformation.	`${GlobalResourcePrefix}-lambda-transform-policy`
CloudWatch Groupe de journaux pour la fonction de transformation	Ce groupe de journaux contient des journaux pour la fonction de transformation.	`/aws/lambda/${LocalResourcePrefix}_lambda_transform_function`
Fonction Lambda qui collecte les métadonnées des actifs	Cette fonction récupère des informations sur les actifs AWS IoT SiteWise et les stocke dans un compartiment Amazon S3 créé par cette pile.	`${LocalResourcePrefix}_lambda_metadata_function`
Couche Lambda pour la fonction de métadonnées	Cette couche fournit un AWS SDK qui contient les AWS IoT SiteWise opérations utilisées par la fonction de métadonnées.	`${LocalResourcePrefix}_lambda_metadata_layer`

Ressource	Description	Nom
Rôle IAM pour la fonction Lambda de métadonnées	Ce rôle permet à Lambda de récupérer des informations sur les actifs dans. AWS IoT SiteWise	`${GlobalResourcePrefix}-lambda-metadata-role`
Politique IAM pour le rôle de la fonction Lambda de métadonnées	Cette politique permet à Lambda de récupérer des informations sur les actifs dans. AWS IoT SiteWise	`${GlobalResourcePrefix}-lambda-metadata-policy`
EventBridgeévénement planifié pour la fonction Lambda de métadonnées	Cet événement planifié exécute le Lambda de métadonnées toutes les 6 heures pour mettre à jour le compartiment de métadonnées des actifs.	`${LocalResourcePrefix}-metadata-event`
CloudWatch Groupe de journaux pour la fonction de métadonnées	Ce groupe de journaux contient des journaux pour la fonction de métadonnées.	`/aws/lambda/${LocalResourcePrefix}_lambda_metadata_function`
Règle AWS IoT	Cette règle interroge les messages de notification relatifs à la valeur des propriétés et envoie les données relatives aux actifs à un flux de diffusion Amazon Data Firehose.	`${LocalResourcePrefix}_iot_topic_rule`
Rôle IAM pour la règle AWS IoT	Ce rôle permet d' AWS IoT envoyer des données au flux de diffusion Firehose.	`${GlobalResourcePrefix}-core-firehose-role`

Ressource	Description	Nom
Politique IAM pour le rôle de AWS IoT règle	Cette politique permet d' AWS IoT envoyer des données au flux de diffusion Firehose.	`${GlobalResourcePrefix}-core-firehose-policy`
Flux de livraison Firehose	Ce flux de diffusion consomme les données de la AWS IoT règle, les aplatit à l'aide d'une fonction Lambda et les transmet à Amazon S3.	`${LocalResourcePrefix}_firehose_delivery_stream`
Rôle IAM pour le flux de diffusion	Ce rôle permet à Firehose d'effectuer des opérations sur le compartiment S3, la AWS Glue table, les fonctions Lambda et CloudWatch le groupe de journaux Logs.	`${GlobalResourcePrefix}-firehose-delivery-role`
CloudWatch Groupe de journaux pour le flux de diffusion	Ce groupe de journaux contient un flux de journaux qui reçoit des journaux sur le flux de diffusion Firehose. `S3 Delivery`	`/aws/kinesisfirehose/${LocalResourcePrefix}_firehose_delivery_stream`

Intégration à Grafana

Grafana est une plateforme de visualisation de données que vous pouvez utiliser pour visualiser et surveiller les données dans des tableaux de bord. Dans les versions 7.3.0 et ultérieures de Grafana, vous pouvez utiliser le AWS IoT SiteWise plugin pour visualiser les données de vos AWS IoT SiteWise actifs dans les tableaux de bord Grafana. Vous pouvez visualiser les données provenant de plusieurs AWS sources (telles qu'AWS IoT SiteWiseAmazon Timestream et CloudWatch Amazon) et d'autres sources de données à l'aide d'un seul tableau de bord Grafana.

Deux options s'offrent à vous pour utiliser le AWS IoT SiteWise plugin :

- Serveurs Grafana locaux

Vous pouvez configurer le AWS IoT SiteWise plugin sur un serveur Grafana que vous gérez. Pour plus d'informations sur l'ajout et l'utilisation du plugin, consultez le fichier AWS IoT SiteWiseDatasource README sur le GitHub site Web.

- AWSService géré pour Grafana

  Vous pouvez utiliser le AWS IoT SiteWise plugin dans le AWS Managed Service for Grafana (AMG). AMG gère les serveurs Grafana pour vous afin que vous puissiez visualiser vos données sans avoir à créer, empaqueter ou déployer du matériel ou toute autre infrastructure Grafana. Pour plus d'informations, consultez les rubriques suivantes dans le guide de l'utilisateur de AWS Managed Service for Grafana :

  - Qu'est-ce qu'Amazon Managed Service for Grafana (AMG) ?
  - Utilisation de la source AWS IoT SiteWise de données

Example Exemple de tableau de bord Grafana

Le tableau de bord Grafana suivant permet de visualiser le parc éolien de démonstration. Vous pouvez accéder à ce tableau de bord de démonstration sur le site Web de Grafana Play.

Intégration d'AWS IoT SiteWise et de AWS IoT TwinMaker

L'intégration AWS IoT TwinMaker permet d'accéder à des fonctionnalités robustesAWS IoT SiteWise, telles que l'`ExecuteQuery`API de récupération de AWS IoT SiteWise données et la recherche avancée d'actifs dans la AWS IoT SiteWise console. Pour intégrer les services et utiliser ces fonctionnalités, vous devez d'abord activer l'intégration.

Rubriques

- Activation de l'intégration
- Intégration d'AWS IoT SiteWise et de AWS IoT TwinMaker

Activation de l'intégration

Les administrateurs peuvent utiliser les politiques JSON AWS pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions. L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Pour plus d'informations sur les actions AWS IoT SiteWise prises en charge, consultez la section Actions définies par AWS IoT SiteWise dans la référence d'autorisation de service.

Pour plus d'informations sur les rôles AWS IoT TwinMaker liés à un service, consultez la section Rôles liés à un service AWS IoT TwinMaker dans le Guide de l'utilisateur. AWS IoT TwinMaker

Avant de pouvoir intégrer AWS IoT SiteWise etAWS IoT TwinMaker, vous devez accorder les autorisations suivantes qui permettent l'intégration AWS IoT SiteWise à un espace de travail AWS IoT TwinMaker lié :

- `iotsitewise:EnableSiteWiseIntegration`— Permet AWS IoT SiteWise de s'intégrer à un AWS IoT TwinMaker espace de travail lié. Cette intégration permet AWS IoT TwinMaker de lire toutes vos informations de modélisation AWS IoT SiteWise via un rôle AWS IoT TwinMaker lié à un service. Pour activer cette autorisation, ajoutez la politique suivante à votre rôle IAM :

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

Intégration d'AWS IoT SiteWise et de AWS IoT TwinMaker

Pour intégrer AWS IoT SiteWise etAWS IoT TwinMaker, vous devez disposer des éléments suivants :

- AWS IoT SiteWiserôle lié au service configuré dans votre compte

- AWS IoT TwinMakerrôle lié au service configuré dans votre compte
- AWS IoT TwinMakerespace de travail avec identifiant `IoTSiteWiseDefaultWorkspace` dans votre compte dans la région.

Pour intégrer à l'aide de la AWS IoT SiteWise console

Lorsque la AWS IoT TwinMaker bannière Intégration avec apparaît dans la console, choisissez Accorder l'autorisation. Les prérequis sont créés dans votre compte.

Pour effectuer l'intégration à l'aide du AWS CLI

Pour intégrer AWS IoT SiteWise et à AWS IoT TwinMaker l'aide duAWS CLI, entrez les commandes suivantes :

1. Appelez `CreateServiceLinkedRole` avec un `AWSServiceName` `deiotsitewise.amazonaws.com`.

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

2. Appelez `CreateServiceLinkedRole` avec un `AWSServiceName` de `iottwinmaker.amazonaws.com`.

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

3. Appelez `CreateWorkspace` avec un `ID` de`IoTSiteWiseDefaultWorkspace`.

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

Détecter les anomalies des équipements avec Amazon Lookout for Equipment

> **Note**
>
> La détection des anomalies n'est disponible que dans les régions où Amazon Lookout for Equipment est disponible.

Vous pouvez intégrer AWS IoT SiteWise Amazon Lookout for Equipment pour obtenir des informations sur votre équipement industriel grâce à la détection des anomalies et à la maintenance prédictive des équipements industriels. Lookout for Equipment est un service d'apprentissage automatique (ML) pour la surveillance des équipements industriels qui détecte le comportement anormal des équipements et identifie les défaillances potentielles. Lookout for Equipment vous permet de mettre en œuvre des programmes de maintenance prédictive et d'identifier les processus sous-optimaux liés aux équipements. Pour plus d'informations sur Lookout for Equipment, consultez l'article Qu'est-ce qu'Amazon Lookout for Equipment ? dans le guide de l'utilisateur d'Amazon Lookout for Equipment.

Lorsque vous créez une prédiction pour entraîner un modèle d'apprentissage automatique afin de détecter le comportement anormal de l'équipement, vous envoyez les valeurs AWS IoT SiteWise des propriétés des actifs à Lookout for Equipment pour entraîner un modèle d'apprentissage automatique afin de détecter le comportement anormal de l'équipement. Pour définir une définition de prédiction sur un modèle d'actif, vous devez spécifier les rôles IAM nécessaires pour que Lookout for Equipment accède à vos données et les propriétés à envoyer à Lookout for Equipment et à envoyer les données traitées à Amazon S3. Pour plus d'informations, consultez Création de modèles de ressources.

Pour intégrer AWS IoT SiteWise Lookout for Equipment à Lookout for Equipment, vous devez suivre les étapes de haut niveau suivantes :

- Ajoutez une définition de prédiction sur un modèle d'actif qui décrit les propriétés que vous souhaitez suivre. La définition de prédiction est un ensemble réutilisable de mesures, de transformations et de métriques qui est utilisé pour créer des prédictions sur les actifs basées sur ce modèle d'actif.
- Entraînez la prédiction en fonction des données historiques que vous fournissez.
- Planifier l'inférence, qui indique à AWS IoT SiteWise quelle fréquence une prédiction spécifique doit être exécutée.

Une fois l'inférence planifiée, le modèle Lookout for Equipment surveille les données qu'il reçoit de votre équipement et recherche les anomalies de comportement de l'équipement. Vous pouvez consulter et analyser les résultats dans SiteWise Monitor, à l'aide des opérations de l'API AWS IoT SiteWise GET ou de la console Lookout for Equipment. Vous pouvez également créer des alarmes à l'aide des détecteurs d'alarme du modèle d'équipement pour vous avertir en cas de comportement anormal de l'équipement.

Rubriques

- Ajouter une définition de prédiction (console)
- Entraînement d'une prédiction (console)
- Démarrer ou arrêter l'inférence sur une prédiction (console)
- Ajouter une définition de prédiction (CLI)
- Entraînement d'une prédiction et démarrage de l'inférence (CLI)
- Entraînement d'une prédiction (CLI)
- Démarrer ou arrêter l'inférence sur une prédiction (CLI)

Ajouter une définition de prédiction (console)

Pour commencer à envoyer les données collectées par AWS IoT SiteWise Lookout for Equipment, vous devez ajouter AWS IoT SiteWise une définition de prédiction à un modèle d'actif.

Pour ajouter une définition de prédiction à un modèle AWS IoT SiteWise d'actif

1. Accédez à la console AWS IoT SiteWise.
2. Dans le volet de navigation, choisissez Models et sélectionnez le modèle de ressource auquel vous souhaitez ajouter la définition de prédiction.
3. Choisissez Prédictions.
4. Choisissez Ajouter une définition de prédiction.
5. Définissez les détails de la définition de la prédiction.

    a. Entrez un nom unique et une description pour la définition de votre prédiction. Choisissez le nom avec soin, car une fois que vous avez créé la définition de prédiction, vous ne pouvez pas le modifier.

    b. Créez ou sélectionnez un rôle d'autorisation IAM qui permet de AWS IoT SiteWise partager les données de vos actifs avec Amazon Lookout for Equipment. Le rôle doit respecter les politiques IAM et de confiance suivantes. Pour obtenir de l'aide sur la création du rôle, voir Création d'un rôle à l'aide de politiques de confiance personnalisées (console).

    Politique 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"
        }
    ]
}
```

Politique d'approbation

```
{
    "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. Choisissez Suivant.

6. Sélectionnez les attributs de données (mesures, transformations et métriques) que vous souhaitez envoyer à Lookout for Equipment.

   a. (Facultatif) Sélectionnez les mesures.

   b. (Facultatif) Sélectionnez les transformations.

   c. (Facultatif) Sélectionnez les métriques.

   d. Choisissez Suivant.

7. Passez en revue vos sélections. Pour ajouter la définition de prédiction au modèle de ressource, sur la page de résumé, choisissez Ajouter une définition de prédiction.

Vous pouvez également modifier ou supprimer une définition de prédiction existante à laquelle sont associées des prédictions actives.

Entraînement d'une prédiction (console)

Après avoir ajouté une définition de prédiction à un modèle d'actifs, vous pouvez entraîner les prédictions relatives à vos actifs.

Pour entraîner une prédiction dans AWS IoT SiteWise

1. Accédez à la console AWS IoT SiteWise.
2. Dans le volet de navigation, choisissez Assets, puis sélectionnez l'actif que vous souhaitez surveiller.
3. Choisissez Prédictions.
4. Sélectionnez les prédictions que vous souhaitez entraîner.
5. Sous Actions, choisissez Commencer l'entraînement, puis procédez comme suit :

a. Sous Détails de la prédiction, sélectionnez un rôle d'autorisation IAM qui permet de AWS IoT SiteWise partager les données de vos actifs avec Lookout for Equipment. Si vous devez créer un nouveau rôle, choisissez Créer un nouveau rôle.

b. Pour les paramètres des données d'entraînement, entrez une plage temporelle des données d'entraînement pour sélectionner les données à utiliser pour entraîner la prédiction.

c. (Facultatif) Sélectionnez le taux d'échantillonnage des données après le post-traitement.

d. (Facultatif) Pour les étiquettes de données, fournissez un compartiment Amazon S3 et un préfixe contenant vos données d'étiquetage. Pour plus d'informations sur les données d'étiquetage, consultez la section Étiquetage de vos données dans le guide de l'utilisateur d'Amazon Lookout for Equipment.

e. Choisissez Suivant.

6. (Facultatif) Si vous souhaitez que la prédiction soit active dès la fin de l'entraînement, sous Paramètres avancés, sélectionnez Activer automatiquement la prédiction après l'entraînement, puis procédez comme suit :

   a. Sous Données d'entrée, pour Fréquence de téléchargement des données, définissez la fréquence à laquelle les données sont téléchargées, et pour Temps de décalage, définissez la quantité de mémoire tampon à utiliser.

   b. Choisissez Suivant.

7. Passez en revue les détails de la prédiction et choisissez Enregistrer et démarrer.

Démarrer ou arrêter l'inférence sur une prédiction (console)

> **Note**
>
> Les frais de Lookout for Equipment s'appliquent aux inférences planifiées avec les données transférées AWS IoT SiteWise entre Lookout for Equipment et Lookout for Equipment. Pour plus d'informations, consultez les tarifs d'Amazon Lookout for Equipment.

Si vous avez ajouté une prédiction « blookoutequipment : CreateDataset », mais que vous n'avez pas choisi de l'activer après l'entraînement, vous devez l'activer pour qu'elle puisse commencer à surveiller vos actifs.

Pour démarrer l'inférence d'une prédiction

1. Accédez à la console AWS IoT SiteWise.
2. Dans le volet de navigation, choisissez Assets, puis sélectionnez l'actif auquel la prédiction est ajoutée.
3. Choisissez Prédictions.
4. Sélectionnez les prédictions que vous souhaitez activer.
5. Sous Actions, choisissez Démarrer l'inférence, puis procédez comme suit :

    a. Sous Données d'entrée, pour Fréquence de téléchargement des données, définissez la fréquence à laquelle les données sont téléchargées, et pour Temps de décalage, définissez la quantité de mémoire tampon à utiliser.

    b. Choisissez Enregistrer et commencez.

Pour arrêter l'inférence pour une prédiction

1. Accédez à la console AWS IoT SiteWise.
2. Dans le volet de navigation, choisissez Assets, puis sélectionnez l'actif auquel la prédiction est ajoutée.
3. Choisissez Prédictions.
4. Sélectionnez les prédictions que vous souhaitez arrêter.
5. Sous Actions, choisissez Arrêter l'inférence.

Ajouter une définition de prédiction (CLI)

Pour définir une définition de prédiction sur un modèle d'actif nouveau ou existant, vous pouvez utiliser le AWS Command Line Interface (AWS CLI). Après avoir défini la définition de prédiction sur le modèle d'actif, vous entraînez et planifiez l'inférence pour une prédiction sur un actif AWS IoT SiteWise afin de détecter les anomalies avec Lookout for Equipment.

Prérequis

Pour effectuer ces étapes, vous devez avoir créé un modèle d'actif et au moins un actif. Pour plus d'informations, consultez Création d'un modèle d'actifs (AWS CLI) et Création d'un actif (AWS CLI).

Si vous débutez dans ce AWS IoT SiteWise domaine, vous devez appeler l'opération `CreateBulkImportJob` API pour y importer les valeurs des propriétés des actifs AWS IoT

SiteWise, qui seront utilisées pour entraîner le modèle. Pour plus d'informations, consultez Création d'une tâche d'importation en bloc (AWS CLI).

Pour ajouter une définition de prédiction

1. Créez un fichier, appelé `asset-model-payload.json`. Suivez les étapes décrites dans ces autres sections pour ajouter les détails de votre modèle d'actif au fichier, mais ne soumettez pas de demande de création ou de mise à jour du modèle d'actif.

   - Pour plus d'informations sur la création d'un modèle d'actifs, voir Création d'un modèle d'actifs (AWS CLI)
   - Pour plus d'informations sur la mise à jour d'un modèle d'actif existant, voir Mettre à jour un modèle d'actif ou de composant (AWS CLI)
2. Ajoutez un modèle composite Lookout for Equipment `assetModelCompositeModels` () au modèle d'actif en ajoutant le code suivant.

   - *`Property`*Remplacez-le par l'ID des propriétés que vous souhaitez inclure. Pour obtenir ces identifiants, appelez `DescribeAssetModel`.
   - *`RoleARN`*Remplacez-le par l'ARN d'un rôle IAM qui permet à Lookout for Equipment d'accéder AWS IoT SiteWise à vos données.

```
{
  ...
  "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. Créez le modèle d'actif ou mettez à jour le modèle d'actif existant. Effectuez l'une des actions suivantes :

   - Pour créer le modèle d'actif, exécutez la commande suivante :

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

   - Pour mettre à jour le modèle d'actif existant, exécutez la commande suivante. *asset-model-id*Remplacez-le par l'ID du modèle d'actif que vous souhaitez mettre à jour.

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

Après avoir exécuté la commande, notez le `assetModelId` dans la réponse.

Entraînement d'une prédiction et démarrage de l'inférence (CLI)

Maintenant que la définition de la prédiction est définie, vous pouvez entraîner les actifs en fonction de celle-ci et commencer l'inférence. Si vous souhaitez affiner votre prédiction sans commencer

l'inférence, passez directement àEntraînement d'une prédiction (CLI). Pour entraîner la prédiction et commencer à inférer sur l'actif, vous aurez besoin `assetId` de celui de la ressource cible.

Pour entraîner et démarrer l'inférence de la prédiction

1. Exécutez la commande suivante pour trouver le `assetModelCompositeModelId` dessous`assetModelCompositeModelSummaries`. *`asset-model-id`*Remplacez-le par l'ID du modèle d'actif que vous avez créé dansMettre à jour un modèle d'actif ou de composant (AWS CLI).

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

2. Exécutez la commande suivante pour trouver `actionDefinitionId` l'`TrainingWithInference`action. Remplacez *`asset-model-id`*par l'ID utilisé à l'étape précédente et remplacez *`asset-model-composite-model-id`*par l'ID renvoyé à l'étape précédente.

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

3. Créez un fichier appelé `train-start-inference-prediction.json` et ajoutez-y le code suivant, en remplaçant le suivant :

   - *`asset-id`*avec l'ID de l'actif cible
   - *`action-definition-id`*avec l'identifiant de l' TrainingWithInference action
   - *`StartTime`*avec le début des données d'entraînement, fournies en secondes
   - *`EndTime`*avec les données de fin d'entraînement, fournies en secondes d'époque
   - *`TargetSamplingRate`*avec le taux d'échantillonnage des données après post-traitement par Lookout for Equipment. Les valeurs autorisées sont :`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. Exécutez la commande suivante pour démarrer l'entraînement et l'inférence :

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

Entraînement d'une prédiction (CLI)

Maintenant que la définition de la prédiction est définie, vous pouvez entraîner les actifs en fonction de celle-ci. Pour entraîner la prédiction sur l'actif, vous aurez besoin `assetId` de celui de la ressource cible.

Pour entraîner la prédiction

1. Exécutez la commande suivante pour trouver le `assetModelCompositeModelId` dessous`assetModelCompositeModelSummaries`. *`asset-model-id`*Remplacez-le par l'ID du modèle d'actif que vous avez créé dansMettre à jour un modèle d'actif ou de composant (AWS CLI).

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

2. Exécutez la commande suivante pour trouver `actionDefinitionId` l'`Training`action. Remplacez *`asset-model-id`*par l'ID utilisé à l'étape précédente et remplacez *`asset-model-composite-model-id`*par l'ID renvoyé à l'étape précédente.

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

3. Créez un fichier appelé `train-prediction.json` et ajoutez-y le code suivant, en remplaçant le suivant :

- *asset-id*avec l'ID de l'actif cible
- *action-definition-id*avec l'identifiant de l'action de formation
- *StartTime*avec le début des données d'entraînement, fournies en secondes
- *EndTime*avec les données de fin d'entraînement, fournies en secondes d'époque
- (Facultatif) *BucketName* avec le nom du compartiment Amazon S3 qui contient vos données d'étiquette
- (Facultatif) *Prefix* avec le préfixe associé au compartiment Amazon S3.
- *TargetSamplingRate*avec le taux d'échantillonnage des données après post-traitement par Lookout for Equipment. Les valeurs autorisées sont :`PT1S | PT5S | PT10S | PT15S | PT30S | PT1M | PT5M | PT10M | PT15M | PT30M | PT1H`.

> **Note**
>
> Incluez à la fois le nom et le préfixe du compartiment, ou aucun des deux.

```
{
  "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. Exécutez la commande suivante pour démarrer l'entraînement :

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

Avant de pouvoir commencer l'inférence, vous devez suivre une formation. Pour vérifier le statut de la formation, effectuez l'une des opérations suivantes :

- Depuis la console, accédez à l'actif sur lequel porte la prédiction.

- À partir du AWS CLI, appelez `BatchGetAssetPropertyValue` en utilisant le `propertyId` nom de la `trainingStatus` propriété.

Démarrer ou arrêter l'inférence sur une prédiction (CLI)

Une fois la prédiction établie, vous pouvez commencer l'inférence pour demander à Lookout for Equipment de commencer à surveiller vos actifs. Pour démarrer ou arrêter l'inférence, vous aurez besoin `assetId` de la ressource cible.

Pour démarrer l'inférence

1. Exécutez la commande suivante pour trouver le `assetModelCompositeModelId` dessous`assetModelCompositeModelSummaries`. *`asset-model-id`*Remplacez-le par l'ID du modèle d'actif que vous avez créé dansMettre à jour un modèle d'actif ou de composant (AWS CLI).

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

2. Exécutez la commande suivante pour trouver `actionDefinitionId` l'`Inference`action. Remplacez *`asset-model-id`*par l'ID utilisé à l'étape précédente et remplacez *`asset-model-composite-model-id`*par l'ID renvoyé à l'étape précédente.

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

3. Créez un fichier appelé `start-inference.json` et ajoutez-y le code suivant, en remplaçant le suivant :

   - *`asset-id`*avec l'ID de l'actif cible
   - *`action-definition-id`*avec l'ID de l'action d'inférence de départ
   - *`Offset`*avec la quantité de mémoire tampon à utiliser
   - *`Frequency`*avec la fréquence à laquelle les données sont téléchargées

   ```
   {
     "targetResource": {
       "assetId": "asset-id"
   ```

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

4. Exécutez la commande suivante pour démarrer l'inférence :

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

Pour arrêter l'inférence

1. Exécutez la commande suivante pour trouver le `assetModelCompositeModelId` dessous`assetModelCompositeModelSummaries`. *`asset-model-id`*Remplacez-le par l'ID du modèle d'actif que vous avez créé dansMettre à jour un modèle d'actif ou de composant (AWS CLI).

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

2. Exécutez la commande suivante pour trouver `actionDefinitionId` l'`Inference`action. Remplacez *`asset-model-id`*par l'ID utilisé à l'étape précédente et remplacez *`asset-model-composite-model-id`*par l'ID renvoyé à l'étape précédente.

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

3. Créez un fichier appelé `stop-inference.json` et ajoutez-y le code suivant, en remplaçant le suivant :

   - *`asset-id`*avec l'ID de l'actif cible
   - *`action-definition-id`*avec l'ID de l'action d'inférence de départ

```
{
  "targetResource": {
    "assetId": "asset-id"
  },
  "actionDefinitionId": "action-definition-Id",
```

```
  "actionPayload":{ "stringValue": "{\"l4EInference\":{\"inferenceMode\":\"STOP
\"}}"
}}
```

4. Exécutez la commande suivante pour arrêter l'inférence :

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

Gestion du stockage des données

Vous pouvez configurer AWS IoT SiteWise pour enregistrer vos données dans les niveaux de stockage suivants :

Niveau chaud

Le niveau de stockage à chaud est un stockage de séries chronologiques AWS IoT SiteWise géré. Le mode Hot Tier est particulièrement efficace pour les données fréquemment consultées, avec une faible write-to-read latence. Les données stockées dans le hot tier sont utilisées par les applications industrielles qui ont besoin d'un accès rapide aux dernières valeurs de mesure de votre équipement. Cela inclut les applications qui visualisent les métriques en temps réel à l'aide d'un tableau de bord interactif, ou les applications qui surveillent les opérations et lancent des alarmes pour identifier les problèmes de performance.

Par défaut, les données ingérées sont AWS IoT SiteWise stockées dans le hot tier. Vous pouvez définir une période de conservation pour le niveau chaud, après quoi les AWS IoT SiteWise données du niveau chaud sont transférées vers le niveau de stockage chaud ou froid, en fonction de votre configuration. Pour optimiser les performances et la rentabilité, définissez la période de rétention de votre hot tier de manière à ce qu'elle soit plus longue que le temps nécessaire pour récupérer souvent les données. Ceci est utilisé pour les métriques en temps réel, les alarmes et les scénarios de surveillance. Si aucune période de conservation n'est définie, vos données sont stockées indéfiniment dans le hot tier.

Niveau chaud

Le niveau de stockage à chaud est un niveau AWS IoT SiteWise géré efficace pour le stockage rentable des données historiques. Il est préférable de l'utiliser pour récupérer de gros volumes de données présentant des caractéristiques de write-to-read latence moyenne. Utilisez le niveau chaud pour stocker les données historiques nécessaires aux charges de travail importantes. Par exemple, il est utilisé pour la récupération de données pour les analyses, les applications de business intelligence (BI), les outils de reporting et la formation de modèles d'apprentissage automatique (ML). Si vous activez le niveau de stockage à froid, vous pouvez définir une période de rétention du niveau chaud. Une fois la période de conservation terminée, AWS IoT SiteWise les données sont supprimées du niveau chaud.

Niveau froid

Le niveau de stockage à froid utilise un compartiment Amazon S3 pour stocker des données rarement utilisées. Lorsque le niveau froid est activé, AWS IoT SiteWise reproduit les séries

chronologiques, y compris les mesures, les métriques, les transformations et les agrégats, ainsi que les définitions des modèles d'actifs toutes les 6 heures. Le niveau froid est utilisé pour stocker des données qui tolèrent une latence de lecture élevée pour les rapports historiques et les sauvegardes.

Rubriques

- Configuration des paramètres de stockage
- Résoudre les problèmes liés aux paramètres de stockage
- Chemins de fichiers et schémas de données enregistrés dans le niveau froid

Configuration des paramètres de stockage

Vous pouvez configurer les paramètres de stockage pour opter pour le stockage de niveau chaud géré par service et également pour répliquer les données vers le niveau froid. Pour en savoir plus sur la durée de conservation des niveaux chaud et chaud, consultezImpact sur la conservation des données. Lors de la configuration des paramètres de stockage, procédez comme suit :

- Rétention de niveau chaud : définissez une période de conservation pour la durée pendant laquelle vos données sont stockées dans le niveau chaud avant d'être supprimées, puis transférées vers le stockage de niveau chaud ou le stockage de niveau froid géré par le service en fonction de vos paramètres de stockage. AWS IoT SiteWise supprimera toutes les données du hot tier qui existaient avant la fin de la période de conservation. Si vous ne définissez pas de période de conservation, vos données sont stockées indéfiniment dans le hot tier.
- Rétention au niveau chaud : définissez une période de conservation pour la durée pendant laquelle vos données sont stockées dans le niveau chaud avant qu'elles ne soient supprimées du AWS IoT SiteWise stockage et transférées vers le stockage à froid géré par le client. AWS IoT SiteWise supprime toutes les données du niveau chaud qui existaient avant la fin de la période de rétention. Si aucune période de conservation n'est définie, vos données sont stockées indéfiniment dans le niveau chaud.

> **Note**
>
> Pour améliorer les performances des requêtes, définissez une période de rétention de niveau chaud avec un stockage de niveau chaud.

Impact de la conservation des données dans les systèmes de stockage à chaud et à haute température

- Lorsque vous réduisez la durée de conservation du niveau de stockage chaud, les données sont définitivement déplacées du niveau chaud vers le niveau chaud ou froid. Lorsque vous réduisez la durée de conservation du niveau chaud, les données sont déplacées vers le niveau froid et définitivement supprimées du niveau chaud.
- Lorsque vous augmentez la durée de conservation du niveau de stockage chaud ou chaud, la modification affecte les données qui sont ensuite envoyées AWS IoT SiteWise . AWS IoT SiteWise ne récupère pas les données du stockage chaud ou froid pour alimenter le niveau chaud. Par exemple, si la période de conservation du stockage de niveau chaud est initialement fixée à 30 jours, puis portée à 60 jours, il faut 30 jours pour que le stockage de niveau chaud contienne 60 jours de données.

Rubriques

- Configurer les paramètres de stockage pour Warm Tier (console)
- Configurer les paramètres de stockage pour Warm Tier (AWS CLI)
- Configuration des paramètres de stockage pour le niveau froid (console)
- Configurer les paramètres de stockage pour Cold Tier (AWS CLI)

Configurer les paramètres de stockage pour Warm Tier (console)

La procédure suivante explique comment configurer les paramètres de stockage pour répliquer les données vers le niveau chaud de la AWS IoT SiteWise console.

Pour configurer les paramètres de stockage dans la console

1. Accédez à la console AWS IoT SiteWise.
2. Dans le volet de navigation, sous Paramètres, choisissez Stockage.
3. Dans le coin supérieur droit, choisissez Modifier.
4. Sur la page Modifier le stockage, procédez comme suit :
5. Pour les paramètres Hot Tier, procédez comme suit :

    - Si vous souhaitez définir une période de conservation correspondant à la durée pendant laquelle vos données sont stockées dans le niveau chaud avant d'être supprimées et

déplacées vers le stockage à chaud géré par le service, choisissez Activer la période de conservation.

- Pour configurer une période de rétention, entrez un nombre entier et choisissez une unité. La durée de conservation doit être supérieure ou égale à 30 jours.

AWS IoT SiteWise supprime toutes les données du hot tier qui sont antérieures à la période de conservation. Si vous ne définissez pas de période de conservation, vos données sont stockées indéfiniment.

6. (Recommandé) Pour les paramètres du niveau Warm, procédez comme suit :

   - Pour opter pour le stockage à niveau chaud, sélectionnez Je confirme pour activer le stockage à niveau chaud pour opter pour le stockage à niveau chaud.
   - (Facultatif) Pour configurer une période de rétention, entrez un nombre entier et choisissez une unité. La durée de conservation doit être supérieure ou égale à 365 jours.

   AWS IoT SiteWise supprime les données du niveau chaud qui existaient avant la période de rétention. Si vous ne définissez pas de période de conservation, vos données sont stockées indéfiniment.

   > **Note**
   >
   > - Lorsque vous optez pour le niveau chaud, la configuration ne s'affiche qu'une seule fois.
   > - Pour définir le niveau de rétention à chaud, vous devez disposer d'un niveau de stockage à chaud ou à froid. Pour des raisons de rentabilité et de récupération des données historiques, il est AWS IoT SiteWise recommandé de stocker les données à long terme dans le niveau chaud.
   > - Pour définir le niveau de rétention à chaud, vous devez disposer d'un niveau de stockage à froid.

7. Choisissez Enregistrer pour enregistrer vos paramètres de stockage.

Dans la section AWS IoT SiteWise stockage, le stockage de niveau Warm se trouve dans l'un des états suivants :

- Activé : si vos données existaient avant la période de rétention du niveau chaud, AWS IoT SiteWise déplacez-les vers le niveau chaud. »
- Désactivé : le stockage à chaud est désactivé.

Configurer les paramètres de stockage pour Warm Tier (AWS CLI)

Vous pouvez configurer les paramètres de stockage pour déplacer les données vers le niveau chaud à l' AWS CLI aide des commandes suivantes.

Pour éviter de remplacer la configuration existante, récupérez les informations de configuration de stockage actuelles en exécutant la commande suivante :

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

Example réponse sans configuration de niveau froid existante

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

Example réponse avec la configuration de niveau froid existante

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

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

Configurez les paramètres de stockage pour le niveau chaud avec AWS CLI

Exécutez la commande suivante pour configurer les paramètres de stockage. Remplacez `file-name` par le nom du fichier contenant la configuration AWS IoT SiteWise de stockage.

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

Example AWS IoT SiteWise configuration avec niveau chaud et niveau chaud

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

}
```

`hot-tier-retention-in-days`doit être un nombre entier supérieur ou égal à 30 jours.

Example réponse

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

Si le stockage à froid est activé, consultezConfiguration des paramètres de stockage avec un AWS CLI niveau froid existant.

Configuration des paramètres de stockage avec un AWS CLI niveau froid existant

Configuration des paramètres de stockage à l' AWS CLI aide du stockage à froid existant

- Exécutez la commande suivante pour configurer les paramètres de stockage. Remplacez *file-name* par le nom du fichier contenant la configuration de AWS IoT SiteWise stockage.

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

Example AWS IoT SiteWise configuration de stockage

- Remplacez *le nom du compartiment par le nom* de votre compartiment Amazon S3.
- Remplacez le *préfixe* par votre préfixe Amazon S3.
- Remplacez *aws-account-id*par votre identifiant de AWS compte.
- Remplacez *role-name* par le nom du rôle d'accès Amazon S3 qui permet d'envoyer des données AWS IoT SiteWise à Amazon S3.
- Remplacez *hot-tier-retention-in-days* par un nombre entier supérieur ou égal à 30 jours.
- Remplacez *warm-tier-retention-in-days* par un nombre entier supérieur ou égal à 365 jours.

> **Note**
>
> AWS IoT SiteWise supprimera toutes les données du niveau chaud qui sont antérieures à la période de conservation du niveau froid. Si vous ne définissez pas de période de conservation, vos données sont stockées indéfiniment.

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

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

Example réponse

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

Configuration des paramètres de stockage pour le niveau froid (console)

La procédure suivante explique comment configurer les paramètres de stockage pour répliquer les données vers le niveau froid de la AWS IoT SiteWise console.

Pour configurer les paramètres de stockage dans la console

1. Accédez à la console AWS IoT SiteWise.
2. Dans le volet de navigation, sous Paramètres, choisissez Stockage.
3. Dans le coin supérieur droit, choisissez Modifier.
4. Sur la page Modifier le stockage, procédez comme suit :

    a. Pour les paramètres de stockage, choisissez Activer le stockage à froid. Le stockage à froid est désactivé par défaut.

    b. Pour l'emplacement du compartiment S3, entrez le nom d'un compartiment Amazon S3 existant et un préfixe.

> **Note**
>
> - Amazon S3 utilise le préfixe comme nom de dossier dans le compartiment Amazon S3. Le préfixe doit comporter de 1 à 255 caractères et se terminer par une barre oblique (/). Vos AWS IoT SiteWise données sont enregistrées dans ce dossier.
> - Si vous n'avez pas de compartiment Amazon S3, choisissez View, puis créez-en un dans la console Amazon S3. Pour plus d'informations, consultez Créer votre premier compartiment S3 dans le guide de l'utilisateur Amazon S3.

c. Pour le rôle d'accès S3, effectuez l'une des opérations suivantes :

- Choisissez Create a role from an AWS managed template, puis créez AWS automatiquement un rôle IAM qui permet d' AWS IoT SiteWise envoyer des données à Amazon S3.
- Choisissez Utiliser un rôle existant, puis choisissez le rôle que vous avez créé dans la liste.

> **Note**
>
> - Vous devez utiliser le même nom de compartiment Amazon S3 pour l'emplacement du compartiment S3 que celui que vous avez utilisé à l'étape précédente et dans votre politique IAM.
> - Assurez-vous que votre rôle dispose des autorisations indiquées dans l'exemple suivant.
>
>   Example politique d'autorisations :
>
> ```
> {
>       "Version": "2012-10-17",
>       "Statement": [
>           {
>               "Effect": "Allow",
>               "Action": [
>                   "s3:PutObject",
>                   "s3:GetObject",
>                   "s3:DeleteObject",
>                   "s3:GetBucketLocation",
> ```

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

Remplacez *bucket-name* par le nom de votre compartiment Amazon S3.

d. Pour configurer le hot tier, reportez-vous à l'étape 5 de[Configurer les paramètres de stockage pour Warm Tier (console)](#).

e. (Facultatif) Pour AWS IoT Analytics l'intégration, procédez comme suit.

   i. Si vous souhaitez l'utiliser AWS IoT Analytics pour interroger vos données, choisissez Enabled AWS IoT Analytics data store.

   ii. AWS IoT SiteWise génère un nom pour votre banque de données ou vous pouvez saisir un autre nom.

   AWS IoT SiteWise crée automatiquement un magasin de données AWS IoT Analytics pour enregistrer vos données. Pour interroger les données, vous pouvez AWS IoT Analytics créer des ensembles de données. Pour plus d'informations, consultez la section [Utilisation des AWS IoT SiteWise données](#) dans le Guide de AWS IoT Analytics l'utilisateur.

f. Choisissez Enregistrer.

Dans la section AWS IoT SiteWise stockage, le stockage à froid peut prendre l'une des valeurs suivantes :

- Activé : AWS IoT SiteWise réplique vos données dans le compartiment Amazon S3 spécifié.
- Activation : AWS IoT SiteWise traite votre demande pour activer le stockage à froid. Ce processus peut prendre plusieurs minutes.
- Enable_Failed : AWS IoT SiteWise impossible de traiter votre demande d'activation du stockage à froid. Si vous avez activé AWS IoT SiteWise l'envoi de journaux vers Amazon CloudWatch Logs, vous pouvez utiliser ces journaux pour résoudre les problèmes. Pour plus d'informations, consultez [Surveillance avec Amazon CloudWatch Logs](#).

- Désactivé : le stockage à froid est désactivé.

Configurer les paramètres de stockage pour Cold Tier (AWS CLI)

La procédure suivante explique comment configurer les paramètres de stockage pour répliquer les données vers le niveau froid à l'aide AWS CLI de.

Pour configurer les paramètres de stockage à l'aide de AWS CLI

1. Pour exporter des données vers un compartiment Amazon S3 de votre compte, exécutez la commande suivante pour configurer les paramètres de stockage. Remplacez *file-name* par le nom du fichier contenant la configuration de AWS IoT SiteWise stockage.

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

   Example AWS IoT SiteWise configuration de stockage

   - Remplacez *le nom du compartiment par le nom* de votre compartiment Amazon S3.
   - Remplacez le *préfixe* par votre préfixe Amazon S3.
   - Remplacez *aws-account-id*par votre identifiant de AWS compte.
   - Remplacez *role-name* par le nom du rôle d'accès Amazon S3 qui permet d'envoyer des données AWS IoT SiteWise à Amazon S3.
   - Remplacez *retention-in-days*par un nombre entier supérieur ou égal à 30 jours.

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

Note

- Vous devez utiliser le même nom de compartiment Amazon S3 dans la configuration de AWS IoT SiteWise stockage et dans la politique IAM.
- Assurez-vous que votre rôle dispose des autorisations indiquées dans l'exemple suivant.

  Example politique d'autorisations :

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

  Remplacez *bucket-name* par le nom de votre compartiment Amazon S3.

Example réponse

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

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

> **Note**
>
> La mise à jour de la configuration AWS IoT SiteWise de stockage peut prendre quelques minutes.

2. Pour récupérer les informations de configuration du stockage, exécutez la commande suivante.

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

Example réponse

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

3. Pour arrêter d'exporter des données vers le compartiment Amazon S3, exécutez la commande suivante pour configurer les paramètres de stockage.

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

> **Note**
>
> Par défaut, vos données ne sont stockées que dans le niveau chaud de AWS IoT SiteWise.

Example réponse

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

4. Pour récupérer les informations de configuration du stockage, exécutez la commande suivante.

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

Example réponse

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

(Facultatif) Créez un magasin de AWS IoT Analytics données (AWS CLI)

Un magasin de AWS IoT Analytics données est un référentiel évolutif et interrogeable qui reçoit et stocke des données. Vous pouvez utiliser la AWS IoT SiteWise console ou les AWS IoT Analytics API pour créer un magasin de AWS IoT Analytics données afin de sauvegarder vos AWS IoT SiteWise données. Pour interroger les données, vous créez des ensembles de données à l'aide AWS IoT Analytics de. Pour plus d'informations, consultez la section Utilisation des AWS IoT SiteWise données dans le Guide de AWS IoT Analytics l'utilisateur.

Les étapes suivantes permettent AWS CLI de créer un magasin de données dans AWS IoT Analytics.

Pour créer un magasin de données, exécutez la commande suivante. Remplacez *file-name* par le nom du fichier contenant la configuration du magasin de données.

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

> **Note**
>
> - Vous devez spécifier le nom d'un compartiment Amazon S3 existant. Si vous n'avez pas de compartiment Amazon S3, créez-en un d'abord. Pour plus d'informations, consultez Créer votre premier compartiment S3 dans le guide de l'utilisateur Amazon S3.
> - Vous devez utiliser le même nom de compartiment Amazon S3 dans la configuration du AWS IoT SiteWise stockage, la politique IAM et la configuration du magasin de AWS IoT Analytics données.

Example AWS IoT Analytics configuration du magasin de données

Remplacez *data-store-name*et *s3-bucket-name par le nom* de votre banque de AWS IoT Analytics données et le nom du compartiment Amazon S3.

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

Example réponse

```
{
      "datastoreName": "datastore_IoTSiteWise_demo",
```

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

Résoudre les problèmes liés aux paramètres de stockage

Utilisez les informations suivantes pour résoudre les problèmes liés à la configuration du stockage.

Problèmes

- Erreur : le compartiment n'existe pas
- Erreur : accès refusé au chemin Amazon S3
- Erreur : l'ARN du rôle ne peut pas être assumé
- Erreur : Impossible d'accéder au compartiment Amazon S3 interrégional

Erreur : le compartiment n'existe pas

Solution : AWS IoT SiteWise impossible de trouver votre compartiment Amazon S3. Assurez-vous de saisir le nom d'un compartiment Amazon S3 existant dans la région actuelle.

Erreur : accès refusé au chemin Amazon S3

Solution : AWS IoT SiteWise impossible d'accéder à votre compartiment Amazon S3. Procédez comme suit :

- Assurez-vous d'utiliser le même compartiment Amazon S3 que celui que vous avez spécifié dans la politique IAM.
- Assurez-vous que votre rôle dispose des autorisations indiquées dans l'exemple suivant.

  Example stratégie d'autorisation

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

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

Remplacez *bucket-name* par le nom de votre compartiment Amazon S3.

Erreur : l'ARN du rôle ne peut pas être assumé

Solution : AWS IoT SiteWise je n'ai pas pu assumer le rôle IAM en votre nom. Assurez-vous que votre rôle fait confiance au service suivant :`iotsitewise.amazonaws.com`. Pour plus d'informations, voir Je ne peux pas assumer un rôle, voir le guide de l'utilisateur IAM.

Erreur : Impossible d'accéder au compartiment Amazon S3 interrégional

Solution : Le compartiment Amazon S3 que vous avez spécifié se trouve dans une autre AWS région. Assurez-vous que votre compartiment Amazon S3 et vos AWS IoT SiteWise actifs se trouvent dans la même région.

Chemins de fichiers et schémas de données enregistrés dans le niveau froid

AWS IoT SiteWise stocke vos données dans la couche froide en répliquant des séries chronologiques, notamment des mesures, des métriques, des transformations et des agrégats, ainsi que des définitions d'actifs et de modèles d'actifs. Ce qui suit décrit les chemins de fichiers et les schémas de données envoyés au niveau froid.

Rubriques

- Données relatives à l'équipement (mesures)

- Métriques, transformations et agrégats
- Métadonnées relatives aux actifs
- Métadonnées de hiérarchie des actifs
- Fichiers d'index des données de stockage

Données relatives à l'équipement (mesures)

AWS IoT SiteWise exporte les données de l'équipement (mesures) vers le niveau froid une fois toutes les six heures. Les données brutes sont enregistrées dans le niveau froid au format Apache AVRO (`.avro`).

Chemin d'accès du fichier

AWS IoT SiteWise stocke les données de l'équipement (mesures) dans le niveau froid à l'aide du modèle suivant.

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

Chaque chemin de fichier vers les données brutes dans Amazon S3 contient les composants suivants.

Composant Path	Description
`keyPrefix`	Le préfixe Amazon S3 que vous avez spécifié dans la configuration AWS IoT SiteWise de stockage. Amazon S3 utilise le préfixe comme nom de dossier dans le compartiment.
`raw`	Le dossier qui stocke les séries chronologiques des équipements (mesures). Le `raw` dossier est enregistré dans le dossier des préfixes.
`seriesBucket`	Nombre hexadécimal compris entre 00 et ff. Ce numéro est dérivé `detimeSeriesId` . Cette partition est utilisée pour augmenter le débit lors des AWS IoT SiteWise écritures sur

Composant Path	Description
	le niveau froid. Lorsque vous utilisez Amazon Athena pour exécuter des requêtes, vous pouvez utiliser la partition pour un partition nement précis afin d'améliorer les performan ces des requêtes. `seriesBucket` et `timeSeriesBucket` dans les métadonnées des actifs figurent le même numéro.
`startYear`	L'année de l'heure de début exclusive associée aux données de la série chronologique.
`startMonth`	Le mois de l'heure de début exclusive associée aux données de la série chronologique.
`startDay`	Le jour du mois de l'heure de début exclusive associée aux données de la série chronolog ique.

Composant Path	Description
`fileName`	Le nom du fichier utilise le trait de soulignem ent (_) comme séparateur pour séparer les éléments suivants : • Le `raw` préfixe. • La `timeSeriesId` valeur. • L'horodatage de l'heure de début exclusive associée aux données de la série chronolog ique. • La qualité des données. Valeurs valides : `GOODBAD`, et`UNCERTAIN` . Pour plus d'informations, consultez AssetPropertyla section Valeur dans la référence de AWS IoT SiteWise l'API. Le fichier est enregistré au `.avro` format à l'aide de la compression Snappy.

Example chemin du fichier vers les données brutes dans le niveau froid

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

Champs

Le schéma des données brutes exportées vers le niveau froid contient les champs suivants.

Nom de champ	Types pris en charge	Type par défaut	Description
`seriesId`	`string`	N/A	L'identifiant qui identifie les séries chronologiques de l'équipement

Nom de champ	Types pris en charge	Type par défaut	Description
			(mesures). Vous pouvez utiliser ce champ pour joindre des données brutes et des métadonnées d'actifs dans des requêtes.
`timeInSeconds`	`long`	N/A	Date d'horodatage, en secondes, au format Unix Epoch. Les données de nanosecondes fractionnaires sont fournies par. `offsetInNanos`
`offsetInNanos`	`long`	N/A	Le décalage de nanosecondes par rapport à. `timeInSeconds`
`quality`	`string`	N/A	Qualité de la valeur de la série chronologique.
`doubleValue`	`double` ou `null`	`null`	Données de séries chronologiques de type double (nombre à virgule flottante).
`stringValue`	`string` ou `null`	`null`	Données de séries chronologiques de type chaîne (séquence de caractères).

Nom de champ	Types pris en charge	Type par défaut	Description
`integerValue`	`int` ou `null`	`null`	Données de séries chronologiques de type entier (nombre entier).
`booleanValue`	`boolean` ou `null`	`null`	Données de séries chronologiques de type booléen (vrai ou faux).
`jsonValue`	`string` ou `null`	`null`	Données de séries chronologiques de type JSON (types de données complexes stockés sous forme de chaîne).
`recordVersion`	`long` ou `null`	`null`	Le numéro de version de l'enregistrement. Vous pouvez utiliser le numéro de version pour sélectionner le dernier enregistr ement. Les nouveaux enregistrements ont des numéros de version plus grands.

Example données brutes dans la couche froide

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

```
  {"seriesId":"e9687d2a-0dbe-4f65-9ed6-6f443cba41f7_95e63da7-d34e-43e1-
bc6f-1b490154b07a","timeInSeconds":1625675890,"offsetInNanos":0,"quality":"GOOD","doubleValue":
{"double":0.66},"stringValue":null,"integerValue":null,"booleanValue":null,"jsonValue":null,"re
  {"seriesId":"e9687d2a-0dbe-4f65-9ed6-6f443cba41f7_95e63da7-d34e-43e1-
bc6f-1b490154b07a","timeInSeconds":1625675891,"offsetInNanos":0,"quality":"GOOD","doubleValue":
{"double":0.92},"stringValue":null,"integerValue":null,"booleanValue":null,"jsonValue":null,"re
  {"seriesId":"e9687d2a-0dbe-4f65-9ed6-6f443cba41f7_95e63da7-d34e-43e1-
bc6f-1b490154b07a","timeInSeconds":1625675892,"offsetInNanos":0,"quality":"GOOD","doubleValue":
{"double":0.73},"stringValue":null,"integerValue":null,"booleanValue":null,"jsonValue":null,"re
```


Métriques, transformations et agrégats

AWS IoT SiteWise exporte les métriques, les transformations et les agrège vers le niveau froid une fois toutes les six heures. Les métriques, les transformations et les agrégats sont enregistrés dans le niveau froid au format Apache AVRO (`.avro`).

Chemin d'accès du fichier

AWS IoT SiteWise stocke les métriques, les transformations et les agrégats dans le niveau froid à l'aide du modèle suivant.

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

Chaque chemin de fichier vers les métriques, les transformations et les agrégats dans Amazon S3 contient les composants suivants.

Composant Path	Description
`keyPrefix`	Le préfixe Amazon S3 que vous avez spécifié dans la configuration AWS IoT SiteWise de stockage. Amazon S3 utilise le préfixe comme nom de dossier dans le compartiment.
`agg`	Le dossier qui stocke les données de séries chronologiques issues des métriques. Le `agg` dossier est enregistré dans le dossier des préfixes.

Composant Path	Description
`seriesBucket`	Nombre hexadécimal compris entre 00 et ff. Ce numéro est dérivé de `timeSeriesId` . Cette partition est utilisée pour augmenter le débit lors des AWS IoT SiteWise écritures sur le niveau froid. Lorsque vous utilisez Amazon Athena pour exécuter des requêtes, vous pouvez utiliser la partition pour un partition nement précis afin d'améliorer les performan ces des requêtes. `seriesBucket` et `timeSeriesBucket` dans les métadonnées des actifs figurent le même numéro.
`startYear`	L'année de l'heure de début exclusive associée aux données de la série chronologique.
`startMonth`	Le mois de l'heure de début exclusive associée aux données de la série chronologique.
`startDay`	Le jour du mois de l'heure de début exclusive associée aux données de la série chronolog ique.

Composant Path	Description
`fileName`	Le nom du fichier utilise le trait de soulignem ent (_) comme séparateur pour séparer les éléments suivants : • Le `raw` préfixe. • La `timeSeriesId` valeur. • L'horodatage de l'heure de début exclusive associée aux données de la série chronolog ique. • La qualité des données. Valeurs valides : `GOODBAD`, et`UNCERTAIN` . Pour plus d'informations, consultez AssetPropertyla section Valeur dans la référence de AWS IoT SiteWise l'API. Le fichier est enregistré au `.avro` format à l'aide de la compression Snappy.

Example chemin du fichier vers les métriques dans le niveau froid

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

Champs

Le schéma des métriques, des transformations et des agrégats exportés vers le niveau froid contient les champs suivants.

Nom de champ	Types pris en charge	Type par défaut	Description
`seriesId`	`string`	N/A	L'identifiant qui identifie les séries chronologiques issues

Nom de champ	Types pris en charge	Type par défaut	Description
			de l'équipement, des métriques ou des transformations. Vous pouvez utiliser ce champ pour joindre des données brutes et des métadonné es d'actifs dans des requêtes.
`timeInSeconds`	`long`	N/A	Date d'horodat age, en secondes, au format Unix Epoch. Les données de nanosecon des fractionnaires sont fournies par. `offsetInNanos`
`offsetInNanos`	`long`	N/A	Le décalage de nanosecondes par rapport à. `timeInSec onds`
`quality`	`string`	N/A	La qualité selon laquelle les données relatives aux actifs doivent être filtrées.
`resolution`	`string`	N/A	Intervalle de temps pendant lequel les données doivent être agrégées.

Nom de champ	Types pris en charge	Type par défaut	Description
`count`	`double` ou `null`	`null`	Le nombre total de points de données pour les variables données sur l'interva lle de temps actuel.
`average`	`double` ou `null`	`null`	La moyenne des valeurs des variables données sur l'interva lle de temps actuel.
`min`	`double` ou `null`	`null`	Le minimum des valeurs des variables données sur l'interva lle de temps actuel.
`max`	`boolean` ou `null`	`null`	Le maximum des valeurs des variables données sur l'interva lle de temps actuel.
`sum`	`string` ou `null`	`null`	Somme des valeurs des variables données sur l'interva lle de temps actuel.
`recordVersion`	`long` ou `null`	`null`	Le numéro de version de l'enregistrement. Vous pouvez utiliser le numéro de version pour sélectionner le dernier enregistr ement. Les nouveaux enregistrements ont des numéros de version plus grands.

Example Données métriques dans la couche froide

```
{"seriesId":"f74c2828-5317-4df3-
ba16-6d41b5bcb531","timeInSeconds":1637334060,"offsetInNanos":0,"quality":"GOOD","resolution":"
{"double":16.0},"min":{"double":1.0},"max":{"double":31.0},"sum":
{"double":496.0},"recordVersion":null}
  {"seriesId":"f74c2828-5317-4df3-
ba16-6d41b5bcb531","timeInSeconds":1637334120,"offsetInNanos":0,"quality":"GOOD","resolution":"
{"double":46.0},"min":{"double":32.0},"max":{"double":60.0},"sum":
{"double":1334.0},"recordVersion":null}
  {"seriesId":"f74c2828-5317-4df3-
ba16-6d41b5bcb531","timeInSeconds":1637334540,"offsetInNanos":0,"quality":"GOOD","resolution":"
{"double":16.0},"min":{"double":1.0},"max":{"double":31.0},"sum":
{"double":496.0},"recordVersion":null}
  {"seriesId":"f74c2828-5317-4df3-
ba16-6d41b5bcb531","timeInSeconds":1637334600,"offsetInNanos":0,"quality":"GOOD","resolution":"
{"double":46.0},"min":{"double":32.0},"max":{"double":60.0},"sum":
{"double":1334.0},"recordVersion":null}
  {"seriesId":"f74c2828-5317-4df3-
ba16-6d41b5bcb531","timeInSeconds":1637335020,"offsetInNanos":0,"quality":"GOOD","resolution":"
{"double":16.0},"min":{"double":1.0},"max":{"double":31.0},"sum":
{"double":496.0},"recordVersion":null}
```

Métadonnées relatives aux actifs

Lorsque vous activez l'exportation de données AWS IoT SiteWise vers le niveau froid pour la première fois, les métadonnées des actifs sont exportées vers le niveau froid. Après la configuration initiale, AWS IoT SiteWise exporte les métadonnées des actifs vers le niveau uniquement lorsque vous modifiez les définitions des modèles d'actifs ou les définitions des actifs. Les métadonnées des actifs sont enregistrées dans le niveau froid au format JSON (`.ndjson`) délimité par une nouvelle ligne.

Chemin d'accès du fichier

AWS IoT SiteWise stocke les métadonnées des actifs dans le niveau froid à l'aide du modèle suivant.

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

Chaque chemin de fichier vers les métadonnées des actifs dans le niveau froid contient les composants suivants.

Composant Path	Description
`keyPrefix`	Le préfixe Amazon S3 que vous avez spécifié dans la configuration de stockage AWS IoT SiteWise s. Amazon S3 utilise le préfixe comme nom de dossier dans le compartiment.
`asset_metadata`	Le dossier qui stocke les métadonnées des actifs. Le `asset_metadata` dossier est enregistré dans le dossier des préfixes.
`fileName`	Le nom du fichier utilise le trait de soulignem ent (_) comme séparateur pour séparer les éléments suivants : • Le `asset` préfixe. • La `assetId` valeur. Le fichier est enregistré au `.ndjson` format.

Example chemin du fichier vers les métadonnées des actifs dans le niveau le plus froid

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

Champs

Le schéma des métadonnées des actifs exportées vers le niveau froid contient les champs suivants.

Nom de champ	Description
`assetId`	ID de la ressource .
`assetName`	Le nom de l'actif.
`assetExternalId`	L'ID externe de la ressource.
`assetModelId`	ID du modèle d'actif utilisé pour créer cet actif.

Nom de champ	Description
`assetModelName`	Nom du modèle d'actif.
`assetModelExternalId`	ID externe du modèle d'actif.
`assetPropertyId`	ID de la propriété de ressource.
`assetPropertyName`	Le nom de la propriété de l'actif.
`assetPropertyExternalId`	ID externe de la propriété de l'actif.
`assetPropertyDataType`	Type de données de la propriété de l'actif.
`assetPropertyUnit`	Unité de la propriété de l'actif (par exemple, `Newtons` et`RPM`).
`assetPropertyAlias`	Alias qui identifie la propriété de l'actif, tel qu'un chemin de flux de données du serveur OPC-UA (par exemple,`/company/windfarm/3/turbine/7/temperature`).
`timeSeriesId`	L'identifiant qui identifie les séries chronologiques issues de l'équipement, des métriques ou des transformations. Vous pouvez utiliser ce champ pour joindre des données brutes et des métadonnées d'actifs dans des requêtes.

Nom de champ	Description
`timeSeriesBucket`	Nombre hexadécimal compris entre 00 et ff. Ce numéro est dérivé de `timeSeriesId` . Cette partition est utilisée pour augmenter le débit lors des AWS IoT SiteWise écritures sur le niveau froid. Lorsque vous utilisez Amazon Athena pour exécuter des requêtes, vous pouvez utiliser la partition pour un partition nement précis afin d'améliorer les performan ces des requêtes. `timeSeriesBucket` et `seriesBucket` le chemin du fichier vers les données brutes contient le même numéro.
`assetCompositeModelId`	ID du modèle composite.
`assetCompositeModelExternalId`	ID externe du modèle composite.
`assetCompositeModelDescription`	Description du modèle composite.
`assetCompositeModelName`	Nom du modèle composite.
`assetCompositeModelType`	Type du modèle composite. Pour les modèles composites d'alarme, ce type est `AWS/ALARM` .
`assetCreationDate`	Date de création de la ressource, à l'époque Unix.
`assetLastUpdateDate`	Date à laquelle la ressource a été mise à jour pour la dernière fois, à l'époque Unix.
`assetStatusErrorCode`	Code de l'erreur.
`assetStatusErrorMessage`	Message d'erreur.
`assetStatusState`	État actuel de l'actif.

Example métadonnées des actifs dans le niveau froid


```
  {"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
```


Métadonnées de hiérarchie des actifs

Lorsque vous activez AWS IoT SiteWise l'enregistrement des données dans le niveau froid pour la première fois, les métadonnées de la hiérarchie des actifs sont exportées vers le niveau froid. Après la configuration initiale, AWS IoT SiteWise exporte les métadonnées de la hiérarchie des actifs

vers le niveau froid uniquement lorsque vous modifiez le modèle d'actif ou les définitions des actifs. Les métadonnées de la hiérarchie des actifs sont enregistrées dans le niveau froid au format JSON (`.ndjson`) délimité par une nouvelle ligne.

Un identifiant externe pour la hiérarchie, la ressource cible ou la ressource source est récupéré en appelant l'DescribeAssetAPI.

Chemin d'accès du fichier

AWS IoT SiteWise stocke les métadonnées de la hiérarchie des actifs dans le niveau froid à l'aide du modèle suivant.

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

Chaque chemin de fichier vers les métadonnées de la hiérarchie des actifs dans le niveau froid contient les composants suivants.

Composant Path	Description
`keyPrefix`	Le préfixe Amazon S3 que vous avez spécifié dans la configuration AWS IoT SiteWise de stockage. Amazon S3 utilise le préfixe comme nom de dossier dans le compartiment.
`asset_hierarchy_metadata`	Le dossier qui stocke les métadonnées de la hiérarchie des actifs. Le `asset_hierarchy_metadata` dossier est enregistré dans le dossier des préfixes.
`fileName`	Le nom du fichier utilise le trait de soulignement (_) comme séparateur pour séparer les éléments suivants : • La `parentAssetId` valeur. • La `hierarchyId` valeur. Le fichier est enregistré au `.ndjson` format.

Example chemin du fichier vers les métadonnées de la hiérarchie des actifs dans le niveau froid

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

Champs

Le schéma des métadonnées de hiérarchie des actifs exportées vers le niveau froid contient les champs suivants.

Nom de champ	Description
`sourceAssetId`	L'ID de l'actif source dans cette relation d'actif.
`targetAssetId`	L'ID de l'actif cible dans cette relation d'actif.
`hierarchyId`	ID de la hiérarchie.
`associationType`	Type d'association de cette relation patrimoniale. La valeur doit êtreCHILD. L'actif cible est un actif enfant de l'actif source.

Example métadonnées de hiérarchie des actifs dans le niveau froid

```
{"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"}
```

Pour consulter vos données dans le cadre de la couche froide

1. Accédez à la console Amazon S3.
2. Dans le volet de navigation, choisissez Buckets, puis choisissez votre compartiment Amazon S3.

3. Accédez au dossier contenant les données brutes, les métadonnées des actifs ou les métadonnées de la hiérarchie des actifs.
4. Sélectionnez les fichiers, puis dans Actions, choisissez Télécharger.

Fichiers d'index des données de stockage

AWS IoT SiteWise utilise ces fichiers pour optimiser les performances des requêtes de données. Ils apparaissent dans votre compartiment Amazon S3, mais vous n'avez pas besoin de les utiliser.

Chemin d'accès du fichier

AWS IoT SiteWise stocke les fichiers d'index de données dans le niveau froid en utilisant le modèle suivant.

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

Example chemin du fichier vers le fichier d'index de stockage des données

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

Sécurité dans AWS IoT SiteWise

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le AWS cadre des programmes de de). Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS IoT SiteWise, consultez la section AWS services concernés par programme de conformité et .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de son utilisation AWS IoT SiteWise. Les rubriques suivantes expliquent comment procéder à la configuration AWS IoT SiteWise pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos AWS IoT SiteWise ressources.

Rubriques

- Protection des données dans AWS IoT SiteWise
- Chiffrement des données
- Gestion des identités et des accès pour AWS IoT SiteWise
- Validation de conformité pour AWS IoT SiteWise
- Résilience dans AWS IoT SiteWise
- Sécurité de l'infrastructure dans AWS IoT SiteWise
- Analyse de la configuration et des vulnérabilités
- Points de terminaison d'un VPC
- Bonnes pratiques de sécurité pour AWS IoT SiteWise

Protection des données dans AWS IoT SiteWise

Le modèle de responsabilité AWS partagée de s'applique à la protection des données dans AWS IoT SiteWise. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec AWS IoT SiteWise ou d'autres Services AWS utilisateurs de la console, de l'API ou AWS des SDK. AWS CLI Toutes les données

que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Rubriques

- Confidentialité du trafic inter-réseau

Confidentialité du trafic inter-réseau

Les connexions entre les applications locales AWS IoT SiteWise et entre elles, telles que les passerelles SiteWise Edge, sont sécurisées par le biais de connexions TLS (Transport Layer Security). Pour plus d'informations, consultez Chiffrement en transit.

AWS IoT SiteWise ne prend pas en charge les connexions entre les zones de disponibilité d'une AWS région ni les connexions entre AWS comptes.

Vous ne pouvez configurer IAM Identity Center que dans une seule région à la fois. SiteWise Monitor se connecte à la région que vous avez configurée pour IAM Identity Center. Cela signifie que vous utilisez une région pour accéder à l'IAM Identity Center, mais que vous pouvez créer des portails dans n'importe quelle région.

Chiffrement des données

Le chiffrement des données fait référence à la protection des données en transit (lorsqu'elles voyagent vers et depuis AWS IoT SiteWise, et entre les passerelles SiteWise Edge et les serveurs) et au repos (lorsqu'elles sont stockées sur des appareils locaux ou dans AWS des services). Vous pouvez protéger les données en transit à l'aide du protocole TLS (Transport Layer Security) ou au repos à l'aide du chiffrement côté client.

> **Note**
>
> AWS IoT SiteWise le traitement Edge expose les API hébergées sur les passerelles SiteWise Edge et accessibles via le réseau local. Ces API sont exposées via une connexion TLS soutenue par un certificat de serveur appartenant au AWS IoT SiteWise connecteur Edge. Pour l'authentification du client, ces API utilisent un mot de passe de contrôle d'accès. La clé privée du certificat de serveur et le mot de passe de contrôle d'accès sont tous deux

stockés sur disque. AWS IoT SiteWise le traitement périphérique repose sur le chiffrement du système de fichiers pour la sécurité de ces informations d'identification au repos.

Pour plus d'informations sur le chiffrement côté serveur et le chiffrement côté client, consultez les rubriques ci-dessous.

Rubriques

- Chiffrement au repos
- Chiffrement en transit
- Gestion des clés

Chiffrement au repos

AWS IoT SiteWise stocke vos données dans le AWS cloud et sur des passerelles AWS IoT SiteWise Edge.

Données au repos dans le AWS cloud

AWS IoT SiteWise stocke les données dans d'autres AWS services qui chiffrent les données au repos par défaut. Encryption at rest s'intègre à AWS Key Management Service (AWS KMS) pour gérer la clé de chiffrement utilisée pour chiffrer les valeurs des propriétés de vos actifs et les valeurs agrégées dans AWS IoT SiteWise. Vous pouvez choisir d'utiliser une clé gérée par le client pour chiffrer les valeurs des propriétés des actifs et les valeurs agrégées dans AWS IoT SiteWise. Vous pouvez créer, gérer et consulter votre clé de chiffrement via AWS KMS.

Vous pouvez choisir une clé Clé détenue par AWS pour chiffrer vos données ou une clé gérée par le client pour chiffrer les valeurs des propriétés et les valeurs agrégées de vos actifs :

Comment ça marche

Le chiffrement au repos s'intègre AWS KMS à la gestion de la clé de chiffrement utilisée pour chiffrer vos données.

- Clé détenue par AWS — Clé de chiffrement par défaut. AWS IoT SiteWise possède cette clé. Vous ne pouvez pas voir cette clé dans votre AWS compte. Vous ne pouvez pas non plus voir les opérations effectuées sur la clé dans AWS CloudTrail les journaux. Vous pouvez utiliser cette clé sans frais supplémentaires.

- Clé gérée par le client — La clé est stockée dans votre compte, que vous créez, détenez et gérez. Vous avez le contrôle total de la clé KMS. Des AWS KMS frais supplémentaires s'appliquent.

Clés détenues par AWS

Clés détenues par AWS ne sont pas enregistrés dans votre compte. Elles font partie d'un ensemble de clés KMS qui AWS possède et gère pour une utilisation dans plusieurs AWS comptes. AWS services que vous pouvez Clés détenues par AWS utiliser pour protéger vos données.

Vous ne pouvez pas afficher, gérer Clés détenues par AWS, utiliser ou auditer leur utilisation. Cependant, vous n'avez pas besoin de travailler ou de modifier de programme pour protéger les clés qui chiffrent vos données.

Aucuns frais mensuels ni frais d'utilisation ne vous sont facturés si vous en utilisez Clés détenues par AWS, et ils ne sont pas pris en compte dans les AWS KMS quotas de votre compte.

Clés gérées par le client

Les clés gérées par le client sont des clés KMS de votre compte que vous créez, possédez et gérez. Vous avez le contrôle total de ces clés KMS, telles que les suivantes :

- Établir et maintenir leurs politiques clés, leurs politiques IAM et leurs subventions
- Les activer et les désactiver
- Rotation de leur matériel cryptographique
- Ajout de balises
- Création d'alias qui y font référence
- Planifier leur suppression

Vous pouvez également utiliser CloudTrail Amazon CloudWatch Logs pour suivre les demandes AWS IoT SiteWise envoyées AWS KMS en votre nom.

Si vous utilisez des clés gérées par le client, vous devez autoriser l' AWS IoT SiteWise accès à la clé KMS enregistrée dans votre compte. AWS IoT SiteWise utilise le chiffrement des enveloppes et la hiérarchie des clés pour chiffrer les données. Votre clé de AWS KMS chiffrement est utilisée pour chiffrer la clé racine de cette hiérarchie de clés. Pour plus d'informations, consultez Chiffrement d'enveloppe dans le Guide du développeur AWS Key Management Service .

L'exemple de politique suivant accorde des AWS IoT SiteWise autorisations pour créer une clé gérée par le client en votre nom. Lorsque vous créez votre clé, vous devez autoriser les `kms:DescribeKey` actions `kms:CreateGrant` et.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1603902045292",
      "Action": [
        "kms:CreateGrant",
        "kms:DescribeKey"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Le contexte de chiffrement de la subvention que vous avez créée utilise votre identifiant de compte `aws:iotsitewise:subscriberId` et.

Données inactives sur les passerelles SiteWise Edge

AWS IoT SiteWise les passerelles stockent les données suivantes sur le système de fichiers local :

- Informations de configuration de source OPC-UA
- Ensemble de chemins de flux de données OPC-UA à partir de sources OPC-UA connectées
- Données industrielles mises en cache lorsque la passerelle SiteWise Edge perd la connexion à Internet

SiteWise Les passerelles Edge fonctionnent. AWS IoT Greengrass AWS IoT Greengrass s'appuie sur les autorisations de fichiers Unix et le chiffrement complet du disque (s'il est activé) pour protéger les données au repos sur le cœur. Il est de votre responsabilité de sécuriser le système de fichiers et l'appareil.

Toutefois, chiffre AWS IoT Greengrass les copies locales des secrets de votre serveur OPC-UA récupérés depuis Secrets Manager. Pour plus d'informations, consultez la section Chiffrement des secrets dans le guide du AWS IoT Greengrass Version 1 développeur.

Pour plus d'informations sur le chiffrement au repos sur les AWS IoT Greengrass cœurs, consultez la section Chiffrement au repos dans le manuel du AWS IoT Greengrass Version 1 développeur.

Chiffrement en transit

AWS IoT SiteWise dispose de trois modes de communication lorsque les données sont en transit :

- Sur Internet : les communications entre les appareils locaux (y compris les passerelles SiteWise Edge) AWS IoT SiteWise sont cryptées.
- Sur le réseau local : les communications entre SiteWise l'application et OpsHub les passerelles SiteWise Edge sont toujours cryptées. La communication entre l'application de SiteWise surveillance exécutée dans votre navigateur et les passerelles SiteWise Edge est toujours cryptée. Les communications entre les passerelles SiteWise Edge et les sources OPC-UA peuvent être cryptées.
- Entre les composants des passerelles SiteWise Edge : les communications entre les AWS IoT Greengrass composants des passerelles SiteWise Edge ne sont pas chiffrées.

Rubriques

- Données en transit sur Internet
- Données en transit sur le réseau local
- Données en transit entre les composants locaux sur les passerelles SiteWise Edge

Données en transit sur Internet

AWS IoT SiteWise utilise le protocole TLS (Transport Layer Security) pour chiffrer toutes les communications sur Internet. Toutes les données envoyées au AWS Cloud sont envoyées via une connexion TLS à l'aide des protocoles MQTT ou HTTPS. Elles sont donc sécurisées par défaut. SiteWise Les passerelles Edge, qui s'exécutent sur AWS IoT Greengrass, et les notifications relatives à la valeur des propriétés utilisent le modèle de sécurité du AWS IoT transport. Pour de plus amples informations, veuillez consulter Sécurité du transport dans le Manuel du développeur AWS IoT .

Données en transit sur le réseau local

SiteWise Les passerelles Edge suivent les spécifications OPC-UA pour la communication avec les sources OPC-UA locales. Il est de votre responsabilité de configurer vos sources pour utiliser un mode de sécurité des messages qui chiffre les données en transit.

Si vous choisissez un mode de sécurité des messages de signature, les données en transit entre les passerelles SiteWise Edge et les sources sont signées mais pas chiffrées. Si vous choisissez un mode de sécurité des messages par signature et chiffrement, les données en transit entre les passerelles SiteWise Edge et les sources sont signées et chiffrées. Pour de plus amples informations sur les sources de configuration, veuillez consulter Configuration des sources de données.

La communication entre l'application de console Edge et les passerelles SiteWise Edge est toujours chiffrée par le protocole TLS. Le connecteur SiteWise Edge de la passerelle SiteWise Edge génère et stocke un certificat auto-signé afin de pouvoir établir une connexion TLS avec la console Edge pour AWS IoT SiteWise l'application. Vous devez copier ce certificat de votre passerelle SiteWise Edge vers la console Edge pour AWS IoT SiteWise l'application avant de connecter l'application à la passerelle SiteWise Edge. Cela garantit que la console Edge pour AWS IoT SiteWise l'application est en mesure de vérifier qu'elle est connectée à votre passerelle SiteWise Edge approuvée.

Outre le protocole TLS pour garantir la confidentialité et l'authenticité du serveur, SiteWise Edge utilise le protocole SigV4 pour établir l'authenticité de l'application de console Edge. Le connecteur SiteWise Edge de la passerelle SiteWise Edge accepte et stocke un mot de passe afin de vérifier les connexions entrantes provenant de l'application de console Edge, de l'application de SiteWise surveillance exécutée dans les navigateurs et d'autres clients basés sur le AWS IoT SiteWise SDK.

Pour plus d'informations sur la génération du mot de passe et du certificat de serveur, consultezthe section called “Gestion des passerelles SiteWise Edge”.

Données en transit entre les composants locaux sur les passerelles SiteWise Edge

SiteWise Les passerelles Edge s'exécutent AWS IoT Greengrass, ce qui ne chiffre pas les données échangées localement sur le AWS IoT Greengrass cœur, car elles ne quittent pas l'appareil. Cela inclut la communication entre AWS IoT Greengrass les composants tels que le AWS IoT SiteWise connecteur. Pour plus d'informations, consultez la section Données relatives à l'appareil principal dans le Guide du AWS IoT Greengrass Version 1 développeur.

Gestion des clés

AWS IoT SiteWise gestion des clés dans le cloud

Par défaut, AWS IoT SiteWise utilise Clés gérées par AWS pour protéger vos données dans le AWS cloud. Vous pouvez mettre à jour vos paramètres afin d'utiliser une clé gérée par le client pour chiffrer certaines données. AWS IoT SiteWise Vous pouvez créer, gérer et consulter votre clé de chiffrement via AWS Key Management Service (AWS KMS).

AWS IoT SiteWise prend en charge le chiffrement côté serveur en stockant les clés gérées par le client AWS KMS pour chiffrer les données suivantes :

- Valeurs des propriétés des actifs
- Valeurs agrégées

> **Note**
>
> Les autres données et ressources sont cryptées à l'aide du chiffrement par défaut avec des clés gérées par AWS IoT SiteWise. Cette clé est enregistrée dans le AWS IoT SiteWise compte.

Pour plus d'informations, voir Qu'est-ce que c'est AWS Key Management Service ? dans le Guide AWS Key Management Service du développeur.

Activer le chiffrement à l'aide de clés gérées par le client

Pour utiliser des clés gérées par le client avec AWS IoT SiteWise, vous devez mettre à jour vos AWS IoT SiteWise paramètres.

Pour activer le chiffrement à l'aide de clés KMS

1. Accédez à la console AWS IoT SiteWise.
2. Choisissez Paramètres du compte, puis Modifier pour ouvrir la page Modifier les paramètres du compte.
3. Pour le type de clé de chiffrement, choisissez Choisir une autre AWS KMS clé. Cela permet le chiffrement avec les clés gérées par le client stockées dans AWS KMS.

   > **Note**
   >
   > Actuellement, vous ne pouvez utiliser le chiffrement par clé géré par le client que pour les valeurs des propriétés des actifs et les valeurs agrégées.

4. Choisissez votre clé KMS avec l'une des options suivantes :

   - Pour utiliser une clé KMS existante : choisissez l'alias de votre clé KMS dans la liste.

- Pour créer une nouvelle clé KMS, choisissez Create an AWS KMS key.

> **Note**
>
> Cela ouvre le tableau de bord AWS KMS . Pour plus d'informations sur la création d'une clé KMS, consultez la section Création de clés dans le Guide du AWS Key Management Service développeur.

5. Choisissez Enregistrer pour mettre à jour vos paramètres.

SiteWise Gestion des clés de la passerelle Edge

SiteWise Les passerelles Edge fonctionnent AWS IoT Greengrass, et les appareils AWS IoT Greengrass principaux utilisent des clés publiques et privées pour s'authentifier auprès du AWS cloud et chiffrer les secrets locaux, tels que les secrets d'authentification OPC-UA. Pour plus d'informations, consultez la section Gestion des clés dans le Guide du AWS IoT Greengrass Version 1 développeur.

Gestion des identités et des accès pour AWS IoT SiteWise

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser AWS IoT SiteWise les ressources. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Public ciblé
- Authentification par des identités
- Comment AWS IoT SiteWise fonctionne avec IAM
- AWS politiques gérées pour AWS IoT SiteWise
- Utilisation des rôles liés aux services pour AWS IoT SiteWise
- Configuration des autorisations pour les AWS IoT Events alarmes
- Prévention du problème de l'adjoint confus entre services
- Résolution des problèmes AWS IoT SiteWise d'identité et d'accès

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez. AWS IoT SiteWise

Utilisateur du service : si vous utilisez le AWS IoT SiteWise service pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de nouvelles AWS IoT SiteWise fonctionnalités pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans AWS IoT SiteWise, consultez Résolution des problèmes AWS IoT SiteWise d'identité et d'accès.

Administrateur du service — Si vous êtes responsable des AWS IoT SiteWise ressources de votre entreprise, vous avez probablement un accès complet à AWS IoT SiteWise. C'est à vous de déterminer les AWS IoT SiteWise fonctionnalités et les ressources auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser IAM avec AWS IoT SiteWise, voirComment AWS IoT SiteWise fonctionne avec IAM.

Administrateur IAM – Si vous êtes un administrateur IAM, vous souhaiterez peut-être en savoir plus sur la façon d'écrire des politiques pour gérer l'accès à AWS IoT SiteWise. Pour consulter des exemples de politiques AWS IoT SiteWise basées sur l'identité que vous pouvez utiliser dans IAM, consultez. AWS IoT SiteWise exemples de politiques basées sur l'identité

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec

des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section Signature des demandes AWS d'API dans le guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur racine, consultez Tâches nécessitant les informations d'identification de l'utilisateur racine dans le Guide de l'utilisateur IAM.

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer

des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .

- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.
- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.
  - Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
  - Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage

des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Comment AWS IoT SiteWise fonctionne avec IAM

Avant d'utiliser AWS Identity and Access Management (IAM) pour gérer l'accès à AWS IoT SiteWise, vous devez connaître les fonctionnalités IAM disponibles. AWS IoT SiteWise

Fonction IAM	Soutenu par AWS IoT SiteWis
Stratégies basées sur l'identité avec autorisations au niveau des ressources	Oui
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition d'une politique	Oui
Politiques basées sur les ressources	Non
Listes de contrôle d'accès (ACL)	Non
Autorisation basée sur des balises (ABAC)	Oui
Informations d'identification temporaires	Oui
Sessions d'accès transféré (FAS)	Oui

Fonction IAM	Soutenu par AWS IoT SiteWis
Rôles liés à un service	Oui
Fonctions de service	Oui

Pour obtenir une vue d'ensemble de la façon dont AWS IoT SiteWise les autres AWS services fonctionnent avec IAM, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur d'IAM.

Table des matières

- AWS IoT SiteWise Rôles IAM
  - Utilisation d'informations d'identification temporaires avec AWS IoT SiteWise
  - Sessions d'accès direct (FAS) pour AWS IoT SiteWise
  - Rôles liés à un service
  - Rôles de service
  - Choix d'un rôle IAM dans AWS IoT SiteWise
- Autorisation basée sur les balises AWS IoT SiteWise
- AWS IoT SiteWise politiques basées sur l'identité
  - Actions de politique
    - BatchPutAssetPropertyValue autorisation
  - Ressources de politique
  - Clés de condition d'une politique
  - Exemples
- AWS IoT SiteWise exemples de politiques basées sur l'identité
  - Bonnes pratiques en matière de politiques
  - Utilisation de la console AWS IoT SiteWise
  - Autoriser des utilisateurs à afficher leurs propres autorisations
  - Autoriser les utilisateurs à ingérer des données dans des actifs dans une hiérarchie

  - Affichage des ressources AWS IoT SiteWise basées sur des balises
- Gestion des accès à l'aide de politiques
  - Politiques basées sur l'identité
  - politiques basées sur les ressources
  - Listes de contrôle d'accès (ACL)
  - Autres types de politique
  - Plusieurs types de politique

AWS IoT SiteWise Rôles IAM

Un rôle IAM est une entité au sein de votre Compte AWS qui dispose d'autorisations spécifiques.

Utilisation d'informations d'identification temporaires avec AWS IoT SiteWise

Vous pouvez utiliser des informations d'identification temporaires pour vous connecter à l'aide de la fédération, endosser un rôle IAM ou encore pour endosser un rôle intercompte. Vous obtenez des informations d'identification de sécurité temporaires en appelant des opérations d' AWS STS API telles que AssumeRoleou GetFederationToken.

AWS IoT SiteWise prend en charge l'utilisation d'informations d'identification temporaires.

SiteWise Monitor aide les utilisateurs fédérés à accéder aux portails. Les utilisateurs du portail s'authentifient à l'aide de leurs informations d'identification IAM Identity Center ou IAM.

> **Important**
>
> Les utilisateurs ou les rôles doivent être `iotsitewise:DescribePortal` autorisés à se connecter au portail.

Lorsqu'un utilisateur se connecte à un portail, SiteWise Monitor génère une politique de session qui fournit les autorisations suivantes :

- Accès en lecture seule aux actifs et aux données des actifs de AWS IoT SiteWise votre compte auxquels le rôle de ce portail permet d'accéder.
- Accès aux projets de ce portail auxquels l'utilisateur dispose d'un accès administrateur (propriétaire du projet) ou en lecture seule (visualiseur de projet).

Pour de plus amples informations sur les autorisations utilisateur du portail fédéré, veuillez consulter Utilisation des rôles de service pour AWS IoT SiteWise Monitor.

Sessions d'accès direct (FAS) pour AWS IoT SiteWise

Prend en charge les sessions d'accès direct (FAS)	Oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Rôles liés à un service

Les rôles liés aux AWS services permettent aux services d'accéder aux ressources d'autres services pour effectuer une action en votre nom. Les rôles liés à un service s'affichent dans votre Compte AWS et sont détenus par le service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

AWS IoT SiteWise prend en charge les rôles liés aux services. Pour plus d'informations sur la création ou la gestion des rôles liés à un service AWS IoT SiteWise , consultez Utilisation des rôles liés aux services pour AWS IoT SiteWise.

Rôles de service

Cette fonction permet à un service d'endosser une fonction du service en votre nom. Ce rôle autorise le service à accéder à des ressources d'autres services pour effectuer une action en votre nom. Les rôles de service apparaissent dans votre compte Compte AWS et sont détenus par celui-ci. Cela signifie qu'un administrateur IAM peut modifier les autorisations associées à ce rôle. Toutefois, une telle action peut perturber le bon fonctionnement du service.

AWS IoT SiteWise utilise un rôle de service pour permettre aux utilisateurs du portail SiteWise Monitor d'accéder à certaines de vos AWS IoT SiteWise ressources en votre nom. Pour plus d'informations, consultez Utilisation des rôles de service pour AWS IoT SiteWise Monitor.

Vous devez disposer des autorisations requises pour pouvoir créer des modèles AWS IoT Events d'alarme dans AWS IoT SiteWise. Pour plus d'informations, consultez Configuration des autorisations pour les AWS IoT Events alarmes.

Choix d'un rôle IAM dans AWS IoT SiteWise

Lorsque vous créez une `portal` ressource dans AWS IoT SiteWise, vous devez choisir un rôle pour permettre aux utilisateurs fédérés de votre portail SiteWise Monitor d'y accéder en votre AWS IoT SiteWise nom. Si vous avez déjà créé un rôle de service, il vous AWS IoT SiteWise fournit une liste de rôles parmi lesquels choisir. Sinon, vous pouvez créer un rôle avec les autorisations requises lorsque vous créez un portail. Il est important de choisir un rôle qui permet d'accéder à vos actifs et à vos données d'actifs. Pour plus d'informations, consultez Utilisation des rôles de service pour AWS IoT SiteWise Monitor.

Autorisation basée sur les balises AWS IoT SiteWise

Vous pouvez associer des balises aux AWS IoT SiteWise ressources ou transmettre des balises dans une demande à AWS IoT SiteWise. Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou `aws:TagKeys`. Pour plus d'informations sur le balisage des ressources AWS IoT SiteWise , consultez Marquer vos ressources AWS IoT SiteWise.

Pour visualiser un exemple de politique basée sur l'identité permettant de limiter l'accès à une ressource en fonction des balises de cette ressource, consultez Affichage des ressources AWS IoT SiteWise basées sur des balises.

AWS IoT SiteWise politiques basées sur l'identité

Les politiques IAM vous permettent de contrôler qui peut faire quoi. AWS IoT SiteWise Vous pouvez décider quelles actions sont autorisées ou non et définir des conditions spécifiques pour ces actions. Par exemple, vous pouvez définir des règles concernant les personnes autorisées à consulter ou à modifier des informations dans AWS IoT SiteWise. AWS IoT SiteWise prend en charge des actions, des ressources et des clés de condition spécifiques. Pour en savoir plus sur tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Actions de politique

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Les actions de politique en AWS IoT SiteWise cours utilisent le préfixe suivant avant l'action :`iotsitewise:`. Par exemple, pour autoriser une personne à télécharger les données relatives AWS IoT SiteWise aux propriétés des actifs dans le cadre de l'opération d'`BatchPutAssetPropertyValue`API, vous devez inclure l'`iotsitewise:BatchPutAssetPropertyValue`action dans sa politique. Les déclarations de politique doivent inclure un `NotAction` élément `Action` ou. AWS IoT SiteWise définit son propre ensemble d'actions décrivant les tâches que vous pouvez effectuer avec ce service.

Pour spécifier plusieurs actions dans une seule instruction, séparez-les par des virgules, comme suit :

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

Vous pouvez aussi préciser plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `Describe`, incluez l'action suivante.

```
"Action": "iotsitewise:Describe*"
```

Pour consulter la liste des AWS IoT SiteWise actions, reportez-vous à la section Actions définies par AWS IoT SiteWise dans le guide de l'utilisateur IAM.

BatchPutAssetPropertyValue autorisation

AWS IoT SiteWise autorise l'accès à l'action BatchPutAssetPropertyValue de manière inhabituelle. Pour la plupart des actions, lorsque vous autorisez ou refusez l'accès, cette action renvoie une erreur si les autorisations ne sont pas accordées. Avec`BatchPutAssetPropertyValue`, vous pouvez envoyer plusieurs entrées de données à différents actifs et propriétés d'actifs dans une seule demande d'API. AWS IoT SiteWise autorise chaque saisie de données indépendamment. Pour toute entrée individuelle dont l'autorisation échoue dans la demande, AWS IoT SiteWise inclut une erreur `AccessDeniedException` dans la liste d'erreurs renvoyée. AWS IoT SiteWise reçoit les données pour toute entrée autorisée et réussie, même si une autre entrée dans la même demande échoue.

> **Important**
>
> Avant d'ingérer des données dans un flux de données, procédez comme suit :
>
> - Autorisez la `time-series` ressource si vous utilisez un alias de propriété pour identifier le flux de données.
> - Autorisez la `asset` ressource si vous utilisez un ID d'actif pour identifier l'actif qui contient la propriété d'actif associée.

Ressources de politique

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Chaque déclaration de politique IAM s'applique aux ressources que vous spécifiez à l'aide de leur ARN. Un ARN a la syntaxe générale suivante :

```
arn:${Partition}:${Service}:${Region}:${Account}:${ResourceType}/${ResourcePath}
```

Pour plus d'informations sur le format des ARN, consultez Amazon Resource Names (ARN) et espaces de noms de AWS services.

Par exemple, pour spécifier l'actif avec l'ID `a1b2c3d4-5678-90ab-cdef-22222EXAMPLE` dans votre instruction, utilisez l'ARN suivant :

```
"Resource": "arn:aws:iotsitewise:region:123456789012:asset/a1b2c3d4-5678-90ab-
cdef-22222EXAMPLE"
```

Pour spécifier tous les flux de données appartenant à un compte spécifique, utilisez le caractère générique (*) :

```
"Resource": "arn:aws:iotsitewise:region:123456789012:time-series/*"
```

Pour spécifier tous les actifs appartenant à un compte spécifique, utilisez le caractère générique (*) :

```
"Resource": "arn:aws:iotsitewise:region:123456789012:asset/*"
```

Certaines AWS IoT SiteWise actions, telles que celles relatives à la création de ressources, ne peuvent pas être effectuées sur une ressource spécifique. Dans ces cas-là, vous devez utiliser le caractère générique (*).

```
"Resource": "*"
```

Pour spécifier plusieurs ressources dans une seule instruction, séparez leurs ARN par des virgules.

```
"Resource": [
  "resource1",
  "resource2"
]
```

Pour consulter la liste des types de AWS IoT SiteWise ressources et de leurs ARN, consultez la section Ressources définies par AWS IoT SiteWise dans le guide de l'utilisateur IAM. Pour savoir

grâce à quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par AWS IoT SiteWise.

Clés de condition d'une politique

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

> **Important**
>
> Plusieurs clés de condition sont propres à une ressource et certaines actions d'API utilisent plusieurs ressources. Si vous écrivez une déclaration de stratégie avec une clé de condition, utilisez l'élément `Resource` de la déclaration pour spécifier la ressource à laquelle la clé de condition s'applique. Dans le cas contraire, la stratégie peut empêcher totalement les utilisateurs d'exécuter l'action, car le contrôle de la condition échoue pour les ressources auxquelles la clé de condition ne s'applique pas. Si vous ne voulez pas spécifier de ressource ou si vous avez écrit l'élément `Action` de votre stratégie pour inclure plusieurs actions d'API, vous devez utiliser le type de condition `...IfExists` pour garantir que la clé de condition

est ignorée pour les ressources qui ne l'utilisent pas. Pour plus d'informations, voir... IfExists conditions énoncées dans le guide de l'utilisateur IAM.

AWS IoT SiteWise définit son propre ensemble de clés de condition et prend également en charge l'utilisation de certaines clés de condition globales. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

AWS IoT SiteWise clés de condition

Clé de condition	Description	Types
`iotsitewise:isAssociatedWithAssetProperty`	Si les flux de données sont associés à une propriété d'actif. Utilisez cette clé de condition pour définir les autorisations en fonction de l'existence d'une propriété d'actif associée pour les flux de données. Exemple de valeur : `true`	Chaîne
`iotsitewise:assetHierarchyPath`	Chemin de hiérarchie de l'actif, qui est une chaîne d'ID d'actif séparés par une barre oblique. Utilisez cette clé de condition pour définir des autorisations en fonction d'un sous-ensemble de votre hiérarchie de tous les actifs de votre compte. Exemple de valeur : `/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE/a1b2c3d4-5678-90ab-cdef-66666EXAMPLE`	Chaîne

Clé de condition	Description	Types
`iotsitewise:propertyId`	ID d'une propriété d'actif. Utilisez cette clé de condition pour définir des autorisations basées sur une propriété spécifiée d'un modèle de ressource. Cette clé de condition s'applique à tous les actifs de ce modèle. Exemple de valeur : `a1b2c3d4-5678-90ab-cdef-33333EXAMPLE`	Chaîne
`iotsitewise:childAssetId`	ID d'une ressource associée en tant qu'enfant à une autre ressource. Utilisez cette clé de condition pour définir les autorisations en fonction des ressources enfants. Pour définir des autorisations en fonction des ressources parent, utilisez la section ressource d'une instruction de stratégie. Exemple de valeur : `a1b2c3d4-5678-90ab-cdef-66666EXAMPLE`	Chaîne

Clé de condition	Description	Types
`iotsitewise:iam`	L'ARN d'une identité IAM lors de la liste des politiques d'accès. Utilisez cette clé de condition pour définir les autorisations de politique d'accès pour une identité IAM. Exemple de valeur : `arn:aws:iam::123456789012:user/JohnDoe`	Chaîne, null
`iotsitewise:propertyAlias`	Alias qui identifie une propriété d'actif ou un flux de données. Utilisez cette clé de condition pour définir les autorisations en fonction de l'alias.	Chaîne
`iotsitewise:user`	ID d'un utilisateur du IAM Identity Center lors de la liste des politiques d'accès. Utilisez cette clé de condition pour définir les autorisations de politique d'accès pour un utilisateur d'IAM Identity Center. Exemple de valeur : `a1b2c3d4e5-a1b2c3d4-5678-90ab-cdef-aaaaEXAMPLE`	Chaîne, null

Clé de condition	Description	Types
`iotsitewise:group`	ID d'un groupe IAM Identity Center lors de la liste des politiques d'accès. Utilisez cette clé de condition pour définir les autorisations de politique d'accès pour un groupe IAM Identity Center. Exemple de valeur : `a1b2c3d4e5-a1b2c3d4-5678-90ab-cdef-bbbbbEXAMPLE`	Chaîne, null
`iotsitewise:portal`	ID d'un portail dans une stratégie d'accès. Utilisez cette clé de condition pour définir les autorisations de stratégie d'accès basées sur un portail. Exemple de valeur : `a1b2c3d4-5678-90ab-cdef-77777EXAMPLE`	Chaîne, null
`iotsitewise:project`	ID d'un projet dans une stratégie d'accès ou ID d'un projet pour un tableau de bord. Utilisez cette clé de condition pour définir des autorisations de stratégie d'accès ou de tableau de bord en fonction d'un projet. Exemple de valeur : `a1b2c3d4-5678-90ab-cdef-88888EXAMPLE`	Chaîne, null

Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, voir Actions définies par AWS IoT SiteWise.

Exemples

Pour consulter des exemples de politiques AWS IoT SiteWise basées sur l'identité, consultez. AWS IoT SiteWise exemples de politiques basées sur l'identité

AWS IoT SiteWise exemples de politiques basées sur l'identité

Par défaut, les entités (utilisateurs et rôles) ne sont pas autorisées à créer ou à modifier AWS IoT SiteWise des ressources. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour ajuster les autorisations, un administrateur AWS Identity and Access Management (IAM) doit effectuer les opérations suivantes :

1. Créez des politiques IAM qui accordent aux utilisateurs et aux rôles l'autorisation d'effectuer des opérations d'API spécifiques sur les ressources dont ils ont besoin.
2. Associez ces politiques aux utilisateurs ou aux groupes qui ont besoin de ces autorisations.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, veuillez consulter Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console AWS IoT SiteWise
- Autoriser des utilisateurs à afficher leurs propres autorisations
- Autoriser les utilisateurs à ingérer des données dans des actifs dans une hiérarchie
- Affichage des ressources AWS IoT SiteWise basées sur des balises

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer AWS IoT SiteWise des ressources dans votre compte. Ces actions peuvent entraîner des frais pour votre

Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accorder les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la console AWS IoT SiteWise

Pour accéder à la AWS IoT SiteWise console, vous avez besoin d'un ensemble d'autorisations de base. Ces autorisations vous permettent de consulter et de gérer les informations relatives aux AWS IoT SiteWise ressources de votre Compte AWS.

Si vous définissez une politique trop restrictive, la console risque de ne pas fonctionner comme prévu pour les utilisateurs ou les rôles (entités) concernés par cette politique. Pour garantir que ces entités peuvent toujours utiliser la AWS IoT SiteWise console, associez-leur la politique AWSIoTSiteWiseConsoleFullAccessgérée ou définissez des autorisations équivalentes pour ces entités. Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

Si les entités utilisent uniquement la AWS Command Line Interface (CLI) ou l' AWS IoT SiteWise API, et non la console, elles n'ont pas besoin de ces autorisations minimales. Dans ce cas, donnez-leur simplement accès aux actions spécifiques dont ils ont besoin pour leurs tâches d'API.

Autoriser des utilisateurs à afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or 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": "*"
        }
    ]
}
```

Autoriser les utilisateurs à ingérer des données dans des actifs dans une hiérarchie

Dans cet exemple, vous souhaitez autoriser un utilisateur à écrire des données sur toutes les propriétés des actifs dans une hiérarchie d'actifs spécifique, en commençant par l'actif racine`a1b2c3d4-5678-90ab-cdef-22222EXAMPLE`. Compte AWS La stratégie accorde l'autorisation `iotsitewise:BatchPutAssetPropertyValue` à l'utilisateur. Cette stratégie utilise la clé de condition `iotsitewise:assetHierarchyPath` pour restreindre l'accès aux ressources dont le chemin hiérarchique correspond à l'actif ou à ses descendants.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PutAssetPropertyValuesForHierarchy",
      "Effect": "Allow",
      "Action": "iotsitewise:BatchPutAssetPropertyValue",
      "Resource": "arn:aws:iotsitewise:*:*:asset/*",
      "Condition": {
        "StringLike": {
          "iotsitewise:assetHierarchyPath": [
            "/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
            "/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE/*"
          ]
        }
      }
```

```
    }
  ]
}
```

Affichage des ressources AWS IoT SiteWise basées sur des balises

Utilisez les conditions de votre politique basée sur l'identité pour contrôler l'accès aux AWS IoT SiteWise ressources en fonction des balises. Cet exemple montre comment créer une politique permettant de visualiser les actifs. Toutefois, l'autorisation est accordée uniquement si la balise de ressource `Owner` a pour valeur le nom d'utilisateur de cet utilisateur. Cette politique accorde également l'autorisation d'effectuer cette action sur la 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}"
        }
      }
    }
  ]
}
```

Associez cette politique aux utilisateurs de votre compte. Si un utilisateur nommé `richard-roe` tente de consulter une AWS IoT SiteWise ressource, celle-ci doit être étiquetée `Owner=richard-roe` ou`owner=richard-roe`. Dans le cas contraire, Richard se voit refuser l'accès. Les noms des clés des balises de condition ne distinguent pas les majuscules et minuscules. Donc, `Owner`

correspond aux deux `0wner` et`owner`. Pour plus d'informations, consultez Éléments de politique JSON IAM : Condition dans le Guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les

politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principals (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez Vue d'ensemble des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour

une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.

- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS Organizations AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

AWS politiques gérées pour AWS IoT SiteWise

Simplifiez l'ajout d'autorisations aux utilisateurs, aux groupes et aux rôles à l'aide de politiques AWS gérées plutôt que de rédiger vous-même des politiques. Il faut du temps et de l'expertise pour créer des politiques IAM gérées par les clients qui fournissent des autorisations précises à votre équipe. Pour une configuration plus rapide, pensez à utiliser nos politiques AWS gérées pour les cas d'utilisation courants. Trouvez les politiques AWS gérées dans votre Compte AWS. Pour plus

d'informations sur les politiques gérées AWS , consultez Politiques gérées AWS dans le Guide de l'utilisateur IAM.

AWS les services se chargent de mettre à jour et de maintenir les politiques AWS gérées, ce qui signifie que vous ne pouvez pas modifier les autorisations de ces politiques. Occasionnellement, des autorisations AWS IoT SiteWise peuvent être ajoutées pour s'adapter à de nouvelles fonctionnalités, ce qui a un impact sur toutes les identités associées à la politique. Ces mises à jour sont courantes lors de l'introduction de nouveaux services ou fonctionnalités. Cependant, les autorisations ne sont jamais supprimées, ce qui garantit que vos configurations restent intactes.

En outre, AWS prend en charge les politiques gérées pour les fonctions professionnelles qui couvrent plusieurs services. Par exemple, la politique ReadOnlyd'accès AWS géré fournit un accès en lecture seule à tous les AWS services et ressources. Lorsqu'un service lance une nouvelle fonctionnalité, il AWS ajoute des autorisations en lecture seule pour les nouvelles opérations et ressources. Pour obtenir une liste avec des descriptions des politiques relatives aux fonctions de travail, voir les politiques AWS gérées pour les fonctions de travail dans le guide de l'utilisateur d'IAM.

AWS politique gérée : AWSIoTSiteWiseReadOnlyAccess

Utilisez la politique `AWSIoTSiteWiseReadOnlyAccess` AWS gérée pour autoriser l'accès en lecture seule à. AWS IoT SiteWise

Vous pouvez associer la politique `AWSIoTSiteWiseReadOnlyAccess` à vos identités IAM.

Autorisations au niveau du service

Cette politique fournit un accès en lecture seule à. AWS IoT SiteWise Cette politique n'inclut aucune autre autorisation de service.

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

```
    ]
}
```

AWS politique gérée : AWSServiceRoleForIoTSiteWise

Le `AWSServiceRoleForIoTSiteWise` rôle utilise la `AWSServiceRoleForIoTSiteWise` politique avec les autorisations suivantes. Cette politique :

- Permet AWS IoT SiteWise de déployer des passerelles SiteWise Edge (qui s'exécutent sur`AWS IoT Greengrass`).
- Permet d' AWS IoT SiteWise effectuer une journalisation.
- Permet AWS IoT SiteWise d'exécuter une requête de recherche de métadonnées sur la AWS IoT TwinMaker base de données.

Si vous utilisez AWS IoT SiteWise un compte utilisateur unique, le `AWSServiceRoleForIoTSiteWise` rôle crée la `AWSServiceRoleForIoTSiteWise` politique dans votre compte IAM et l'associe aux rôles `AWSServiceRoleForIoTSiteWise` liés au service pour. 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 mises à jour des politiques AWS gérées

Vous pouvez consulter les informations relatives aux mises à jour des politiques AWS gérées pour AWS IoT SiteWise, à partir de la date à laquelle ce service a commencé à suivre les modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page Historique du AWS IoT SiteWise document.

Modification	Description	Date
AWSServiceRoleForIoTSiteWise – Mise à jour d'une stratégie existante	AWS IoT SiteWise peut désormais exécuter une requête de recherche de métadonnées sur la AWS IoT TwinMaker base de données.	6 novembre 2023
AWSIoTSiteWiseReadOnlyAccess – Mise à jour d'une politique existante	AWS IoT SiteWise a ajouté un nouveau préfixe de politique `BatchGet*` , qui vous permet d'effectuer des opérations de lecture par lots.	16 septembre 2022
AWSIoTSiteWiseReadOnlyAccess : nouvelle politique	AWS IoT SiteWise a ajouté une nouvelle politique pour accorder un accès en lecture seule à. AWS IoT SiteWise	24 novembre 2021
AWS IoT SiteWise a commencé à suivre les modifications	AWS IoT SiteWise a commencé à suivre les modifications apportées AWS à ses politiques gérées.	24 novembre 2021

Utilisation des rôles liés aux services pour AWS IoT SiteWise

AWS IoT SiteWise utilise des AWS Identity and Access Management rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à. AWS IoT SiteWise Les rôles liés au service sont prédéfinis par AWS IoT SiteWise et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Les rôles liés aux services simplifient la configuration de AWS IoT SiteWise en incluant automatiquement toutes les autorisations nécessaires. AWS IoT SiteWise définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul AWS IoT SiteWise peut assumer ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisations. Et cette politique d'autorisation ne peut être attachée à aucune autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela protège vos AWS IoT SiteWise ressources car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez Services AWS fonctionnant avec IAM et recherchez les services avec un Yes (Oui) dans la colonne Service-Linked Role (Rôle lié à un service). Sélectionnez un Oui ayant un lien pour consulter la documentation du rôle lié à un service, pour ce service.

Rubriques

- Autorisations des rôles liés à un service pour AWS IoT SiteWise
- Création d'un rôle lié à un service pour AWS IoT SiteWise
- Modification d'un rôle lié à un service pour AWS IoT SiteWise
- Suppression d'un rôle lié à un service pour AWS IoT SiteWise
- Régions prises en charge pour les rôles AWS IoT SiteWise liés à un service
- Utilisation des rôles de service pour AWS IoT SiteWise Monitor

Autorisations des rôles liés à un service pour AWS IoT SiteWise

AWS IoT SiteWise utilise le rôle lié au service nommé. AWSServiceRoleForIoTSiteWise AWS IoT SiteWise utilise ce rôle lié à un service pour déployer des passerelles SiteWise Edge (qui s'exécutent AWS IoT Greengrass) et effectuer la journalisation.

Le rôle `AWSServiceRoleForIoTSiteWise` lié au service utilise la `AWSServiceRoleForIoTSiteWise` politique avec les autorisations suivantes. Cette politique :

- Permet AWS IoT SiteWise de déployer des passerelles SiteWise Edge (qui s'exécutent sur`AWS IoT Greengrass`).
- Permet d' AWS IoT SiteWise effectuer une journalisation.
- Permet AWS IoT SiteWise d'exécuter une requête de recherche de métadonnées sur la AWS IoT TwinMaker base de données.

Pour plus d'informations sur les actions autorisées dans`AWSServiceRoleForIoTSiteWise`, consultez les politiques AWS gérées pour 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"
     ]
    }
   }
  }
 ]
}
```

Vous pouvez utiliser les journaux pour surveiller et dépanner vos passerelles SiteWise Edge. Pour plus d'informations, consultez Surveillance des journaux de la passerelle SiteWise Edge.

Pour autoriser une entité IAM (telle qu'un utilisateur, un groupe ou un rôle) à créer, modifier ou supprimer un rôle lié à un service, configurez d'abord les autorisations. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour AWS IoT SiteWise

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous effectuez les opérations suivantes dans la AWS IoT SiteWise console, AWS IoT SiteWise crée le rôle lié au service pour vous.

- Créez une passerelle Greengrass V1.
- Configurez l'option de journalisation.
- Choisir le bouton d'inscription dans le bandeau d'exécution de la requête.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous effectuez une opération dans la AWS IoT SiteWise console, AWS IoT SiteWise crée à nouveau le rôle lié au service pour vous.

Vous pouvez également utiliser la console ou l'API IAM pour créer un rôle lié à un service pour. AWS IoT SiteWise

- Pour ce faire, dans la console IAM, créez un rôle avec la AWSServiceRoleForIoTSiteWisepolitique et une relation de confiance avec`iotsitewise.amazonaws.com`.
- Pour ce faire, utilisez l'API AWS CLI ou IAM, créez un rôle avec la `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise` politique et une relation de confiance avec`iotsitewise.amazonaws.com`.

Pour plus d'informations, consultez Création d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Si vous supprimez ce rôle lié à un service, vous pouvez utiliser ce même processus pour créer le rôle à nouveau.

Modification d'un rôle lié à un service pour AWS IoT SiteWise

AWS IoT SiteWise ne vous permet pas de modifier le rôle AWSServiceRoleForIoTSiteWise lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence au rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour AWS IoT SiteWise

Si une fonctionnalité ou un service nécessitant un rôle lié à un service n'est plus utilisé, il est conseillé de supprimer le rôle associé. Cela permet d'éviter d'avoir une entité inactive qui n'est ni surveillée ni maintenue. Cependant, vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement.

> **Note**
>
> Si le AWS IoT SiteWise service utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, attendez quelques minutes et réessayez.

Pour supprimer AWS IoT SiteWise les ressources utilisées par le AWSServiceRoleForIoTSiteWise

1. Désactivez la journalisation pour AWS IoT SiteWise. Pour plus d'informations, consultez Modification de votre niveau de journalisation.
2. Supprimez toutes les passerelles SiteWise Edge actives.

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au AWSServiceRoleForIoTSiteWise service. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles AWS IoT SiteWise liés à un service

AWS IoT SiteWise prend en charge l'utilisation de rôles liés au service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez Points de terminaison et quotas AWS IoT SiteWise.

Utilisation des rôles de service pour AWS IoT SiteWise Monitor

Une fonction de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

Pour permettre aux utilisateurs du portail SiteWise Monitor fédéré d'accéder à vos AWS IAM Identity Center ressources AWS IoT SiteWiseet à vos ressources, vous devez attribuer un rôle de service à chaque portail que vous créez. Le rôle de service doit spécifier SiteWise Monitor en tant qu'entité de confiance et inclure la politique AWSIoTSiteWiseMonitorPortalAccessgérée ou définir des autorisations équivalentes. Cette politique est gérée par AWS et définit l'ensemble d'autorisations que SiteWise Monitor utilise pour accéder à vos ressources AWS IoT SiteWise et à celles d'IAM Identity Center.

Lorsque vous créez un portail SiteWise Monitor, vous devez choisir un rôle qui permet aux utilisateurs de ce portail d'accéder à vos ressources AWS IoT SiteWiseet à celles d'IAM Identity Center. La AWS IoT SiteWise console peut créer et configurer le rôle pour vous. Vous pourrez modifier le rôle dans IAM ultérieurement. Les utilisateurs de votre portail rencontreront des problèmes lors de l'utilisation de leurs portails SiteWise Monitor si vous supprimez les autorisations requises pour le rôle ou si vous supprimez le rôle.

> **Note**
>
> Les portails créés avant le 29 avril 2020 ne nécessitaient pas de rôles de service. Si vous avez créé des portails avant cette date, vous devez joindre des rôles de service pour continuer à les utiliser. Pour ce faire, accédez à la page Portails de la AWS IoT SiteWise console, puis choisissez Migrer tous les portails pour utiliser les rôles IAM.

Les sections suivantes décrivent comment créer et gérer le rôle de service SiteWise Monitor dans le AWS Management Console ou le AWS Command Line Interface.

Table des matières

- Autorisations de rôle de service pour SiteWise Monitor
- Gestion du rôle de service SiteWise Monitor (console)
  - Recherche du rôle de service d'un portail (console)
  - Création d'un rôle de service de SiteWise surveillance (AWS IoT SiteWise console)
  - Création d'un rôle de service de SiteWise surveillance (console IAM)
  - Modification du rôle de service d'un portail (console)
- Gestion du rôle de service SiteWise Monitor (CLI)
  - Recherche du rôle de service d'un portail (interface de ligne de commande)
  - Création du rôle de service SiteWise Monitor (CLI)
- SiteWise Surveillez les mises à jour de AWSIoTSiteWiseMonitorServiceRole

Autorisations de rôle de service pour SiteWise Monitor

Lorsque vous créez un portail, vous AWS IoT SiteWise permet de créer un rôle dont le nom commence par AWSIoTSiteWiseMonitorServiceRole. Ce rôle permet aux utilisateurs fédérés de SiteWise Monitor d'accéder à la configuration de votre portail, aux actifs, aux données des actifs, ainsi qu'à la configuration d'IAM Identity Center.

Le rôle approuve le fait que le service suivant endosse le rôle :

- `monitor.iotsitewise.amazonaws.com`

Le rôle utilise la politique d'autorisation suivante, dont le nom commence par AWSIoTSiteWiseMonitorServicePortalPolicy, pour permettre aux utilisateurs de SiteWise Monitor d'effectuer des actions sur les ressources de votre compte. La politique AWSIoTSiteWiseMonitorPortalAccessgérée définit des autorisations équivalentes.

```
{
    "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"
                    ]
```

```
                }
            }
        }
    ]
}
```

Pour plus d'informations sur les autorisations requises pour les alarmes, consultezConfiguration des autorisations pour les AWS IoT Events alarmes.

Lorsqu'un utilisateur du portail se connecte, SiteWise Monitor crée une politique de session basée sur l'intersection entre le rôle de service et les politiques d'accès de cet utilisateur. Les stratégies d'accès définissent le niveau d'accès des identités à vos portails et projets. Pour plus d'informations sur les autorisations du portail et les politiques d'accès, consultez la section Administration de vos portails SiteWise Monitor et CreateAccessla politique.

Gestion du rôle de service SiteWise Monitor (console)

Console AWS IoT SiteWise Facilite la gestion du rôle de service SiteWise Monitor pour les portails. Lors de la création d'un portail, la console vérifie les rôles existants susceptibles d'être rattachés. Si aucun n'est disponible, la console peut créer et configurer un rôle de service pour vous. Pour plus d'informations, consultez Création d'un portail.

Rubriques

- Recherche du rôle de service d'un portail (console)
- Création d'un rôle de service de SiteWise surveillance (AWS IoT SiteWise console)
- Création d'un rôle de service de SiteWise surveillance (console IAM)
- Modification du rôle de service d'un portail (console)

Recherche du rôle de service d'un portail (console)

Suivez les étapes ci-dessous pour trouver le rôle de service associé à un portail SiteWise Monitor.

Pour rechercher le rôle de service d'un portail

1. Accédez à la console AWS IoT SiteWise.
2. Dans le volet de navigation de gauche, choisissez Portals (Portails).
3. Choisissez le portail pour lequel vous souhaitez rechercher le rôle de service.

   Le rôle associé au portail apparaît sous Autorisations, rôle de service.

Création d'un rôle de service de SiteWise surveillance (AWS IoT SiteWise console)

Lorsque vous créez un portail SiteWise Monitor, vous pouvez créer un rôle de service pour votre portail. Pour plus d'informations, consultez Création d'un portail.

Vous pouvez également créer un rôle de service pour un portail existant dans la AWS IoT SiteWise console. Cela remplace le rôle de service existant du portail.

Pour créer un rôle de service pour un portail existant

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Portails.
3. Choisissez le portail pour lequel vous souhaitez créer un rôle de service.
4. Sous Détails du portail, choisissez Modifier.
5. Sous Autorisations, choisissez Créer et utiliser un nouveau rôle de service dans la liste.
6. Saisissez un nom pour votre nouveau rôle.
7. Choisissez Enregistrer.

Création d'un rôle de service de SiteWise surveillance (console IAM)

Vous pouvez créer un rôle de service à partir du modèle de rôle de service de la console IAM. Ce modèle de rôle inclut la politique AWSIoTSiteWiseMonitorPortalAccessgérée et spécifie SiteWise Monitor comme une entité de confiance.

Pour créer un rôle de service à partir du modèle de rôle de service du portail

1. Accédez à la Console IAM.
2. Dans le panneau de navigation, choisissez Roles (Rôles).
3. Sélectionnez Create role (Créer un rôle).
4. Dans Choisir un cas d'utilisation, sélectionnez IoT SiteWise.
5. Dans Sélectionnez votre cas d'utilisation, choisissez IoT SiteWise Monitor - Portal.
6. Sélectionnez Next: Permissions (Étape suivante : autorisations).
7. Choisissez Suivant : Balises.
8. Choisissez Suivant : Vérification.
9. Entrez un nom de rôle pour le nouveau rôle de service.
10. Sélectionnez Créer un rôle.

Modification du rôle de service d'un portail (console)

Utilisez la procédure suivante pour choisir un autre rôle de service de SiteWise surveillance pour un portail.

Pour modifier le rôle de service d'un portail

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation, choisissez Portails.
3. Choisissez le portail pour lequel vous souhaitez modifier le rôle de service.
4. Sous Détails du portail, choisissez Modifier.
5. Sous Autorisations, choisissez Utiliser un rôle existant.
6. Choisissez un rôle existant à attacher à ce portail.
7. Choisissez Enregistrer.

Gestion du rôle de service SiteWise Monitor (CLI)

Vous pouvez utiliser le AWS CLI pour les tâches de gestion des rôles de service de portail suivantes :

Rubriques

- Recherche du rôle de service d'un portail (interface de ligne de commande)
- Création du rôle de service SiteWise Monitor (CLI)

Recherche du rôle de service d'un portail (interface de ligne de commande)

Pour trouver le rôle de service associé à un portail de SiteWise surveillance, exécutez la commande suivante pour répertorier tous vos portails dans la région actuelle.

```
aws iotsitewise list-portals
```

L'opération renvoie une réponse qui contient les résumés de vos portails au format suivant.

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

Vous pouvez également utiliser DescribePortalcette opération pour trouver le rôle de votre portail si vous connaissez son identifiant.

Création du rôle de service SiteWise Monitor (CLI)

Suivez les étapes ci-dessous pour créer un nouveau rôle de service de SiteWise surveillance.

Pour créer un rôle SiteWise de service de surveillance

1. Créez un rôle avec une politique de confiance qui permet à SiteWise Monitor d'assumer ce rôle. Cet exemple crée un rôle nommé **`MySiteWiseMonitorPortalRole`** à partir d'une stratégie d'approbation stockée dans une chaîne 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. Copiez l'ARN de rôle du rôle des métadonnées dans la sortie. Lorsque vous créez un portail, vous utilisez cet ARN pour associer le rôle à votre portail. Pour plus d'informations sur la création d'un portail, consultez CreatePortalla référence des AWS IoT SiteWise API.
3. Attachez la stratégie `AWSIoTSiteWiseMonitorPortalAccess` au rôle ou attachez une stratégie qui définit des autorisations équivalentes.

```
aws iam attach-role-policy --role-name MySiteWiseMonitorPortalRole --policy-arn
 arn:aws:iam::aws:policy/service-role/AWSIoTSiteWiseMonitorPortalAccess
```

Pour attacher un rôle de service à un portail existant

1. Pour récupérer les détails existants du portail, exécutez la commande suivante. Remplacez *portal-id* par l'ID du portail.

```
aws iotsitewise describe-portal --portal-id portal-id
```

L'opération renvoie une réponse qui contient les détails du portail dans le format suivant.

```
{
    "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. Pour attacher un rôle de service à un portail, exécutez la commande suivante. Remplacez *role-arn* par l'ARN de rôle de service et remplacez les paramètres restants par les valeurs existantes du portail.

```
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 Surveillez les mises à jour de AWSIoTSiteWiseMonitorServiceRole

Vous pouvez consulter les détails des mises à jour de AWSIoTSiteWiseMonitorServiceRolefor SiteWise Monitor, à partir du moment où ce service a commencé à suivre les modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page Historique du AWS IoT SiteWise document.

Modification	Description	Date
AWSIoTSiteWiseMonitorPortalAccess— Politique mise à jour	AWS IoT SiteWise a mis à jour la politique AWSIoTSiteWiseMonitorPortalAccessgérée pour la fonctionnalité d'alarmes.	27 mai 2021
AWS IoT SiteWise a commencé à suivre les modifications	AWS IoT SiteWise a commencé à suivre les modifications apportées à son rôle de service.	15 décembre 2020

Configuration des autorisations pour les AWS IoT Events alarmes

Lorsque vous utilisez un modèle AWS IoT Events d'alarme pour surveiller la propriété AWS IoT SiteWise d'un actif, vous devez disposer des autorisations IAM suivantes :

- Rôle de AWS IoT Events service qui permet d' AWS IoT Events envoyer des données à AWS IoT SiteWise. Pour plus d'informations, consultez la section Gestion des identités et des accès AWS IoT Events dans le Guide du AWS IoT Events développeur.
- Vous devez disposer des autorisations AWS IoT SiteWise d'action suivantes : `iotsitewise:DescribeAssetModel` et`iotsitewise:UpdateAssetModelPropertyRouting`. Ces autorisations permettent d' AWS IoT SiteWise envoyer les valeurs des propriétés des actifs aux modèles AWS IoT Events d'alarme.

Pour plus d'informations, consultez la section Politiques basées sur les ressources dans le guide de l'utilisateur IAM.

Autorisations d'action requises

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions. L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique.

Avant de définir un modèle AWS IoT Events d'alarme, vous devez accorder les autorisations suivantes qui permettent d' AWS IoT SiteWise envoyer les valeurs des propriétés des actifs au modèle d'alarme.

- `iotsitewise:DescribeAssetModel`— Permet AWS IoT Events de vérifier si une propriété d'actif existe.
- `iotsitewise:UpdateAssetModelPropertyRouting`— Permet AWS IoT SiteWise de créer automatiquement des abonnements permettant AWS IoT SiteWise d'envoyer des données à AWS IoT Events.

Pour plus d'informations sur les actions AWS IoT SiteWise prises en charge, consultez la section Actions définies par AWS IoT SiteWise dans la référence d'autorisation de service.

Example Exemple de politique d'autorisation 1

La politique suivante permet d' AWS IoT SiteWise envoyer les valeurs des propriétés des actifs à n'importe quel modèle AWS IoT Events d'alarme.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iotevents:CreateAlarmModel",
                "iotevents:UpdateAlarmModel"
            ],
            "Resource": "arn:aws:iotevents:us-east-1:123456789012:alarmModel/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iotsitewise:DescribeAssetModel",
                "iotsitewise:UpdateAssetModelPropertyRouting"
            ],
            "Resource": "arn:aws:iotsitewise:us-east-1:123456789012:asset-model/*"
        }
    ]
}
```

Example Exemple de politique d'autorisation 2

La politique suivante permet d' AWS IoT SiteWise envoyer les valeurs d'une propriété d'actif spécifiée à un modèle AWS IoT Events d'alarme spécifié.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iotevents:CreateAlarmModel",
                "iotevents:UpdateAlarmModel"
            ],
            "Resource": "arn:aws:iotevents:us-east-1:123456789012:alarmModel/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iotsitewise:DescribeAssetModel"
            ],
            "Resource": "arn:aws:iotsitewise:us-east-1:123456789012:asset-model/*"
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "iotsitewise:UpdateAssetModelPropertyRouting"
            ],
            "Resource": [
                "arn:aws:iotsitewise:us-east-1:123456789012:asset-model/12345678-90ab-
cdef-1234-567890abcdef"
            ],
            "Condition": {
                "StringLike": {
                    "iotsitewise:propertyId": "abcdef12-3456-7890-abcd-ef1234567890",
                    "iotevents:alarmModelArn": "arn:aws:iotevents:us-
east-1:123456789012:alarmModel/MyAlarmModel"
                }
            }
        }
    ]
}
```

ListInputRoutings Autorisation (facultative)

Lorsque vous mettez à jour ou supprimez un modèle d'actif, vous AWS IoT SiteWise pouvez vérifier si un modèle d'alarme AWS IoT Events surveille une propriété d'actif associée à ce modèle d'actif. Cela vous empêche de supprimer une propriété de ressource actuellement AWS IoT Events utilisée par une alarme. Pour activer cette fonctionnalité dans AWS IoT SiteWise, vous devez avoir l'`iotevents:ListInputRoutings`autorisation. Cette autorisation permet d' AWS IoT SiteWise appeler l'opération de l'API ListInputRoutings prise en charge par AWS IoT Events.

> **Note**
>
> Nous vous recommandons vivement d'ajouter cette `ListInputRoutings` autorisation.

Example Exemple de politique d'autorisation

La politique suivante vous permet de mettre à jour et de supprimer des modèles d'actifs, ainsi que d'utiliser l'`ListInputRoutings`API dans 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/*"
        }
    ]
}
```

Autorisations requises pour SiteWise Monitor

Si vous souhaitez utiliser la fonctionnalité d'alarmes dans les portails de SiteWise surveillance, vous devez mettre à jour le rôle de service de SiteWise surveillance avec la politique suivante :

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

Prévention du problème de l'adjoint confus entre services

Le problème de député confus est un problème de sécurité dans lequel une entité qui n'est pas autorisée à effectuer une action peut contraindre une entité plus privilégiée à le faire. En AWS, l'usurpation d'identité interservices peut entraîner un problème de confusion chez les adjoints. L'usurpation d'identité entre services peut se produire lorsqu'un service (le service appelant) appelle un autre service (le service appelé). Le service appelant peut être manipulé pour utiliser ses autorisations afin d'agir sur les ressources d'un autre client de sorte qu'il n'y aurait pas accès

autrement. Pour éviter cela, AWS fournit des outils qui vous aident à protéger vos données pour tous les services avec des principaux de service qui ont eu accès aux ressources de votre compte.

Nous recommandons d'utiliser les clés de contexte de condition globale `aws:SourceAccount` et les clés contextuelles `aws:SourceArn` dans les politiques de ressources afin de limiter les autorisations qui AWS IoT SiteWise accordent un autre service à la ressource. Si la valeur `aws:SourceArn` ne contient pas l'ID de compte, tel que l'Amazon Resource Name (ARN) d'un compartiment Amazon S3, vous devez utiliser les deux clés de contexte de condition globale pour limiter les autorisations. Si vous utilisez les deux clés de contexte de condition globale et que la valeur `aws:SourceArn` contient l'ID de compte, la valeur `aws:SourceAccount` et le compte dans la valeur `aws:SourceArn` doivent utiliser le même ID de compte lorsqu'ils sont utilisés dans la même instruction de politique.

- Utilisez `aws:SourceArn` si vous souhaitez qu'une seule ressource soit associée à l'accès entre services.
- Utilisez `aws:SourceAccount` si vous souhaitez autoriser l'association d'une ressource de ce compte à l'utilisation interservices.

La valeur de `aws:SourceArn` doit être la ressource AWS IoT SiteWise client associée à la `sts:AssumeRole` demande.

Le moyen le plus efficace de se protéger contre le problème de député confus consiste à utiliser la clé de contexte de condition globale `aws:SourceArn` avec l'ARN complet de la ressource. Si vous ne connaissez pas l'ARN complet de la ressource ou si vous spécifiez plusieurs ressources, utilisez la clé de contexte de condition globale `aws:SourceArn` avec des caractères génériques (*) pour les parties inconnues de l'ARN. Par exemple, `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`.

Example — Prévention adjointe confuse

L'exemple suivant montre comment utiliser les touches de contexte de condition `aws:SourceAccount` globale `aws:SourceArn` et globale AWS IoT SiteWise pour éviter le problème de confusion des adjoints.

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

Résolution des problèmes AWS IoT SiteWise d'identité et d'accès

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec AWS IoT SiteWise et AWS Identity and Access Management (IAM).

Rubriques

- Je ne suis pas autorisé à effectuer une action dans AWS IoT SiteWise
- Je ne suis pas autorisé à effectuer iam:PassRole
- Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes AWS IoT SiteWise ressources

Je ne suis pas autorisé à effectuer une action dans AWS IoT SiteWise

S'il vous AWS Management Console indique que vous n'êtes pas autorisé à effectuer une action, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni votre nom d'utilisateur et votre mot de passe.

L'exemple d'erreur suivant se produit lorsque l'utilisateur `mateojackson` IAM essaie d'utiliser la console pour afficher les détails d'un actif mais ne dispose pas des `iotsitewise:DescribeAsset` autorisations nécessaires.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 iotsitewise:DescribeAsset on resource: a1b2c3d4-5678-90ab-cdef-22222EXAMPLE
```

Dans ce cas, Mateo demande à son administrateur de mettre à jour ses stratégies pour lui permettre d'accéder à la ressource d'actif avec l'ID `a1b2c3d4-5678-90ab-cdef-22222EXAMPLE` à l'aide de l'action `iotsitewise:DescribeAsset`.

Je ne suis pas autorisé à effectuer **`iam:PassRole`**

Si vous recevez une erreur selon laquelle vous n'êtes pas autorisé à exécuter `iam:PassRole` l'action, vos stratégies doivent être mises à jour afin de vous permettre de transmettre un rôle à AWS IoT SiteWise.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour exécuter une action dans AWS IoT SiteWise. Toutefois, l'action nécessite que le service ait des autorisations accordées par une fonction de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

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

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes AWS IoT SiteWise ressources

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si ces fonctionnalités sont prises AWS IoT SiteWise en charge, consultezComment AWS IoT SiteWise fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des politiques basées sur les ressources pour l'accès entre comptes, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

Validation de conformité pour AWS IoT SiteWise

AWS IoT SiteWise ne fait l'objet d'aucun programme de AWS conformité.

Pour une liste des AWS services concernés par des programmes de conformité spécifiques, voir AWS Services concernés par programme de conformitéAWS . Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation AWS IoT SiteWise est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité Guides sur la sécurité et la conformité — Ces guides de déploiement abordent les considérations architecturales et fournissent les étapes à suivre pour déployer des environnements de base axés sur la sécurité et la conformité sur. AWS

- Livre blanc sur l'architecture pour la sécurité et la conformité HIPAA — Ce livre blanc décrit comment les entreprises peuvent créer des applications conformes à la loi HIPAA. AWS
- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- Évaluation des ressources à l'aide des règles énoncées dans le guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Ce AWS service fournit une vue complète de l'état de votre sécurité interne, AWS ce qui vous permet de vérifier votre conformité aux normes et aux meilleures pratiques du secteur de la sécurité.
- Dix règles d'or en matière de sécurité pour les solutions IoT industrielles — Ce billet de blog présente dix règles d'or qui vous aident à sécuriser vos systèmes de contrôle industriel (ICS), l'Internet des objets industriel (IIoT) et vos environnements cloud.
- Meilleures pratiques de sécurité pour l'OT dans le secteur manufacturier : ce livre blanc décrit les meilleures pratiques de sécurité pour concevoir, déployer et structurer ces charges de travail de fabrication hybrides sur site pour le cloud. AWS

Résilience dans AWS IoT SiteWise

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

AWS IoT SiteWise est entièrement géré et utilise des AWS services hautement disponibles et durables, tels qu'Amazon S3 et Amazon EC2. Pour garantir la disponibilité en cas d'interruption de la zone de disponibilité, AWS IoT SiteWise fonctionne sur plusieurs zones de disponibilité.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS mondiale.

Outre l'infrastructure AWS mondiale, AWS IoT SiteWise propose plusieurs fonctionnalités pour répondre à vos besoins en matière de résilience et de sauvegarde des données :

- Vous pouvez publier des mises à jour de la valeur des propriétés par le AWS IoT Core biais de messages MQTT, puis configurer des règles pour agir sur ces données. Grâce à cette fonctionnalité, vous pouvez sauvegarder des données dans d'autres AWS services tels qu'Amazon S3 et Amazon DynamoDB. Pour plus d'informations, consultez Interaction avec d'autres AWS services et Exportez des données vers Amazon S3 avec des notifications relatives aux propriétés des actifs.
- Vous pouvez utiliser les AWS IoT SiteWise `Get*` API pour récupérer et sauvegarder les données historiques des propriétés des actifs. Pour plus d'informations, consultez Interrogation des valeurs historiques de propriété de ressource.
- Vous pouvez utiliser les AWS IoT SiteWise `Describe*` API pour récupérer les définitions de vos ressources, telles que les actifs et les modèles. Vous pouvez sauvegarder ces définitions et les utiliser ultérieurement pour recréer vos ressources. Pour plus d'informations, consultez la page Référence de l'API AWS IoT SiteWise .

Sécurité de l'infrastructure dans AWS IoT SiteWise

En tant que service géré, AWS IoT SiteWise il est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder AWS IoT SiteWise via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

SiteWise Les passerelles Edge, qui s'exécutent sur AWS IoT Greengrass, utilisent des certificats X.509 et des clés cryptographiques pour se connecter et s'authentifier dans le cloud. AWS Pour plus d'informations, consultez la section Authentification et autorisation de l'appareil AWS IoT Greengrass dans le guide du AWS IoT Greengrass Version 1 développeur.

Analyse de la configuration et des vulnérabilités

Les flottes IoT sont composées d'un grand nombre d'appareils disposant de capacités diverses, d'une durée de vie longue et qui sont répartis géographiquement. Ces caractéristiques peuvent rendre la configuration des flottes complexe et source d'erreurs. Étant donné que les appareils ont généralement une puissance de traitement, une mémoire et un stockage limités, ils ne peuvent pas toujours prendre en charge le chiffrement et les autres mesures de sécurité. En outre, les appareils utilisent souvent des logiciels aux vulnérabilités connues. Ces facteurs font des parcs IoT une cible attractive pour les pirates informatiques et rend difficile la sécurisation de votre parc sur une base permanente.

AWS IoT Device Defender répond à ces défis en fournissant des outils permettant d'identifier les problèmes de sécurité et les écarts par rapport aux meilleures pratiques. Utilisez-le AWS IoT Device Defender pour analyser, auditer et surveiller les appareils connectés afin de détecter les comportements anormaux et d'atténuer les risques de sécurité. AWS IoT Device Defender peut auditer les flottes d'appareils pour s'assurer qu'elles respectent les meilleures pratiques de sécurité et détecter les comportements anormaux sur les appareils. Cela permet d'appliquer des politiques de sécurité cohérentes à l'ensemble de votre parc d' AWS IoT appareils et de réagir rapidement lorsque des appareils sont compromis. Pour plus d'informations, consultez AWS IoT Device Defender dans le Guide du développeur AWS IoT .

Si vous utilisez des passerelles SiteWise Edge pour ingérer des données vers le service, il est de votre responsabilité de configurer et de gérer l'environnement de votre passerelle SiteWise Edge. Cette responsabilité inclut la mise à niveau vers les dernières versions du logiciel système, AWS IoT Greengrass du logiciel et du AWS IoT SiteWise connecteur de la passerelle SiteWise Edge. Pour plus d'informations, voir Configurer le AWS IoT Greengrass noyau dans le guide du AWS IoT Greengrass Version 1 développeur etMise à niveau d'un connecteur.

Points de terminaison d'un VPC

Un point de terminaison VPC d'interface établit une connexion privée entre votre cloud privé virtuel (VPC) et. AWS IoT SiteWiseAWS PrivateLinkalimente les points de terminaison de l'interface, permettant un accès privé aux opérations de AWS IoT SiteWise l'API. Vous pouvez éviter d'avoir

besoin d'une passerelle Internet, d'un périphérique NAT, d'une connexion VPN ou AWS Direct Connect. Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour communiquer avec les opérations d' AWS IoT SiteWise API. Le trafic entre votre VPC et celui qui AWS IoT SiteWise ne quitte pas le AWS réseau.

Chaque point de terminaison d'interface est représenté par une ou plusieurs interfaces réseau Elastic dans vos sous-réseaux.

Avant de configurer un point de terminaison VPC d'interface pour AWS IoT SiteWise, consultez les propriétés et les limites du point de terminaison d'interface dans le guide de l'utilisateur Amazon VPC.

Pour de plus amples informations, consultez Points de terminaison VPC (AWS PrivateLink) dans le Guide de l'utilisateur Amazon VPC.

Opérations d'API prises en charge pour les points de terminaison VPC

AWS IoT SiteWise prend en charge les appels aux opérations AWS IoT SiteWise d'API suivantes depuis votre VPC :

- Pour toutes les opérations de l'API du plan de données, utilisez le point de terminaison suivant : Remplacez *region* par votre Région AWS

  ```
  data.iotsitewise.region.amazonaws.com
  ```

  Les opérations de l'API du plan de données sont les suivantes :

  - BatchGetAssetPropertyValeur
  - BatchGetAssetPropertyValueHistory
  - BatchPutAssetPropertyValeur
  - GetAssetPropertyAggregates
  - GetAssetPropertyValue
  - GetAssetPropertyValueHistoire
  - GetInterpolatedAssetPropertyValeurs
- Pour les opérations d'API du plan de contrôle que vous utilisez pour gérer les modèles d'actifs, les actifs, les passerelles SiteWise Edge, les balises et les configurations de compte, utilisez le point de terminaison suivant. *region*Remplacez-le par votre Région AWS.

  ```
  api.iotsitewise.region.amazonaws.com
  ```

Les opérations d'API du plan de contrôle prises en charge sont les suivantes :

- AssociateAssets
- CreateAsset
- CreateAssetModèle
- DeleteAsset
- DeleteAssetModèle
- DeleteDashboard
- DescribeAsset
- DescribeAssetModèle
- DescribeAssetPropriété
- DescribeDashboard
- DescribeLoggingOptions
- DisassociateAssets
- ListAssetModèles
- ListAssetRelations
- ListAssets
- ListAssociatedActifs
- PutLoggingOptions
- UpdateAsset
- UpdateAssetModèle
- UpdateAssetPropriété
- CreateGateway
- DeleteGateway
- DescribeDefaultEncryptionConfiguration
- DescribeGateway
- DescribeGatewayCapabilityConfiguration
- DescribeStorageConfiguration
- ListGateways
- ListTagsForResource
- UpdateGateway

- UpdateGatewayCapabilityConfiguration
- PutDefaultEncryptionConfiguration
- PutStorageConfiguration
- TagResource
- UntagResource

> **Note**
>
> Le point de terminaison VPC de l'interface pour les opérations d'API du plan de contrôle ne prend actuellement pas en charge les appels aux opérations d'API SiteWise Monitor suivantes :
>
> - BatchAssociateProjectAssets
> - BatchDisassociateProjectAssets
> - CreateAccessPolitique
> - CreateDashboard
> - CreatePortal
> - CreateProject
> - DeleteAccessPolitique
> - DeletePortal
> - DeleteProject
> - DescribeAccessPolitique
> - DescribePortal
> - DescribeProject
> - ListAccessPolitiques
> - ListDashboards
> - ListPortals
> - ListProjects
> - ListProjectActifs
> - UpdateAccessPolitique
> - UpdateDashboard
> - UpdatePortal

- UpdateProject

Création d'un point de terminaison de VPC d'interface pour AWS IoT SiteWise

Pour créer un point de terminaison VPC pour le AWS IoT SiteWise service, utilisez la console Amazon VPC ou le (). AWS Command Line Interface AWS CLI Pour plus d'informations, consultez Création d'un point de terminaison d'interface dans le Guide de l'utilisateur Amazon VPC.

Créez un point de terminaison VPC pour AWS IoT SiteWise en utilisant l'un des noms de service suivants :

- Pour les opérations de l'API du plan de données, utilisez le nom de service suivant :

```
com.amazonaws.region.iotsitewise.data
```

- Pour les opérations de l'API du plan de contrôle, utilisez le nom de service suivant :

```
com.amazonaws.region.iotsitewise.api
```

Accès AWS IoT SiteWise via un point de terminaison VPC d'interface

Lorsque vous créez un point de terminaison d'interface, nous générons des noms d'hôte DNS spécifiques au point de terminaison avec lesquels vous pouvez communiquer. AWS IoT SiteWise L'option DNS privé est activée par défaut. Pour plus d'informations, consultez la section Utilisation de zones hébergées privées dans le guide de l'utilisateur Amazon VPC.

Si vous activez le DNS privé pour le point de terminaison, vous pouvez envoyer des demandes d'API AWS IoT SiteWise via l'un des points de terminaison VPC suivants.

- Pour les opérations de l'API du plan de données, utilisez le point de terminaison suivant : Remplacez *la région* par votre Région AWS.

```
data.iotsitewise.region.amazonaws.com
```

- Pour les opérations de l'API du plan de contrôle, utilisez le point de terminaison suivant : Remplacez *la région* par votre Région AWS.

```
api.iotsitewise.region.amazonaws.com
```

Si vous désactivez le DNS privé pour le point de terminaison, vous devez effectuer les opérations suivantes pour y accéder AWS IoT SiteWise via le point de terminaison :

1. Spécifiez l'URL du point de terminaison VPC dans les demandes d'API.
   - Pour les opérations de l'API du plan de données, utilisez l'URL du point de terminaison suivant. Remplacez *vpc-endpoint-id et region par l'ID* de point de terminaison *et* la région de votre VPC.

     ```
     vpc-endpoint-id.data.iotsitewise.region.vpce.amazonaws.com
     ```

   - Pour les opérations de l'API du plan de contrôle, utilisez l'URL du point de terminaison suivant. Remplacez *vpc-endpoint-id et region par l'ID* de point de terminaison *et* la région de votre VPC.

     ```
     vpc-endpoint-id.api.iotsitewise.region.vpce.amazonaws.com
     ```

2. Désactive l'injection de préfixe d'hôte. Les AWS SDK AWS CLI et ajoutent différents préfixes d'hôte au point de terminaison du service lorsque vous appelez chaque opération d'API. Cette fonctionnalité fait en sorte que les AWS SDK AWS CLI et produisent des URL qui ne sont pas valides AWS IoT SiteWise lorsque vous spécifiez un point de terminaison VPC.

   > **Important**
   >
   > Vous ne pouvez pas désactiver l'injection de préfixe d'hôte dans le AWS CLI ou le AWS Tools for PowerShell. Cela signifie que si vous désactivez le DNS privé, vous ne pouvez pas utiliser ces outils pour accéder AWS IoT SiteWise via le point de terminaison VPC. Activez le DNS privé pour utiliser AWS CLI ou AWS Tools for PowerShell pour accéder AWS IoT SiteWise via le point de terminaison.

   Pour plus d'informations sur la façon de désactiver l'injection de préfixe d'hôte dans AWS les SDK, consultez les sections de documentation suivantes pour chaque SDK :

   - AWS SDK for C++
   - AWS SDK for Go

- AWS SDK for Go v2
- AWS SDK for Java
- AWS SDK for Java 2.x
- AWS SDK for JavaScript
- AWS SDK for .NET
- AWS SDK for PHP
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby

Pour plus d'informations, consultez Accès à un service via un point de terminaison d'interface dans le Guide de l'utilisateur Amazon VPC.

Création d'une politique de point de terminaison VPC pour AWS IoT SiteWise

Vous pouvez attacher une stratégie de point de terminaison à votre point de terminaison d'un VPC qui contrôle l'accès à AWS IoT SiteWise. La politique spécifie les informations suivantes :

- Le principal qui peut effectuer des opérations.
- Les opérations qui peuvent être effectuées.
- Les ressources sur lesquelles les opérations peuvent être effectuées.

Pour plus d'informations, consultez Contrôle de l'accès aux services avec points de terminaison d'un VPC dans le Guide de l'utilisateur Amazon VPC.

Exemple : politique de point de terminaison VPC pour les actions AWS IoT SiteWise

Voici un exemple de politique de point de terminaison pour AWS IoT SiteWise. Lorsqu'elle est attachée à un point de terminaison, cette politique accorde à l'utilisateur l'accès aux AWS IoT SiteWise actions répertoriées *iotsitewiseadmin*dans Compte AWS *123456789012* sur l'actif spécifié.

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

Bonnes pratiques de sécurité pour AWS IoT SiteWise

Cette rubrique présente les meilleures pratiques de sécurité pour AWS IoT SiteWise.

Utiliser les informations d'identification d'authentification sur vos serveurs OPC-UA

Exigez des informations d'identification d'authentification pour vous connecter à vos serveurs OPC-UA. Consultez la documentation de vos serveurs pour le faire. Ensuite, pour permettre à votre passerelle SiteWise Edge de se connecter à vos serveurs OPC-UA, ajoutez des secrets d'authentification du serveur à votre passerelle SiteWise Edge. Pour plus d'informations, consultez Configuration de l'authentification source.

Utiliser des modes de communication chiffrés pour vos serveurs OPC-UA

Choisissez un mode de sécurité des messages chiffrés non obsolète lorsque vous configurez vos sources OPC-UA pour votre passerelle Edge. SiteWise Cela permet de sécuriser vos données industrielles lorsqu'elles sont transférées de vos serveurs OPC-UA vers la passerelle SiteWise Edge. Pour plus d'informations, consultez Données en transit sur le réseau local et Configuration des sources de données.

Maintenez vos composants à jour

Si vous utilisez des passerelles SiteWise Edge pour ingérer des données vers le service, il est de votre responsabilité de configurer et de gérer l'environnement de votre passerelle SiteWise Edge. Cette responsabilité inclut la mise à niveau vers les dernières versions du logiciel système, AWS IoT Greengrass des logiciels et des connecteurs de la passerelle.

> **Note**
>
> Le connecteur AWS IoT SiteWise Edge stocke les secrets sur votre système de fichiers. Ces secrets contrôlent les personnes autorisées à consulter les données mises en cache dans votre passerelle SiteWise Edge. Il est vivement recommandé d'activer le chiffrement du disque ou du système de fichiers pour le système exécutant votre passerelle SiteWise Edge.

Chiffrez le système de fichiers de votre passerelle SiteWise Edge

Chiffrez et sécurisez votre passerelle SiteWise Edge afin que vos données industrielles soient sécurisées lorsqu'elles passent par la passerelle SiteWise Edge. Si votre passerelle SiteWise Edge possède un module de sécurité matériel, vous pouvez le configurer AWS IoT Greengrass pour sécuriser votre passerelle SiteWise Edge. Pour plus d'informations, consultez la section Intégration de la sécurité matérielle dans le Guide du AWS IoT Greengrass Version 1 développeur. Sinon, consultez la documentation de votre système d'exploitation pour savoir comment chiffrer et sécuriser votre système de fichiers.

Accès sécurisé à votre configuration Edge

Ne partagez pas le mot de passe de l'application Edge Console ou celui de l'application SiteWise Monitor. Ne mettez pas ce mot de passe dans un endroit où tout le monde peut le voir. Mettez en œuvre une politique saine de rotation des mots de passe en configurant une date d'expiration appropriée pour votre mot de passe.

Accorder aux utilisateurs de SiteWise Monitor les autorisations minimales possibles

Respectez le principe du moindre privilège en utilisant l'ensemble minimal d'autorisations de politique d'accès pour les utilisateurs de votre portail.

- Lorsque vous créez un portail, définissez un rôle qui autorise l'ensemble minimal d'actifs requis pour ce portail. Pour plus d'informations, consultez Utilisation des rôles de service pour AWS IoT SiteWise Monitor.
- Lorsque vous et les administrateurs de votre portail créez et partagez des projets, utilisez l'ensemble minimal d'actifs requis pour ce projet.
- Lorsqu'une identité n'a plus besoin d'accéder à un portail ou à un projet, supprimez-la de cette ressource. Si cette identité n'est plus applicable à votre organisation, supprimez-la de votre banque d'identités.

La meilleure pratique du moindre principe s'applique également aux rôles IAM. Pour plus d'informations, consultez Bonnes pratiques en matière de politiques.

Ne pas exposer d'informations sensibles

Vous devez empêcher l'enregistrement des informations d'identification et d'autres informations sensibles, telles que les informations personnellement identifiables (PII). Nous vous recommandons de mettre en œuvre les mesures de protection suivantes, même si l'accès aux journaux locaux sur une passerelle SiteWise Edge nécessite des privilèges root et que l'accès aux CloudWatch journaux nécessite des autorisations IAM.

- N'utilisez pas d'informations sensibles dans les noms, descriptions ou propriétés de vos ressources ou modèles.
- N'utilisez pas d'informations sensibles dans les noms de source ou de passerelle SiteWise Edge.
- N'utilisez pas d'informations sensibles dans les noms ou descriptions de vos portails, projets ou tableaux de bord.

Suivez les meilleures pratiques en matière de AWS IoT Greengrass sécurité

Suivez les meilleures pratiques de AWS IoT Greengrass sécurité pour votre passerelle SiteWise Edge. Pour plus d'informations, consultez la section Bonnes pratiques en matière de sécurité dans le guide du AWS IoT Greengrass Version 1 développeur.

Consultez aussi

- Bonnes pratiques en matière de sécurité décrites dans le guide du AWS IoT développeur
- Dix règles d'or en matière de sécurité pour les solutions IoT industrielles

Connexion et surveillance AWS IoT SiteWise

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité AWS IoT SiteWise et des performances de vos autres AWS solutions. AWS IoT SiteWise prend en charge les outils de surveillance suivants pour surveiller le service, signaler un problème et prendre des mesures automatiques le cas échéant :

- Amazon CloudWatch surveille vos AWS ressources et les applications que vous utilisez AWS en temps réel. Collectez et suivez les métriques, créez des tableaux de bord personnalisés et définissez des alarmes qui vous avertissent ou prennent des mesures lorsqu'une métrique spécifiée atteint un certain seuil. Par exemple, vous pouvez CloudWatch suivre l'utilisation du processeur ou d'autres indicateurs de vos instances Amazon EC2 et lancer automatiquement de nouvelles instances en cas de besoin. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.
- Amazon CloudWatch Logs surveille, stocke et accède à vos fichiers journaux depuis les passerelles SiteWise Edge et d'autres sources. CloudTrail CloudWatch Les journaux peuvent surveiller les informations contenues dans les fichiers journaux et vous avertir lorsque certains seuils sont atteints. Vous pouvez également archiver vos données de journaux dans une solution de stockage hautement durable. Pour plus d'informations, consultez le guide de l'utilisateur d'Amazon CloudWatch Logs.
- AWS CloudTrailcapture les appels d'API et les événements connexes effectués par ou au nom de votre AWS compte. CloudTrail Transmet ensuite les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. Pour de plus amples informations, veuillez consulter le Guide de l'utilisateur AWS CloudTrail.

Rubriques

- Surveillance avec Amazon CloudWatch Logs
- Surveillance des journaux de la passerelle SiteWise Edge
- Surveillance AWS IoT SiteWise à l'aide des CloudWatch métriques Amazon
- Journalisation des appels d' AWS IoT SiteWise API avec AWS CloudTrail

Surveillance avec Amazon CloudWatch Logs

Configurez AWS IoT SiteWise pour consigner les informations dans CloudWatch les journaux afin de surveiller et de dépanner le service.

Lorsque vous utilisez la AWS IoT SiteWise console, AWS IoT SiteWise crée un rôle lié au service qui permet au service de consigner des informations en votre nom. Si vous n'utilisez pas la AWS IoT SiteWise console, vous devez créer manuellement un rôle lié à un service pour recevoir les journaux. Pour plus d'informations, consultez Création d'un rôle lié à un service pour AWS IoT SiteWise.

Vous devez disposer d'une politique de ressources permettant de AWS IoT SiteWise placer les événements du journal dans des CloudWatch flux. Pour créer et mettre à jour une politique de ressources pour CloudWatch les journaux, exécutez la commande suivante. Remplacez *logging-policy-name*par le nom de la politique à créer.

```
aws logs put-resource-policy --policy-name logging-policy-name --policy-
document "{ \"Version\": \"2012-10-17\", \"Statement\": [ { \"Sid\":
 \"IoTSiteWiseToCloudWatchLogs\", \"Effect\": \"Allow\", \"Principal\": { \"Service\":
 [ \"iotsitewise.amazonaws.com\" ] }, \"Action\":\"logs:PutLogEvents\", \"Resource\":
 \"*\" } ] }"
```

CloudWatch Logs prend également en charge les clés contextuelles de SourceAccount condition aws : SourceArn et aws :. Ces clés de contexte de condition sont facultatives.

Pour créer ou mettre à jour une politique de ressources qui AWS IoT SiteWise permet de placer uniquement les journaux associés à la AWS IoT SiteWise ressource spécifiée dans des CloudWatch flux, exécutez la commande et procédez comme suit :

- Remplacez *logging-policy-name*par le nom de la politique à créer.
- Remplacez *Source-ARN* par l'ARN de votre AWS IoT SiteWise ressource, tel qu'un modèle d'actif ou un actif. Pour trouver l'ARN de chaque type de AWS IoT SiteWise ressource, consultez la section Types de ressources définis par AWS IoT SiteWise dans la référence d'autorisation de service.
- Remplacez *Account-ID* par l'ID de AWS compte associé à la ressource spécifiée AWS IoT SiteWise .

```
aws logs put-resource-policy --policy-name logging-policy-name --policy-
document "{ \"Version\": \"2012-10-17\", \"Statement\": [ { \"Sid\":
```

```
 \"IoTSiteWiseToCloudWatchLogs\", \"Effect\": \"Allow\", \"Principal\": { \"Service
\": [ \"iotsitewise.amazonaws.com\" ] }, \"Action\":\"logs:PutLogEvents\", \"Resource
\": \"*\", \"Condition\":{\"StringLike\":{\"aws:SourceArn\":[\"source-ARN\"],
\"aws:SourceAccount\":[\"account-ID\"]}}}]}"
```

Par défaut, AWS IoT SiteWise n'enregistre pas les informations dans CloudWatch Logs. Pour activer la journalisation, choisissez un niveau de journalisation autre que Disabled (`OFF`). AWS IoT SiteWise prend en charge les niveaux de journalisation suivants :

- `OFF`— La journalisation est désactivée.
- `ERROR`— Les erreurs sont enregistrées.
- `INFO`— Les erreurs et les messages d'information sont enregistrés.

Vous pouvez configurer les passerelles SiteWise Edge pour enregistrer les informations dans CloudWatch Logs through AWS IoT Greengrass. Pour plus d'informations, consultez Surveillance des journaux de la passerelle SiteWise Edge.

Vous pouvez également configurer AWS IoT Core pour consigner les informations dans les CloudWatch journaux si vous dépannez une action de AWS IoT SiteWise règle. Pour plus d'informations, consultez Résolution des problèmes liés à une action de AWS IoT SiteWise règle.

Table des matières

- Gestion de la connexion AWS IoT SiteWise
  - Trouver votre niveau de journalisation
  - Modification de votre niveau de journalisation
- Exemple : entrées de fichier AWS IoT SiteWise journal

Gestion de la connexion AWS IoT SiteWise

Utilisez la AWS IoT SiteWise console ou AWS CLI pour les tâches de configuration de journalisation suivantes.

Trouver votre niveau de journalisation

Console

Suivez la procédure suivante pour trouver votre niveau de journalisation actuel dans la console AWS IoT SiteWise .

Pour trouver votre niveau de AWS IoT SiteWise journalisation actuel

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation de gauche, choisissez Options de journalisation.

   L'état de journalisation actuel apparaît sous Statut de journalisation. Si la journalisation est activée, le niveau de journalisation actuel apparaît sous Niveau de verbosité.

AWS CLI

Exécutez la commande suivante pour trouver votre niveau de AWS IoT SiteWise journalisation actuel avec le AWS CLI.

```
aws iotsitewise describe-logging-options
```

L'opération renvoie une réponse qui contient votre niveau de journalisation au format suivant.

```
{
  "loggingOptions": {
    "level": "String"
  }
}
```

Modification de votre niveau de journalisation

Utilisez la procédure suivante pour modifier votre niveau de journalisation dans la AWS IoT SiteWise console ou à l'aide de AWS CLI.

Console

Pour modifier votre niveau de AWS IoT SiteWise journalisation

1. Accédez à la console AWS IoT SiteWise.
2. Dans le panneau de navigation de gauche, choisissez Options de journalisation.
3. Choisissez Modifier.
4. Choisissez le niveau de verbosité à activer.
5. Choisissez Enregistrer.

AWS CLI

Exécutez la AWS CLI commande suivante pour modifier votre niveau de AWS IoT SiteWise journalisation. Remplacez le *niveau de journalisation* par le niveau de journalisation souhaité.

```
aws iotsitewise put-logging-options --logging-options level=logging-level
```

Exemple : entrées de fichier AWS IoT SiteWise journal

Chaque entrée de AWS IoT SiteWise journal inclut des informations sur l'événement et des ressources pertinentes pour cet événement, afin que vous puissiez comprendre et analyser les données du journal.

L'exemple suivant montre une entrée CloudWatch Logs qui AWS IoT SiteWise se connecte lorsque vous créez avec succès un modèle d'actif.

```
{
  "eventTime": "2020-05-05T00:10:22.902Z",
  "logLevel": "INFO",
  "eventType": "AssetModelCreationSuccess",
  "message": "Successfully created asset model.",
  "resources": {
    "assetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE"
  }
}
```

Surveillance des journaux de la passerelle SiteWise Edge

Vous pouvez configurer votre passerelle AWS IoT SiteWise Edge pour enregistrer les informations dans Amazon CloudWatch Logs ou dans le système de fichiers local.

Rubriques

- Utilisation d'Amazon CloudWatch Logs
- Utilisation des journaux de service
- Utilisation des journaux d'événements

Utilisation d'Amazon CloudWatch Logs

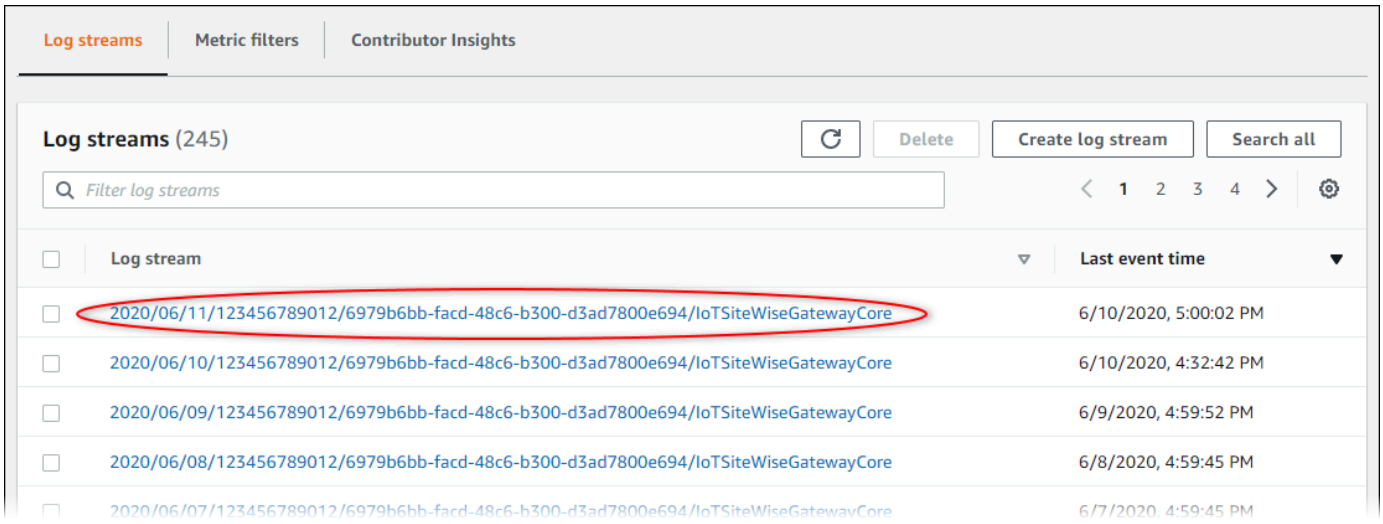
Vous pouvez configurer votre passerelle SiteWise Edge pour envoyer des CloudWatch journaux à Logs. Pour plus d'informations, voir Activer la journalisation des CloudWatch journaux dans le guide du AWS IoT Greengrass Version 2 développeur.

Pour configurer les CloudWatch journaux et y accéder (console)

1. Accédez à la console CloudWatch.
2. Dans le panneau de navigation, choisissez Groupes de journaux.
3. Vous pouvez trouver les journaux des AWS IoT SiteWise composants dans les groupes de journaux suivants :

   - `/aws/greengrass/UserComponent/region/aws.iot.SiteWiseEdgeCollectorOpcua`— Les journaux du composant de la passerelle SiteWise Edge qui collecte les données à partir des sources OPC-UA de la passerelle SiteWise Edge.
   - `/aws/greengrass/UserComponent/region/aws.iot.SiteWiseEdgePublisher`— Les journaux du composant de la passerelle SiteWise Edge qui publie les flux de données OPC-UA vers. AWS IoT SiteWise

   Choisissez le groupe de journaux pour la fonction à déboguer.
4. Choisissez un flux de journal dont le nom se termine par le nom de votre AWS IoT Greengrass groupe. Par défaut, CloudWatch affiche le flux de journal le plus récent en premier.



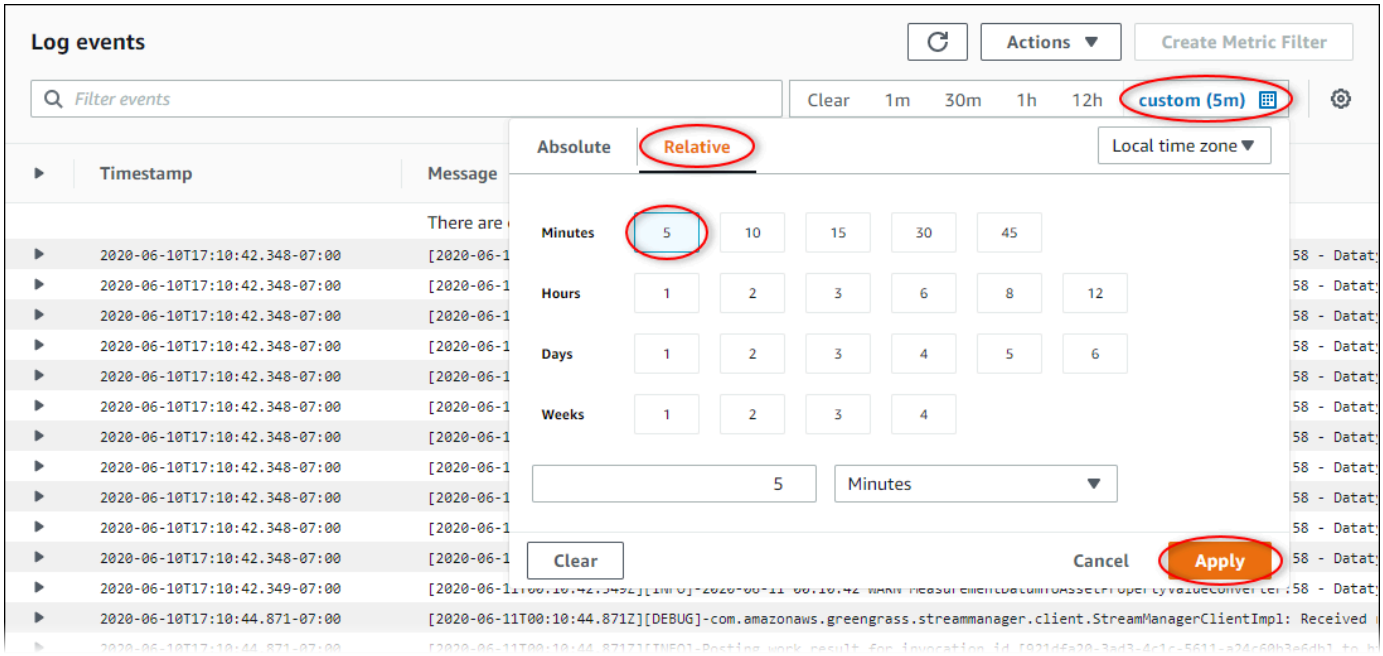
5. Pour afficher les journaux des 5 dernières minutes, procédez comme suit :

a. Choisissez personnalisé dans le coin supérieur droit.

b. Choisissez Relatif.

c. Choisissez 5 minutes.

d. Choisissez Appliquer.



6. (Facultatif) Pour afficher moins de journaux, vous pouvez choisir 1 minute dans le coin supérieur droit.

7. Faites défiler jusqu'au bas des entrées du journal pour afficher les journaux les plus récents.

Utilisation des journaux de service

SiteWise Les périphériques Edge Gateway incluent des fichiers journaux de service pour aider à résoudre les problèmes. Les sections suivantes vous aideront à trouver et à utiliser les fichiers journaux de service pour les composants AWS IoT SiteWise OPC-UA Collector et AWS IoT SiteWise Publisher.

AWS IoT SiteWise Fichier journal du service OPC-UA Collector

Le composant AWS IoT SiteWise OPC-UA Collector utilise le fichier journal suivant.

Linux

```
/greengrass/v2/logs/aws.iot.SiteWiseEdgeCollectorOpcua.log
```

Windows

```
C:\greengrass\v2\logs\aws.iot.SiteWiseEdgeCollectorOpcua.log
```

Pour consulter les journaux de ce composant

- Exécutez la commande suivante sur le périphérique principal pour afficher le fichier journal de ce composant en temps réel. Remplacez */greengrass/v2C:\greengrass\v2* par le chemin d'accès au dossier AWS IoT Greengrass racine.

  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 Fichier journal du service Publisher

Le composant AWS IoT SiteWise Publisher utilise le fichier journal suivant.

Linux

```
/greengrass/v2/logs/aws.iot.SiteWiseEdgePublisher.log
```

Windows

```
C:\greengrass\v2\logs\aws.iot.SiteWiseEdgePublisher.log
```

Pour consulter les journaux de ce composant

- Exécutez la commande suivante sur le périphérique principal pour afficher le fichier journal de ce composant en temps réel. Remplacez */greengrass/v2C:\greengrass\v2* par le chemin d'accès au dossier AWS IoT Greengrass racine.

  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
  ```

Utilisation des journaux d'événements

SiteWise Les périphériques Edge Gateway incluent des fichiers journaux d'événements pour aider à résoudre les problèmes. Les sections suivantes vous aideront à trouver et à utiliser les fichiers journaux d'événements pour les composants AWS IoT SiteWise OPC-UA Collector et AWS IoT SiteWise Publisher.

AWS IoT SiteWise Journaux d'événements OPC-UA Collector

Le composant AWS IoT SiteWise OPC-UA Collector inclut un journal des événements pour aider les clients à identifier et à résoudre les problèmes. Le fichier journal est distinct du fichier journal local et se trouve à l'emplacement suivant. Remplacez */greengrass/v2C:\greengrass\v2* par le chemin d'accès au dossier AWS IoT Greengrass racine.

Linux

```
/greengrass/v2/work/aws.iot.SiteWiseEdgeCollectorOpcua/logs/
IotSiteWiseOpcUaCollectorEvents.log
```

Windows

```
C:\greengrass\v2\work\aws.iot.SiteWiseEdgeCollectorOpcua\logs
\IotSiteWiseOpcUaCollectorEvents.log
```

Ce journal contient des informations détaillées et des instructions de dépannage. Des informations de dépannage sont fournies en même temps que les diagnostics, avec une description de la manière de remédier au problème, et parfois avec des liens vers des informations supplémentaires. Les informations de diagnostic incluent les éléments suivants :

- Niveau de gravité
- Horodatage
- Informations supplémentaires spécifiques à l'événement

Example Exemple de journal

```
dataSourceConnectionSuccess:
  Summary: Successfully connected to OpcUa server
  Level: INFO
  Timestamp: '2023-06-15T21:04:16.303Z'
  Description: Successfully connected to the data source.
  AssociatedMetrics:
  - Name: FetchedDataStreams
    Description: The number of fetched data streams for this data source
    Value: 1.0
    Namespace: IoTSiteWise
    Dimensions:
    - Name: SourceName
      Value: SourceName{value=OPC-UA Server}
    - Name: ThingName
      Value: test-core
  AssociatedData:
  - Name: DataSourceTrace
    Description: Name of the data source
    Data:
    - OPC-UA Server
  - Name: EndpointUri
    Description: The endpoint to which the connection was attempted.
    Data:
    - '"opc.tcp://10.0.0.1:1234"'
```

AWS IoT SiteWise Journaux d'événements de l'éditeur

Le composant AWS IoT SiteWise Publisher inclut un journal des événements pour aider les clients à identifier et à résoudre les problèmes. Le fichier journal est distinct du fichier journal local et se trouve

à l'emplacement suivant. Remplacez */greengrass/v2C:\greengrass\v2* par le chemin d'accès au dossier AWS IoT Greengrass racine.

Linux

```
/greengrass/v2/work/aws.iot.SiteWiseEdgePublisher/logs/
IotSiteWisePublisherEvents.log
```

Windows

```
C:\greengrass\v2\work\aws.iot.SiteWiseEdgePublisher\logs
\IotSiteWisePublisherEvents.log
```

Ce journal contient des informations détaillées et des instructions de dépannage. Des informations de dépannage sont fournies en même temps que les diagnostics, avec une description de la manière de remédier au problème, et parfois avec des liens vers des informations supplémentaires. Les informations de diagnostic incluent les éléments suivants :

- Niveau de gravité
- Horodatage
- Informations supplémentaires spécifiques à l'événement

Example Exemple de journal

```
accountBeingThrottled:
  Summary: Data upload speed slowed due to quota limits
  Level: WARN
  Timestamp: '2023-06-09T21:30:24.654Z'
  Description: The IoT SiteWise Publisher is limited to the "Rate of data points
 ingested"
    quota for a customers account. See the associated documentation and associated
    metric for the number of requests that were limited for more information. Note
    that this may be temporary and not require any change, although if the issue
 continues
    you may need to request an increase for the mentioned quota.
  FurtherInformation:
  - https://docs.aws.amazon.com/iot-sitewise/latest/userguide/quotas.html
  - https://docs.aws.amazon.com/iot-sitewise/latest/userguide/troubleshooting-
gateway.html#gateway-issue-data-streams
```

```
  AssociatedMetrics:
  - Name: TotalErrorCount
    Description: The total number of errors of this type that occurred.
    Value: 327724.0
  AssociatedData:
  - Name: AggregatePropertyAliases
    Description: The aggregated property aliases of the throttled data.
    FileLocation: /greengrass/v2/work/aws.iot.SiteWiseEdgePublisher/./logs/data/
AggregatePropertyAliases_1686346224654.log
```

Surveillance AWS IoT SiteWise à l'aide des CloudWatch métriques Amazon

Vous pouvez surveiller AWS IoT SiteWise l'utilisation CloudWatch, qui collecte les données brutes et les transforme en indicateurs lisibles en temps quasi réel. Ces statistiques sont enregistrées pour une durée de 15 mois ; par conséquent, vous pouvez accéder aux informations historiques et acquérir un meilleur point de vue de la façon dont votre service ou application web s'exécute. Vous pouvez également définir des alarmes qui surveillent certains seuils et envoient des notifications ou prennent des mesures lorsque ces seuils sont atteints. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.

AWS IoT SiteWise publie les métriques et les dimensions répertoriées dans les sections ci-dessous dans l'espace de `AWS/IoTSiteWise` noms.

> **Tip**
>
> AWS IoT SiteWise publie des statistiques à une minute d'intervalle. Lorsque vous visualisez ces statistiques sous forme de graphiques dans la CloudWatch console, nous vous recommandons de choisir une période d'une minute. Cela vous permet de voir la résolution la plus élevée disponible de vos données de métrique.

Rubriques

- AWS IoT Greengrass Version 2 métriques de passerelle
- AWS IoT Greengrass Version 1 métriques de passerelle

AWS IoT Greengrass Version 2 métriques de passerelle

AWS IoT SiteWise publie les métriques de passerelle SiteWise Edge suivantes. Toutes les métriques de la passerelle SiteWise Edge sont publiées à une minute d'intervalle.

SiteWise Mesures relatives à la passerelle Edge

Métrique	Description
`Gateway.CpuUsage`	L'utilisation du processeur d'une passerelle SiteWise Edge. Unité : pourcentage Dimension : Aucune
`Gateway.TotalDiskSpace`	Espace disque total d'une passerelle SiteWise Edge. Unité : octets Dimension : Aucune
`Gateway.UsedDiskSpace`	L'espace disque utilisé par une passerelle SiteWise Edge. Unité : octets Dimension : Aucune
`Gateway.AvailableDiskSpace`	L'espace disque disponible d'une passerelle SiteWise Edge. Unité : octets Dimension : Aucune
`Gateway.UsedPercentageDiskSpace`	Pourcentage d'espace disque utilisé par une passerelle SiteWise Edge. Unité : octets

Métrique	Description
	Dimension : Aucune
`Gateway.TotalMemory`	Mémoire totale d'une passerelle SiteWise Edge. Unité : octets Dimension : Aucune
`Gateway.UsedMemory`	Mémoire utilisée d'une passerelle SiteWise Edge. Unité : octets Dimension : Aucune
`Gateway.AvailableMemory`	Mémoire disponible d'une passerelle SiteWise Edge. Unité : octets Dimension : Aucune
`Gateway.UsedPercentageMemory`	Pourcentage de mémoire utilisé par une passerelle SiteWise Edge. Unité : octets Dimension : Aucune
`Gateway.CloudConnectivity`	État de connectivité cloud d'une passerelle SiteWise Edge. Unité : aucune Dimension : GatewayId

Métrique	Description
`Gateway.SWE.Component.RunningStatus`	État de fonctionnement des composants sur une passerelle SiteWise Edge. Unité : aucune Dimension : GatewayId

Métriques du collecteur OPC-UA

Métrique	Description
`OpcUaCollector.Heartbeat`	Généré toutes les minutes pour chaque source OPC-UA (`sourceName`) connectée à une passerelle SiteWise Edge (`gatewayId`). Unité : Nombre (1 représentant la source est connectée et 0 représentant la source est déconnectée.) Dimensions : GatewayId, SourceName
`OpcUaCollector.ActiveDataStreamCount`	Nombre de flux de données auxquels une passerelle SiteWise Edge (`gatewayId`) s'est abonnée pour une source OPC-UA ()`sourceName` . Unité : nombre GatewayIdDimensioni : SourceName, PropertyGroup
`OpcUaCollector.IncomingValuesCount`	Le nombre de points de données qu'une passerelle SiteWise Edge (`gatewayId`) a reçus pour une source OPC-UA (`sourceName`), générés chaque minute. Unité : nombre

Métrique	Description
	GatewayIdDimensioni : SourceName, PropertyGroup
`OpcUaCollector.IncomingValuesError`	Nombre de points de données qu'une passerelle SiteWise Edge (`gatewayId`) reçoit d'une source OPC-UA (`sourceName`) qui ne sont pas des valeurs valides. Ces points de données ne sont pas ingérés par le OpcUa collecteur, ils sont générés toutes les minutes. Unité : nombre GatewayIdDimensioni : SourceName, PropertyGroup
`OpcUaCollector.ConversionErrors`	Nombre de points de données reçus par une passerelle SiteWise Edge (`gatewayId`) pour une source OPC-UA (`sourceName`) qui ont entraîné des erreurs de conversion lors de l'envoi des données. AWS IoT SiteWise Ces points de données ne seront pas ingérés par OpcUa Collector. Unité : nombre Dimensions : GatewayId, SourceName

AWS IoT SiteWise métriques du processeur

Métrique	Description
`Gateway.DataProcessor.IngestionSuccess`	Le nombre de points de données qui ont été ingérés avec succès, généré chaque minute. Unité : nombre Dimensions : Aucune

Métrique	Description
`Gateway.DataProcessor.IngestionThrottled`	Le nombre de points de données qui ont été limités, générés chaque minute. Unité : nombre Dimensions : ThrottledAt
`Gateway.DataProcessor.MeasurementRejected`	Le nombre de mesures rejetées, généré chaque minute. Unité : nombre Dimensions : raison
`Gateway.DataProcessor.MeasurementUnmodeled`	Le nombre de mesures non modélisées, générées chaque minute. Unité : nombre Dimensions : raison
`Gateway.DataProcessor.MessagesRemaining`	Le nombre de messages restant dans un flux, généré chaque minute. Unité : nombre Dimensions : StreamName
`Gateway.DataProcessor.ProcessingError`	Le nombre d'erreurs de traitement, générées chaque minute. Unité : nombre Dimensions : raison

Métrique	Description
`IoTSiteWiseProcessor.IsConnectedToMqttBroker`	Généré chaque minute par le processeur de la passerelle SiteWise Edge. Unité : 1 (1 représentant le processeur est connecté à un broker MQTT.) Dimensions : GatewayId
`IoTSiteWiseProcessor.NumberOfSubscriptionsToMqttBroker`	Le nombre de sujets souscrits au broker MQTT par le processeur, généré chaque minute. Un sujet joker à plusieurs niveaux est compté pour 1. Unité : nombre Dimensions : GatewayId
`IoTSiteWiseProcessor.NumberOfUniqueMqttTopicsReceived`	Le nombre de sujets uniques reçus par le processeur par le broker MQTT, générés chaque minute. Unité : nombre Dimensions : GatewayId
`IoTSiteWiseProcessor.MqttMessageReceivedSuccessCount`	Le nombre de messages reçus avec succès par le processeur en provenance du broker MQTT, générés chaque minute. Unité : nombre Dimensions : GatewayId

Métrique	Description
`IoTSiteWiseProcessor.MqttReceivedSuccessBytes`	Le nombre d'octets de données de message reçus avec succès par le processeur en provenance du broker MQTT, générés chaque minute. Unité : nombre Dimensions : GatewayId

AWS IoT SiteWise statistiques relatives aux éditeurs

Métrique	Description
`IoTSiteWisePublisher.Heartbeat`	Généré chaque minute par le Publisher dans la passerelle SiteWise Edge. Unité : 1 (1 représentant l'éditeur est en cours d'exécution et il manque le point de données indiquant que l'éditeur n'est pas en cours d'exécution.) Dimensions : GatewayId
`IoTSiteWisePublisher.PublishSuccessCount`	Le nombre de points de données qu'une passerelle SiteWise Edge (`GatewayId`) a publiés avec succès dans le cloud, générés chaque minute. Unité : nombre Dimensions : GatewayId
`IoTSiteWisePublisher.PublishFailureCount`	Le nombre de points de données qu'une passerelle SiteWise Edge (`GatewayId`) n'a pas réussi à publier, généré chaque minute. Unité : nombre

Métrique	Description
	Dimensions : GatewayId
`IoTSiteWisePublisher.PublishRejectedCount`	Le nombre de points de données rejetés par une passerelle SiteWise Edge (`GatewayId`) depuis le cloud, générés chaque minute. Unité : nombre Dimensions : GatewayId
`IoTSiteWisePublisher.DroppedCount`	Nombre de points de données déposés par une passerelle SiteWise Edge (`GatewayId`) et non publiés dans le cloud, générés chaque minute. Unité : nombre Dimensions : GatewayId
`IoTSiteWisePublisher.IsConnectedToMqttBroker`	Généré chaque minute par le Publisher dans la passerelle SiteWise Edge. Unité : 1 (1 représentant l'éditeur est connecté à un broker MQTT.) Dimensions : GatewayId
`IoTSiteWisePublisher.NumberOfSubscriptionsToMqttBroker`	Le nombre de sujets souscrits au broker MQTT par l'éditeur, généré chaque minute. Un sujet joker à plusieurs niveaux est compté pour 1. Unité : nombre Dimensions : GatewayId

Métrique	Description
`IoTSiteWisePublisher.NumberOfUniqueMqttTopicsReceived`	Le nombre de sujets uniques reçus par l'éditeur par le courtier MQTT, générés chaque minute. Unité : nombre Dimensions : GatewayId
`IoTSiteWisePublisher.MqttMessageReceivedSuccessCount`	Le nombre de messages reçus avec succès par l'éditeur en provenance du broker MQTT, générés chaque minute. Unité : nombre Dimensions : GatewayId
`IoTSiteWisePublisher.MqttReceivedSuccessBytes`	Le nombre d'octets de données de message reçus avec succès par l'éditeur en provenance du broker MQTT, générés chaque minute. Unité : nombre Dimensions : GatewayId

AWS IoT Greengrass Version 1 métriques de passerelle

AWS IoT SiteWise publie les métriques de passerelle SiteWise Edge suivantes. Toutes les métriques de la passerelle SiteWise Edge sont publiées à une minute d'intervalle.

> **Important**
>
> Pour recevoir les métriques de la passerelle SiteWise Edge, vous devez utiliser au moins la version 6 du AWS IoT SiteWise connecteur sur votre passerelle SiteWise Edge. Pour plus d'informations, consultez le collecteur AWS IoT SiteWise OPC-UA dans le guide du AWS IoT Greengrass Version 1 développeur.

SiteWise Mesures relatives à la passerelle Edge

Métrique	Description
`Gateway.Heartbeat`	Généré toutes les minutes pour chaque passerelle SiteWise Edge (`gatewayId`) connectée. Unité : 1 (1 représentant la passerelle SiteWise Edge est active et manquant, le point de données représentant la passerelle SiteWise Edge est déconnecté du cloud.) Dimension : GatewayId
`Gateway.PublishSuccessCount`	Nombre de points de données publiés avec succès par une passerelle SiteWise Edge (`gatewayId`). Unité : nombre Dimension : GatewayId
`Gateway.PublishFailureCount`	Nombre de points de données qu'une passerell e SiteWise Edge (`gatewayId`) n'a pas réussi à publier. Cette métrique compte les erreurs résultant des appels de la passerelle SiteWise Edge à l'BatchPutAssetPropertyValueopération. Pour plus d'informations sur la résolution des problèmes liés aux passerelles SiteWise Edge, consultezRésolution des problèmes liés à une passerelle SiteWise Edge. Unité : nombre Dimension : GatewayId

Métrique	Description
`Gateway.ProcessFailureCount`	Nombre de points de données qu'une passerelle SiteWise Edge (`gatewayId `) n'a pas pu traiter. Cette métrique compte les erreurs qui se produisent entre la passerelle SiteWise Edge et les sources de la passerelle SiteWise Edge, y compris les erreurs signalées par les sources. Pour plus d'informations sur la résolution des problèmes liés aux passerelles SiteWise Edge, consultezRésolution des problèmes liés à une passerelle SiteWise Edge. Unité : nombre Dimension : GatewayId
`Gateway.PublishRejectedCount`	Nombre de points de données rejetés par une passerelle SiteWise Edge (`gatewayId `). Unité : nombre Dimension : GatewayId

Métriques liées à l'OPC-UA

Métrique	Description
`OPCUACollector.Heartbeat`	Généré toutes les minutes pour chaque source OPC-UA (`sourceName `) connectée à une passerelle SiteWise Edge (`gatewayId `). Unité : Nombre (1 représentant la source est connectée et 0 représentant la source est déconnectée.) Dimensions : GatewayId, SourceName

Métrique	Description
`OPCUACollector.ActiveDataStreamCount`	Nombre de flux de données auxquels une passerelle SiteWise Edge (`gatewayId`) s'est abonnée pour une source OPC-UA (`sourceName`). Unité : nombre GatewayIdDimensioni : SourceName, PropertyGroup
`OpcUaCollector.IncomingValuesCount`	Le nombre de points de données qu'une passerelle SiteWise Edge (`gatewayId`) a reçus pour une source OPC-UA (`sourceName`), générés chaque minute. Unité : nombre GatewayIdDimensioni : SourceName, PropertyGroup
`OpcUaCollector.IncomingValuesError`	Nombre de points de données qu'une passerelle SiteWise Edge (`gatewayId`) a reçus d'une source OPC-UA (`sourceName`) qui ne sont pas des valeurs valides. Ces points de données ne seront pas ingérés par le OpcUa collecteur, générés toutes les minutes. Unité : nombre GatewayIdDimensioni : SourceName, PropertyGroup

Métrique	Description
`OpcUaCollector.ConversionErrors`	Nombre de points de données reçus par une passerelle SiteWise Edge (`gatewayId`) pour une source OPC-UA (`sourceName`) qui ont entraîné des erreurs de conversion lors de l'envoi des données. AWS IoT SiteWise Ces points de données ne seront pas ingérés par OpcUa Collector. Unité : nombre Dimensions : GatewayId, SourceName

Métriques liées à l'EIP

Métrique	Description
`EIPCollector.Heartbeat`	Généré toutes les minutes pour chaque source EIP (`sourceName`) connectée à une passerell e SiteWise Edge (`gatewayId`). Unité : 1 (1 représentant la source est connectée et il manque le point de données représentant la source est déconnecté.) Dimensions : GatewayId, SourceName
`EIPCollector.IncomingValuesCount`	Nombre de flux de données auxquels une passerelle SiteWise Edge (`gatewayId`) est abonnée pour une source EIP (`sourceName`). Unité : nombre Dimensions : GatewayId, SourceName
`EIPCollector.ActiveDataStre amCount`	Le nombre de points de données qu'une passerelle SiteWise Edge (`gatewayId`) a reçus pour une source EIP (`sourceName`).

Métrique	Description
	Unité : nombre Dimensions : GatewayId, SourceName

Métriques liées à Modbus

Métrique	Description
`ModbusTCPCollector.Heartbeat`	Généré toutes les minutes pour chaque source Modbus (`sourceName`) connectée à une passerelle SiteWise Edge (`gatewayId`). Unité : 1 (1 représentant la source Modbus est connectée et il manque le point de données représentant la source est déconnecté.) Dimensions : GatewayId, SourceName
`ModbusTCPCollector.IncomingValuesCount`	Nombre de flux de données auxquels une passerelle SiteWise Edge (`gatewayId`) est abonnée pour une source Modbus (`sourceName`). Unité : nombre Dimensions : GatewayId, SourceName
`ModbusTCPCollector.ActiveDataStreamCount`	Le nombre de points de données qu'une passerelle SiteWise Edge (`gatewayId`) a reçus pour une source Modbus (`sourceName`). Unité : nombre Dimensions : GatewayId, SourceName

Journalisation des appels d' AWS IoT SiteWise API avec AWS CloudTrail

AWS IoT SiteWise est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans AWS IoT SiteWise. CloudTrail capture les appels d'API AWS IoT SiteWise sous forme d'événements. Les appels capturés incluent des appels provenant de la AWS IoT SiteWise console et des appels de code vers les opérations de l' AWS IoT SiteWise API. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris les événements pour AWS IoT SiteWise. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite AWS IoT SiteWise, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires.

Pour plus d'informations CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

AWS IoT SiteWise informations dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité événementielle prise en charge se produit dans AWS IoT SiteWise, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements AWS de service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre AWS compte. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre AWS compte, y compris des événements pour AWS IoT SiteWise, créez un parcours. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un parcours dans la console, celui-ci s'applique à toutes les AWS régions. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Présentation de la création d'un journal de suivi
- CloudTrail services et intégrations pris en charge

- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec les informations d'identification de l'utilisateur root ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec des informations d'identification de sécurité temporaires pour un rôle ou un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

AWS IoT SiteWise événements de données dans CloudTrail

Les événements de données fournissent des informations sur les opérations de ressources effectuées sur ou dans une ressource (par exemple, lecture ou écriture de données dans un objet Amazon S3). Ils sont également connus sous le nom opérations de plans de données. Les événements de données sont souvent des activités dont le volume est élevé. Par défaut, CloudTrail n'enregistre pas les événements liés aux données. L'historique des CloudTrail événements n'enregistre pas les événements liés aux données.

Des frais supplémentaires s'appliquent pour les événements de données. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

Vous pouvez enregistrer les événements de données pour les types de AWS IoT SiteWise ressources à l'aide de la CloudTrail console ou AWS CLI des opérations de CloudTrail l'API. Le tableau de cette section indique les types de ressources disponibles pour AWS IoT SiteWise.

- Pour enregistrer les événements de données à l'aide de la CloudTrail console, créez un magasin de données de suivi ou d'événement pour enregistrer les événements, ou mettez à jour un magasin de données de suivi ou d'événement existant pour enregistrer les événements de données.

  1. Choisissez Data events pour enregistrer les événements liés aux données.

2. Dans la liste des types d'événements de données, choisissez le type de ressource pour lequel vous souhaitez enregistrer les événements de données.
3. Choisissez le modèle de sélecteur de journal que vous souhaitez utiliser. Vous pouvez enregistrer tous les événements de données pour le type de ressource, consigner tous les `readOnly` événements, consigner tous les `writeOnly` événements ou créer un modèle de sélecteur de journal personnalisé pour filtrer les `resources.ARN` champs `readOnlyeventName`, et.

- Pour enregistrer des événements de données à l'aide de AWS CLI, configurez le `--advanced-event-selectors` paramètre pour définir le `eventCategory` champ égal à la valeur du type de ressource `Data` et le `resources.type` champ égal à la valeur du type de ressource (voir le tableau). Vous pouvez ajouter des conditions pour filtrer les valeurs des `resources.ARN` champs `readOnlyeventName`, et.
  - Pour configurer un suivi afin de consigner les événements liés aux données, exécutez la AWS CloudTrail put-event-selectorscommande. Pour plus d'informations, consultez la section Enregistrement des événements de données pour les sentiers avec le AWS CLI.
  - Pour configurer un magasin de données d'événements afin de consigner les événements, exécutez la AWS CloudTrail create-event-data-storecommande pour créer un nouveau magasin de données d'événements pour enregistrer les événements ou exécutez la AWS CloudTrail update-event-data-storecommande pour mettre à jour un magasin de données d'événements existant. Pour plus d'informations, consultez la section Enregistrement des événements de données pour les magasins de données d'événements avec le AWS CLI.

Le tableau suivant répertorie les types de AWS IoT SiteWise ressources. La colonne Type d'événement de données (console) indique la valeur à choisir dans la liste des types d'événements de données de la CloudTrail console. La colonne de valeur resources.type indique la **`resources.type`** valeur que vous devez spécifier lors de la configuration de sélecteurs d'événements avancés à l'aide des API or. AWS CLI CloudTrail La CloudTrail colonne Data APIs logged to indique les appels d'API enregistrés CloudTrail pour le type de ressource.

Type d'événement de données (console)	valeur resources.type	API de données connectées à CloudTrail *
AWS IoT SiteWise asset	`AWS::IoTSiteWise::Asset`	• BatchPutAssetPropertyValue • GetAssetPropertyValue

Type d'événement de données (console)	valeur resources.type	API de données connectées à CloudTrail *
		• GetAssetPropertyValueHistory • GetAssetPropertyAggregates • GetInterpolatedAssetPropertyValues • BatchGetAssetPropertyValue • BatchGetAssetPropertyValueHistory • BatchGetAssetPropertyAggregates
AWS IoT SiteWise séries chronologiques	`AWS::IoTSiteWise::TimeSeries`	• BatchPutAssetPropertyValue • GetAssetPropertyValue • GetAssetPropertyValueHistory • GetAssetPropertyAggregates • GetInterpolatedAssetPropertyValues • BatchGetAssetPropertyValue • BatchGetAssetPropertyValueHistory • BatchGetAssetPropertyAggregates

> **Note**
>
> Le fichier resources.type enregistré dans l'événement Cloudtrail dépend de l'identifiant utilisé dans la demande d'API. Si un identifiant d'actif est spécifié dans la demande, le fichier Asset resources.type est enregistré, sinon le fichier TimeSeries resources.type est enregistré.

*Vous pouvez configurer des sélecteurs d'événements avancés pour filtrer les `eventName`, `readOnly`, et des `resources.ARN` champs pour enregistrer uniquement les événements qui sont importants pour vous. Pour plus d'informations sur ces champs, consultez AdvancedFieldSelector.

AWS IoT SiteWise événements de gestion dans CloudTrail

Les événements de gestion fournissent des informations sur les opérations de gestion effectuées sur les ressources de votre AWS compte. Ils sont également connus sous le nom opérations de plan de contrôle. Par défaut, CloudTrail enregistre les événements de gestion.

AWS IoT SiteWise enregistre toutes les opérations AWS IoT SiteWise du plan de contrôle en tant qu'événements de gestion. Pour obtenir la liste des opérations du plan de AWS IoT SiteWise contrôle auxquelles AWS IoT SiteWise se connecte CloudTrail, consultez la référence de l'AWS IoT SiteWise API.

Exemple : entrées de fichier AWS IoT SiteWise journal

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'opération demandée, la date et l'heure de l'opération, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics. Ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`CreateAsset`opération.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
```

```
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::123456789012:user/Administrator",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Administrator",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2020-03-11T17:26:40Z"
      }
    },
    "invokedBy": "signin.amazonaws.com"
  },
  "eventTime": "2020-03-11T18:01:22Z",
  "eventSource": "iotsitewise.amazonaws.com",
  "eventName": "CreateAsset",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.0",
  "userAgent": "signin.amazonaws.com",
  "requestParameters": {
    "assetName": "Wind Turbine 1",
    "assetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
    "clientToken": "a1b2c3d4-5678-90ab-cdef-00000EXAMPLE"
  },
  "responseElements": {
    "assetId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
    "assetArn": "arn:aws:iotsitewise:us-east-1:123456789012:asset/a1b2c3d4-5678-90ab-
cdef-22222EXAMPLE",
    "assetStatus": {
      "state": "CREATING"
    }
  },
  "requestID": "a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE",
  "eventID": "a1b2c3d4-5678-90ab-cdef-bbbbbEXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
```

Marquer vos ressources AWS IoT SiteWise

Le balisage de vos AWS IoT SiteWise ressources constitue un moyen puissant de catégoriser, de gérer et de récupérer efficacement les actifs de l'organisation. En attribuant des balises, qui consistent en des paires clé-valeur, vous pouvez associer des métadonnées descriptives à vos ressources. Les métadonnées des balises peuvent être utilisées pour rationaliser les opérations. Par exemple, dans un scénario de parc éolien, les balises vous permettent d'étiqueter les turbines avec des attributs spécifiques tels que l'emplacement, la capacité et l'état opérationnel, ce qui permet une identification et une gestion rapides au sein de celles-ci AWS IoT SiteWise.

L'intégration de balises aux politiques AWS Identity and Access Management (IAM) améliore la sécurité et le contrôle opérationnel en définissant des règles d'accès conditionnel. Cela signifie que vous ne pouvez spécifier que les utilisateurs dotés de certaines balises. Par exemple, seules les personnes associées à un certain rôle ou département peuvent accéder à des ressources spécifiques ou les modifier.

Utilisation de balises dans AWS IoT SiteWise

Utilisez des balises pour classer vos AWS IoT SiteWise ressources par objectif, propriétaire, environnement ou toute autre classification adaptée à votre cas d'utilisation. Lorsque vous avez de nombreuses ressources de même type, vous pouvez rapidement identifier une ressource spécifique en fonction des balises que vous lui avez attribuées.

Chaque balise est composée d'une clé et d'une valeur facultative que vous spécifiez. Par exemple, vous pouvez définir une série de balises pour vos modèles d'actifs afin de les suivre en fonction des processus industriels qu'ils prennent en charge. Il est recommandé de développer un ensemble personnalisé de clés de balise pour chaque type de ressource que vous gérez. L'utilisation d'un ensemble cohérent de clés de balise peut faciliter la gestion des ressources.

Marquage à l'aide du AWS Management Console

L'éditeur de balises AWS Management Console fournit un moyen centralisé et unifié de créer et de gérer vos balises pour les ressources de tous les AWS services. Pour de plus amples informations, veuillez consulter Éditeur de balises dans le Guide de l'utilisateur AWS Resource Groups .

Marquage avec l'API AWS IoT SiteWise

L' AWS IoT SiteWise API utilise également des balises. Avant de créer des balises, tenez compte des restrictions liées aux balises. Pour de plus amples informations, veuillez consulter Conventions de dénomination et d'utilisation des balises dans le Références générales AWS.

- Pour ajouter des balises lorsque vous créez une ressource, définissez-les dans la propriété `tags` de la ressource.
- Pour ajouter des balises à une ressource existante ou pour mettre à jour les valeurs des balises, utilisez l'TagResourceopération.
- Pour supprimer des balises d'une ressource, utilisez l'UntagResourceopération.
- Pour récupérer les balises associées à une ressource, utilisez l'ListTagsForResourceopération ou décrivez la ressource et inspectez ses `tags` propriétés.

Le tableau suivant répertorie les ressources que vous pouvez baliser à l'aide de l' AWS IoT SiteWise API, ainsi que leurs `Describe` opérations `Create` et opérations correspondantes.

Ressources taguables AWS IoT SiteWise

Ressource	Opération de création	Opération de description
Modèle d'actif ou modèle de composant	CreateAssetModel	DescribeAssetModel
Ressource	CreateAsset	DescribeAsset
SiteWise Passerelle Edge	CreateGateway	DescribeGateway
Portal	CreatePortal	DescribePortal
Projet	CreateProject	DescribeProject
Tableau de bord	CreateDashboard	DescribeDashboard
Stratégie d'accès	CreateAccessPolicy	DescribeAccessPolicy
Séries chronologiques	BatchPutAssetPropertyValue	DescribeTimeSeries

En `BatchPutAssetPropertyValue` effet, vous pouvez configurer vos sources de données auxquelles envoyer des données industrielles AWS IoT SiteWise avant de créer des modèles d'actifs et des actifs. AWS IoT SiteWise crée automatiquement des flux de données pour recevoir des flux de données brutes de votre équipement. Pour plus d'informations, consultez la section Gestion de l'ingestion de données.

Utilisez les opérations suivantes afin d'afficher et de gérer des balises pour les ressources qui prennent en charge le balisage :

- TagResource— Ajoute des balises à une ressource ou met à jour la valeur d'une balise existante.
- ListTagsForResource— Répertorie les balises d'une ressource.
- UntagResource— Supprime les balises d'une ressource.

Ajoutez ou supprimez des balises d'une ressource à tout moment. Pour mettre à jour la valeur d'une clé de balise existante, ajoutez une nouvelle balise avec la même clé et la nouvelle valeur souhaitée à la ressource. Cette action remplace l'ancienne valeur par la nouvelle. Bien qu'il soit possible d'attribuer une chaîne vide comme valeur de balise, vous ne pouvez pas attribuer de valeur nulle.

La suppression d'une ressource entraîne également la suppression des balises qui lui sont associées.

Utilisation des balises avec des politiques IAM

Utilisez des balises de ressources dans vos politiques IAM pour contrôler l'accès et les autorisations des utilisateurs. Par exemple, les politiques peuvent autoriser les utilisateurs à créer uniquement des ressources associées à une balise spécifique. Les stratégies peuvent également empêcher les utilisateurs de créer ou de modifier des ressources qui ont des balises spécifiques.

> **Note**
>
> Si vous utilisez des balises pour autoriser ou refuser l'accès des utilisateurs aux ressources, vous devez refuser aux utilisateurs la possibilité d'ajouter ou de supprimer ces balises pour les mêmes ressources. Dans le cas contraire, un utilisateur pourrait contourner vos restrictions et accéder à une ressource en modifiant ses balises.

Vous pouvez utiliser les clés et valeurs de contexte de condition suivantes dans l'élément `Condition` (également appelé le bloc `Condition`) d'une instruction de stratégie.

`aws:ResourceTag/tag-key: tag-value`

Accorder ou refuser aux utilisateurs des actions sur des ressources ayant des balises spécifiques.

`aws:RequestTag/tag-key: tag-value`

Exiger qu'une balise spécifique soit utilisée (ou non) lors de la création ou de la modification d'une ressource balisable.

`aws:TagKeys: [tag-key, ...]`

Exiger qu'un ensemble spécifique de clés de balise soit utilisé (ou non) lors de la création ou de la modification d'une ressource balisable.

> **Note**
>
> Les clés et valeurs de contexte de condition d'une politique IAM s'appliquent uniquement aux actions dont le paramètre obligatoire est une ressource balisable. Par exemple, vous pouvez définir un accès conditionnel basé sur des balises pour ListAssets. Vous ne pouvez pas activer l'accès conditionnel basé sur des balises PutLoggingOptionscar aucune ressource balisable n'est référencée dans la demande.

Pour plus d'informations, consultez la section Contrôle de l'accès aux AWS ressources à l'aide de balises de ressources et la référence de politique IAM JSON dans le guide de l'utilisateur IAM.

Exemples de politiques IAM utilisant des balises

- Affichage des ressources AWS IoT SiteWise basées sur des balises

Résolution des problèmes AWS IoT SiteWise

Utilisez les informations contenues dans ces sections pour résoudre les problèmes liés à AWS IoT SiteWise.

Rubriques

- Résolution des problèmes liés aux opérations d'importation et d'exportation en masse
- Résolution des problèmes liés à un AWS IoT SiteWise portail
- Résolution des problèmes liés à une passerelle SiteWise Edge
- Résolution des problèmes liés à une action de AWS IoT SiteWise règle

Résolution des problèmes liés aux opérations d'importation et d'exportation en masse

Pour gérer et diagnostiquer les erreurs produites lors d'une tâche de transfert, consultez l' AWS IoT TwinMaker GetMetadataTransferJobAPI :

1. Après avoir créé et exécuté une tâche de transfert, appelez l'GetMetadataTransferJobAPI :

```
aws iottwinmaker get-metadata-transfer-job \
--metadata-transfer-job-id your_metadata_transfer_job_id \
--region us-east-1
```

2. L'état de la tâche passe à l'un des états ci-dessous :
   - TERMINÉ
   - CANCELLED
   - ERROR
3. L'GetMetadataTransferJobAPI renvoie un MetadataTransferJobProgressobjet.
4. L'MetadataTransferJobProgressobjet contient les paramètres suivants :
   - FailedCount : indique le nombre d'actifs défaillants pendant le processus de transfert.
   - SkippedCount : indique le nombre d'actifs ignorés pendant le processus de transfert.
   - SucceededCount : indique le nombre d'actifs qui ont réussi pendant le processus de transfert.

- TotalCount : indique le nombre total d'actifs impliqués dans le processus de transfert.

5. En outre, un élément ReportURL est renvoyé par l'appel d'API, qui contient une URL pré-signée. Si votre tâche de transfert comporte des erreurs nécessitant une enquête, vous pouvez télécharger un rapport d'erreur complet à cette adresse URL.

Résolution des problèmes liés à un AWS IoT SiteWise portail

Résolvez les problèmes courants liés à vos AWS IoT SiteWise portails.

Les utilisateurs et les administrateurs ne peuvent pas accéder au AWS IoT SiteWise portail

Si les utilisateurs ou les administrateurs ne peuvent pas accéder à votre AWS IoT SiteWise portail, il se peut que vous disposiez d'autorisations restreintes dans le cadre de politiques associées AWS Identity and Access Management (IAM) qui empêchent les connexions réussies.

Consultez les exemples suivants de politiques IAM susceptibles d'entraîner un échec de connexion :

> **Note**
>
> Toute politique IAM attachée qui inclut un `"Condition"` élément entraînera un échec de connexion.

Exemple 1 : La condition ici est une adresse IP limitée, ce qui entraînera un échec de connexion.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iotsitewise:DescribePortal"
            ],
            "Resource": "*",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": [
```

```
                        "REPLACESAMPLEIP"
                    ]
                }
            }
        }
    ]
}
```

Exemple 2 : La condition ici est une balise incluse, ce qui provoquera un échec de connexion.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iotsitewise:DescribePortal"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/project": "*"
                }
            }
        }
    ]
}
```

Lorsque vous ajoutez des utilisateurs ou des administrateurs au portail, évitez de créer des politiques IAM qui limitent les autorisations des utilisateurs, telles qu'une adresse IP limitée. Les politiques associées avec des autorisations restreintes ne pourront pas se connecter au AWS IoT SiteWise portail.

Résolution des problèmes liés à une passerelle SiteWise Edge

AWS IoT SiteWise Les passerelles Edge exécutent un ensemble de AWS IoT Greengrass composants. Vous pouvez configurer votre passerelle SiteWise Edge pour consigner les événements sur Amazon CloudWatch et dans le système de fichiers local de votre passerelle SiteWise Edge. Vous pouvez ensuite consulter les fichiers journaux pour résoudre les problèmes liés à votre passerelle SiteWise Edge.

Vous pouvez également consulter CloudWatch les métriques signalées par vos passerelles SiteWise Edge pour résoudre les problèmes de connectivité ou de flux de données. Pour plus d'informations, consultez Surveillance AWS IoT SiteWise à l'aide des CloudWatch métriques Amazon.

Rubriques

- Configuration et accès aux journaux de la passerelle SiteWise Edge
- Résolution des problèmes liés à la passerelle SiteWise Edge
- AWS IoT Greengrass Problèmes de résolution des problèmes

Configuration et accès aux journaux de la passerelle SiteWise Edge

Avant de pouvoir consulter les journaux de la passerelle SiteWise Edge, vous devez configurer votre passerelle SiteWise Edge pour qu'elle envoie des journaux à Amazon CloudWatch Logs ou qu'elle les stocke sur le système de fichiers local.

- Utilisez CloudWatch les journaux si vous souhaitez utiliser le AWS Management Console pour afficher les fichiers journaux de votre passerelle SiteWise Edge. Pour plus d'informations, consultez Utilisation d'Amazon CloudWatch Logs.
- Utilisez les journaux du système de fichiers local si vous souhaitez utiliser la ligne de commande ou un logiciel local pour afficher les fichiers journaux de votre passerelle SiteWise Edge. Pour plus d'informations, consultez Utilisation des journaux de service.

Résolution des problèmes liés à la passerelle SiteWise Edge

Utilisez les informations suivantes pour résoudre les problèmes liés à la passerelle SiteWise Edge.

Problèmes

- Impossible de déployer des packs sur les passerelles SiteWise Edge
- AWS IoT SiteWise ne reçoit pas de données en provenance des serveurs OPC-UA
- Aucune donnée n'était affichée dans le tableau de bord
- « Impossible de trouver ou de charger la classe principale » qui s'affiche dans le fichier aws.iot.SiteWiseEdgePublisher erreur de journalisation dans /greengrass/v2/logs

Impossible de déployer des packs sur les passerelles SiteWise Edge

Si le composant AWS IoT Greengrass nucleus (`aws.greengrass.Nucleus`) est obsolète, il se peut que vous ne puissiez pas déployer de packs sur votre passerelle SiteWise Edge. Vous pouvez utiliser la AWS IoT Greengrass V2 console pour mettre à niveau le composant AWS IoT Greengrass Nucleus.

Mettre à niveau le composant AWS IoT Greengrass Nucleus (console)

1. Accédez à la console AWS IoT Greengrass.
2. Dans le volet de navigation, sous AWS IoT Greengrass, choisissez Deployments.
3. Dans la liste des déploiements, sélectionnez le déploiement que vous souhaitez réviser.
4. Choisissez Réviser.
5. Sur la page Spécifier la cible, choisissez Next.
6. Sur la page Sélectionner les composants, sous Composants publics, dans la zone de recherche, entrez**`aws.greengrass.Nucleus`**, puis sélectionnez AWS.Greengrass.Nucleus.
7. Choisissez Suivant.
8. Sur la page Configurer les composants, choisissez Next.
9. Sur la page Configurer les paramètres avancés, choisissez Next.
10. Sur la page Review (Révision), choisissez Deploy (Déployer).

AWS IoT SiteWise ne reçoit pas de données en provenance des serveurs OPC-UA

Si vos AWS IoT SiteWise actifs ne reçoivent pas les données envoyées par vos serveurs OPC-UA, vous pouvez effectuer des recherches dans les journaux de votre passerelle SiteWise Edge pour résoudre les problèmes. Recherchez les `swPublisher` journaux au niveau des informations qui contiennent le message suivant.

```
Emitting diagnostic name=PublishError.SomeException
```

En fonction du type de contenu *`SomeException`*dans le journal, utilisez les types d'exception suivants et les problèmes correspondants pour résoudre les problèmes liés à votre passerelle SiteWise Edge :

- ResourceNotFoundException— Vos serveurs OPC-UA envoient des données qui ne correspondent à aucun alias de propriété pour un actif. Cette exception peut se produire dans deux cas :
  - Vos alias de propriété ne correspondent pas exactement à vos variables OPC-UA, y compris les préfixes source que vous avez définis. Vérifiez que vos alias de propriété et vos préfixes source sont corrects.
  - Vous n'avez pas mappé vos variables OPC-UA aux propriétés de la ressource. Pour plus d'informations, consultez Mappage des flux de données industrielles avec des propriétés de ressources.

    Si vous avez déjà mappé toutes les variables OPC-UA souhaitées AWS IoT SiteWise, vous pouvez filtrer les variables OPC-UA envoyées par la passerelle Edge. SiteWise Pour plus d'informations, consultez Utilisation des filtres de nœuds OPC-UA.
- InvalidRequestException— Les types de données de vos variables OPC-UA ne correspondent pas aux types de données des propriétés de vos actifs. Par exemple, si un flux OPC-UA a un type de données entier, votre propriété de ressource correspondante doit être un type de données entier. Une propriété de ressource de type double ne peut pas recevoir de valeurs entières OPC-UA. Pour résoudre ce problème, définissez de nouvelles propriétés avec les types de données corrects.
- TimestampOutOfRangeException— Votre passerelle SiteWise Edge envoie des données qui se situent en dehors de la plage d' AWS IoT SiteWise acceptation. AWS IoT SiteWise rejette tous les points de données dont l'horodatage est antérieur à 7 jours dans le passé ou inférieur à 5 minutes dans le futur. En cas de perte d'alimentation ou de connexion au AWS cloud de votre passerelle SiteWise Edge, vous devrez peut-être vider le cache de votre passerelle SiteWise Edge.
- ThrottlingExceptionou LimitExceededException: votre demande a dépassé un quota de AWS IoT SiteWise service, tel que le taux de points de données ingérés ou le taux de demandes pour les opérations de l'API de données relatives aux propriétés des actifs. Vérifiez que votre configuration ne dépasse pas le AWS IoT SiteWise quotas.

Aucune donnée n'était affichée dans le tableau de bord

Si aucune donnée n'apparaît dans votre tableau de bord, il est possible que la configuration de l'éditeur et la source de données de la passerelle SiteWise Edge ne soient pas synchronisées. S'ils ne sont pas synchronisés, la mise à jour du nom de la source de données peut accélérer la synchronisation entre le cloud et le périphérique, corrigeant ainsi l'erreur de désynchronisation.

Pour mettre à jour le nom d'une source de données

1. Accédez à la console AWS IoT SiteWise.
2. Dans le volet de navigation, choisissez Edge gateways.
3. Sélectionnez la passerelle SiteWise Edge connectée au tableau de bord.
4. Sous Sources de données, sélectionnez Modifier.
5. Sélectionnez un nouveau nom de source, puis sélectionnez Enregistrer pour confirmer votre modification.
6. Vérifiez vos modifications en confirmant que le nom de la source de données a été mis à jour dans le tableau des sources de données.

« Impossible de trouver ou de charger la classe principale » qui s'affiche dans le fichier aws.iot. SiteWiseEdgePublisher erreur de journalisation dans /greengrass/v2/logs

Si cette erreur s'affiche, vous devrez peut-être mettre à jour la version Java de votre passerelle SiteWise Edge.

- Depuis un terminal, exécutez la commande suivante :

  ```
  java -version
  ```

  La version de Java avec SiteWise laquelle votre passerelle Edge est exécutée s'affichera sous`OpenJDK Runtime Environment`. Vous verrez une réponse semblable à la suivante :

  ```
  openjdk version "11.0.20" 2023-07-18 LTS
  OpenJDK Runtime Environment Corretto011.0.20.8.1 (build 11.0.20+8-LTS
  OpenJDK 64-Bit Server VM Corretto-11.0.20.8.1 (build 11.0.20+8-LTS, mixed node)
  ```

Si vous utilisez la version 11.0.20.8.1 de Java, vous devez mettre à jour le pack IoT SiteWise Publisher vers la version 2.4.1 ou une version ultérieure. Seule la version 11.0.20.8.1 de Java est affectée. Les environnements dotés d'autres versions de Java peuvent continuer à utiliser les anciennes versions du composant IoT SiteWise Publisher. Pour plus d'informations sur la mise à jour d'un pack de composants, consultezModification de la version des packs de composants de la passerelle SiteWise Edge.

AWS IoT Greengrass Problèmes de résolution des problèmes

Pour trouver des solutions à de nombreux problèmes liés à la configuration ou au déploiement de votre passerelle SiteWise Edge AWS IoT Greengrass, consultez la section Résolution des problèmes AWS IoT Greengrass dans le Guide du AWS IoT Greengrass développeur.

Résolution des problèmes liés à une action de AWS IoT SiteWise règle

Pour résoudre les problèmes liés à l'action de votre AWS IoT SiteWise règle dans AWS IoT Core, vous pouvez suivre l'une des procédures suivantes :

- Configuration d'Amazon CloudWatch Logs
- Configurer une action d'erreur de republication pour votre règle

Ensuite, comparez les messages d'erreur avec les erreurs de cette rubrique pour résoudre le problème.

Rubriques

- Configuration des AWS IoT Core journaux
- Configuration d'une action d'erreur de republication
- Résolution des problèmes
- Résolution des problèmes d'une règle
- Résolution des problèmes d'une règle

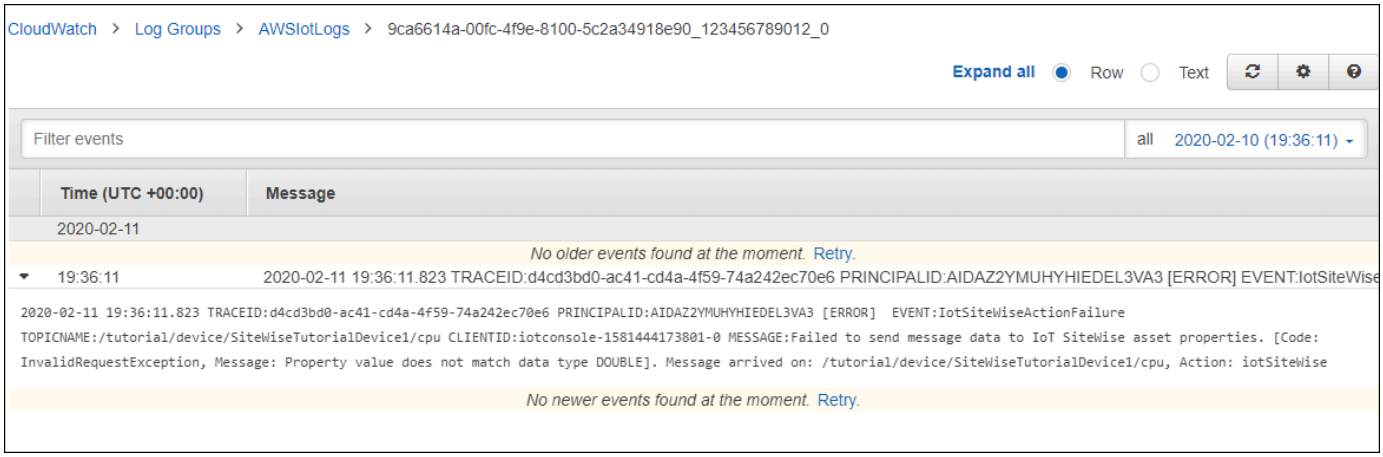
Configuration des AWS IoT Core journaux

Vous pouvez configurer AWS IoT pour consigner différents niveaux d'informations dans CloudWatch Logs.

Pour configurer les CloudWatch journaux et y accéder

1. Pour configurer la journalisation pour AWS IoT Core, consultez la section Surveillance à l'aide CloudWatch des journaux dans le guide du AWS IoT développeur.
2. Accédez à la console CloudWatch .

3. Dans le panneau de navigation, choisissez Groupes de journaux.
4. Choisissez le AWSIotLogsgroupe.
5. Choisissez un flux de journaux récent. Par défaut, CloudWatch affiche le flux de journal le plus récent en premier.
6. Choisissez une entrée de journal pour développer le message de journal. Votre entrée de journal peut ressembler à la capture d'écran suivante.



7. Comparez les messages d'erreur avec les erreurs de cette rubrique pour résoudre le problème.

Configuration d'une action d'erreur de republication

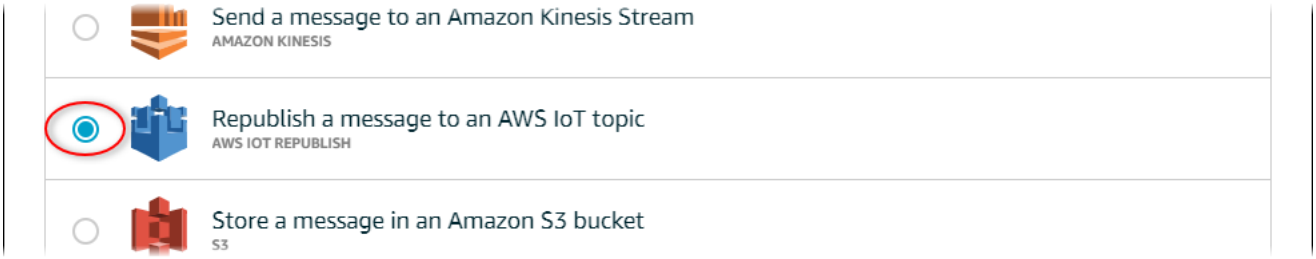
Vous pouvez configurer une action d'erreur au niveau d'une règle pour gérer les messages d'erreur. Dans cette procédure, vous configurez l'action de règle de republication en tant qu'action d'erreur pour afficher les messages d'erreur dans le client de test MQTT.

> **Note**
>
> L'action d'erreur de republication ne génère que l'équivalent des journaux de niveau ERROR. Si vous souhaitez des journaux plus détaillés, vous devez configurer CloudWatch les journaux.

Pour ajouter une action d'erreur de republication à une règle

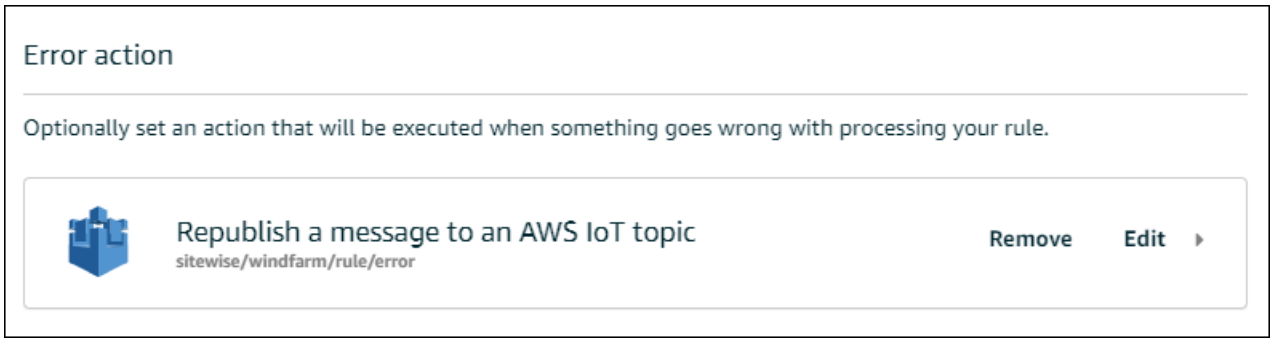
1. Accédez à la console AWS IoT.
2. Dans le panneau de navigation de gauche, choisissez Act (Agir) puis Rules (Règles).
3. Choisissez une règle.

4. Sous Error action (Action d'erreur), choisissez Add action (Ajouter une action).
5. Choisissez Republier un message dans un AWS IoT sujet.



6. En bas de la page, choisissez Configure action (Configurer l'action).
7. Dans Sujet, entrez un sujet unique (par exemple,**`sitewise/windfarm/rule/error`**). AWS IoT Core republiera les messages d'erreur dans cette rubrique.
8. Choisissez Sélectionner pour autoriser AWS IoT Core l'accès afin d'exécuter l'action d'erreur.
9. Choisissez Select (Sélectionner) en regard du rôle que vous avez créé pour la règle.
10. Choisissez Update Role (Mettre à jour le rôle) pour ajouter les autorisations supplémentaires au rôle.
11. Choisissez Add action.

    L'action d'erreur de la règle devrait ressembler à la capture d'écran suivante.



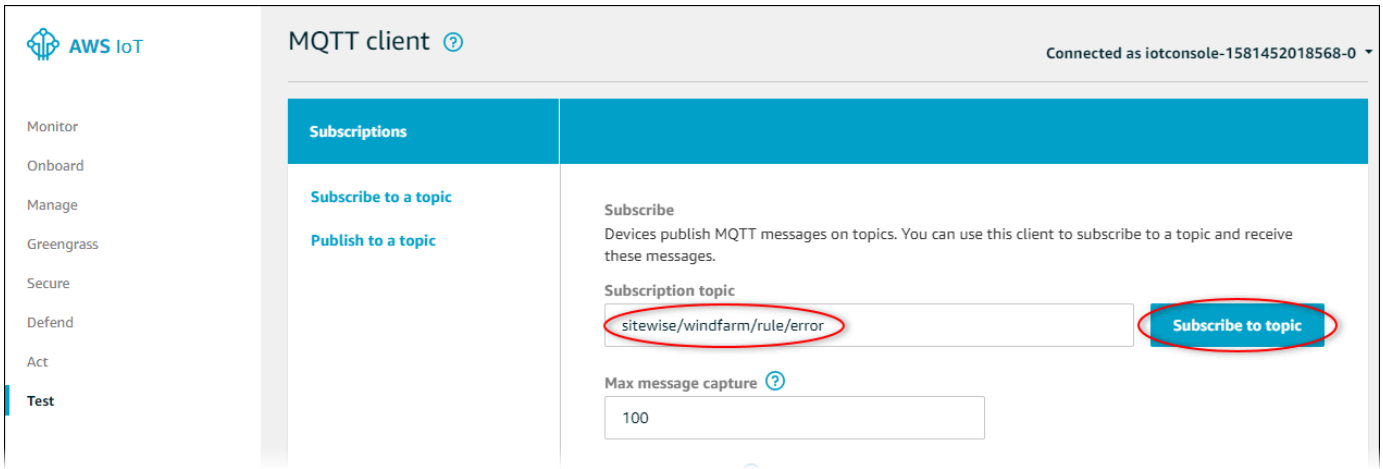
12. Cliquez sur la flèche de retour en haut à gauche de la console pour revenir à la page d'accueil de la AWS IoT console.

Après avoir configuré l'action d'erreur de republication, vous pouvez afficher les messages d'erreur dans le client de test MQTT dans AWS IoT Core.

Dans la procédure suivante, vous vous abonnez à la rubrique d'erreur dans le client de test MQTT. Le client de test MQTT vous permet de recevoir les messages d'erreur de la règle afin de résoudre le problème.

Pour vous abonner à la rubrique d'action d'erreur

1. Accédez à la console AWS IoT.
2. Dans la page de navigation de gauche, choisissez Test pour ouvrir le client de test MQTT.
3. Dans le champ Subscription topic (Rubrique d'abonnement), entrez la rubrique d'erreur que vous avez configurée précédemment (par exemple, **`sitewise/windfarm/rule/error`**) et choisissez Subscribe to topic (S'abonner à la rubrique).



4. Surveillez les messages d'erreur qui s'affichent, puis développez le tableau `failures` dans chaque message d'erreur.

   Ensuite, comparez les messages d'erreur avec les erreurs de cette rubrique pour résoudre le problème.

Résolution des problèmes

Utilisez les informations suivantes pour résoudre les problèmes de règle.

Problèmes

- Erreur : le membre doit être dans les 604800 secondes avant et 300 secondes après l'horodatage actuel
- Erreur : la valeur de la propriété ne correspond pas au type de données <type>
- Erreur : L'utilisateur <role-arn>n'est pas autorisé à exécuter : iotsitewise : aucune ressource BatchPutAssetPropertyValue
- Erreur : iot.amazonaws.com ne parvient pas à exécuter : sts : on resource : AssumeRole <role-arn>

- Info : aucune demande n'a été envoyée. PutAssetPropertyValueEntries était vide après avoir effectué des modèles de substitution.

Erreur : le membre doit être dans les 604800 secondes avant et 300 secondes après l'horodatage actuel

Votre horodatage date de plus de 7 jours ou de moins de 5 minutes, par rapport à l'époque Unix actuelle. Essayez les éléments suivants :

- Vérifiez que l'horodatage est au format d'heure Unix epoch (UTC). Si vous fournissez un horodatage avec un fuseau horaire différent, vous rencontrerez cette erreur.
- Vérifiez que votre horodatage est en secondes. AWS IoT SiteWise attend des horodatages divisés en secondes (à l'époque Unix) et décalés en nanosecondes.
- Vérifiez que vous téléchargez des données horodatées au plus tard de 7 jours plus tôt.

Erreur : la valeur de la propriété ne correspond pas au type de données <type>

Une entrée de votre action de règle comporte un type de données différent de celui de la propriété de ressource cible. Par exemple, la propriété de ressource cible est de type `DOUBLE`, tandis que le type de données que vous avez sélectionné est Integer ou que vous avez transmis la valeur dans `integerValue`. Essayez les éléments suivants :

- Si vous configurez la règle depuis la AWS IoT console, vérifiez que vous avez choisi le bon type de données pour chaque entrée.
- Si vous configurez la règle depuis l'API ou AWS Command Line Interface (AWS CLI), vérifiez que votre `value` objet utilise le champ de type correct (par exemple, `doubleValue` pour une `DOUBLE` propriété).

Erreur : L'utilisateur <role-arn>n'est pas autorisé à exécuter : iotsitewise : aucune ressource BatchPutAssetPropertyValue

Soit la règle n'est pas autorisée à accéder à la propriété de ressource cible, soit la propriété de ressource cible n'existe pas. Essayez les éléments suivants :

- Vérifiez que l'alias de la propriété est correct et que la propriété de ressource dispose de l'alias de propriété donné. Pour plus d'informations, consultez Mappage des flux de données industrielles avec des propriétés de ressources.
- Vérifiez que la règle est associée à un rôle et que le rôle `iotsitewise:BatchPutAssetPropertyValue` donne l'autorisation à la propriété de ressource cible, par exemple via la hiérarchie de la ressource cible. Pour plus d'informations, consultez Octroi AWS IoT de l'accès requis.

Erreur : iot.amazonaws.com ne parvient pas à exécuter : sts : on resource : AssumeRole <role-arn>

Votre utilisateur n'est pas autorisé à assumer le rôle dans votre règle dans AWS Identity and Access Management (IAM).

Vérifiez que votre utilisateur est `iam:PassRole` autorisé à accéder au rôle indiqué dans votre règle. Pour plus d'informations, consultez la section Transmettre les autorisations de rôle dans le guide du AWS IoT développeur.

Info : aucune demande n'a été envoyée. PutAssetPropertyValueEntries était vide après avoir effectué des modèles de substitution.

> **Note**
>
> Ce message est un journal de niveau `INFO`.

Votre demande doit comporter au moins une entrée avec tous les paramètres requis.

Vérifiez que les paramètres de la règle, y compris les modèles de substitution, génèrent des valeurs non vides. Les modèles de substitution ne peuvent pas accéder aux valeurs définies dans les clauses `AS` de l'instruction de requête de la règle. Pour plus d'informations, consultez la section Modèles de substitution dans le Guide du AWS IoT développeur.

Résolution des problèmes d'une règle

Suivez les étapes de cette procédure pour résoudre les problèmes liés à votre règle si les données d'utilisation du processeur et de la mémoire ne s'affichent pas AWS IoT SiteWise comme prévu.

Dans cette procédure, vous configurez l'action de règle de republication en tant qu'action d'erreur pour afficher les messages d'erreur dans le client de test MQTT. Vous pouvez également configurer la journalisation dans CloudWatch Logs pour résoudre les problèmes. Pour plus d'informations, consultez Résolution des problèmes liés à une action de AWS IoT SiteWise règle.

Pour ajouter une action d'erreur de republication à une règle

1. Accédez à la console AWS IoT.
2. Dans le volet de navigation de gauche, choisissez Routage des messages, puis sélectionnez Règles.
3. Choisissez la règle que vous avez créée précédemment, puis cliquez sur Modifier.
4. Sous Action d'erreur - facultatif, choisissez Ajouter une action d'erreur.
5. Choisissez Republier un message dans un AWS IoT sujet.
6. Dans Sujet, entrez le chemin de votre erreur (par exemple,**`sitewise/rule/tutorial/error`**). AWS IoT Core republiera les messages d'erreur dans cette rubrique.
7. Choisissez le rôle que vous avez créé précédemment (par exemple, SiteWiseTutorialDeviceRuleRole).
8. Choisissez Mettre à jour.

Après avoir configuré l'action d'erreur de republication, vous pouvez afficher les messages d'erreur dans le client de test MQTT dans AWS IoT Core.

Dans la procédure suivante, vous vous abonnez à la rubrique d'erreur dans le client de test MQTT.

Pour vous abonner à la rubrique d'action d'erreur

1. Accédez à la console AWS IoT.
2. Dans la page de navigation de gauche, choisissez le client de test MQTT pour ouvrir le client de test MQTT.
3. Dans le champ Filtre par sujet, entrez **`sitewise/rule/tutorial/error`** et choisissez S'abonner.

Lorsque des messages d'erreur apparaissent, affichez le tableau `failures` dans n'importe quel message d'erreur pour diagnostiquer les problèmes. Pour plus d'informations sur les problèmes et les solutions possibles, consultez Résolution des problèmes liés à une action de AWS IoT SiteWise règle.

Si aucune erreur ne s'affiche, vérifiez que votre règle est activée et que vous vous êtes abonné à la même rubrique que celle que vous avez configurée dans l'action d'erreur de republication. Si des erreurs ne s'affichent toujours pas, vérifiez que le script du périphérique est en cours d'exécution et qu'il met à jour l'ombre du périphérique avec succès.

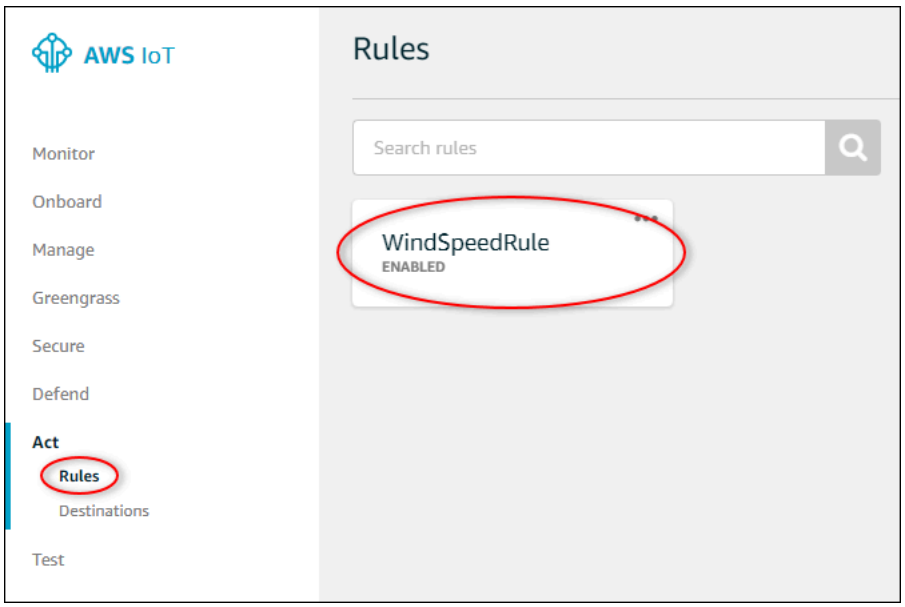
> **Note**
>
> Vous pouvez également vous abonner à la rubrique de mise à jour parallèle de votre appareil pour voir la charge utile analysée par votre AWS IoT SiteWise action. Pour ce faire, abonnez-vous à la rubrique suivante.
>
> ```
> $aws/things/+/shadow/update/accepted
> ```

Résolution des problèmes d'une règle

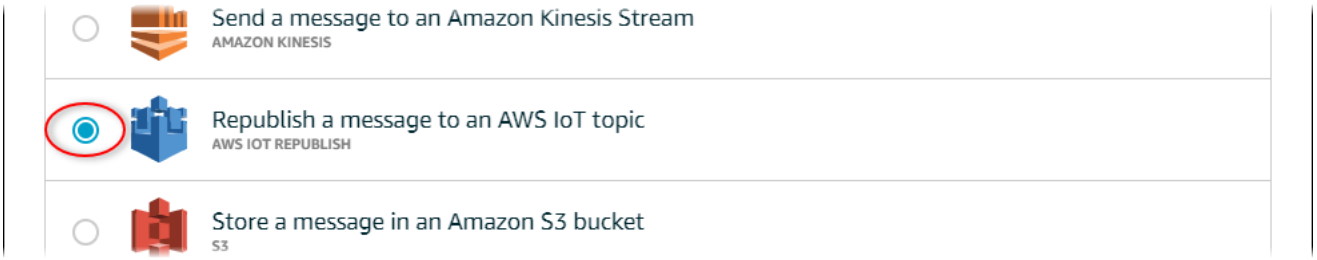
Suivez les étapes de cette procédure pour résoudre les problèmes liés à votre règle si les données des actifs de démonstration n'apparaissent pas dans le tableau DynamoDB comme prévu. Dans cette procédure, vous configurez l'action de règle de republication en tant qu'action d'erreur pour afficher les messages d'erreur dans le client de test MQTT. Vous pouvez également configurer la journalisation dans CloudWatch Logs pour résoudre les problèmes. Pour plus d'informations, consultez la section Surveillance à l'aide CloudWatch des journaux dans le guide du AWS IoT développeur.

Pour ajouter une action d'erreur de republication à une règle

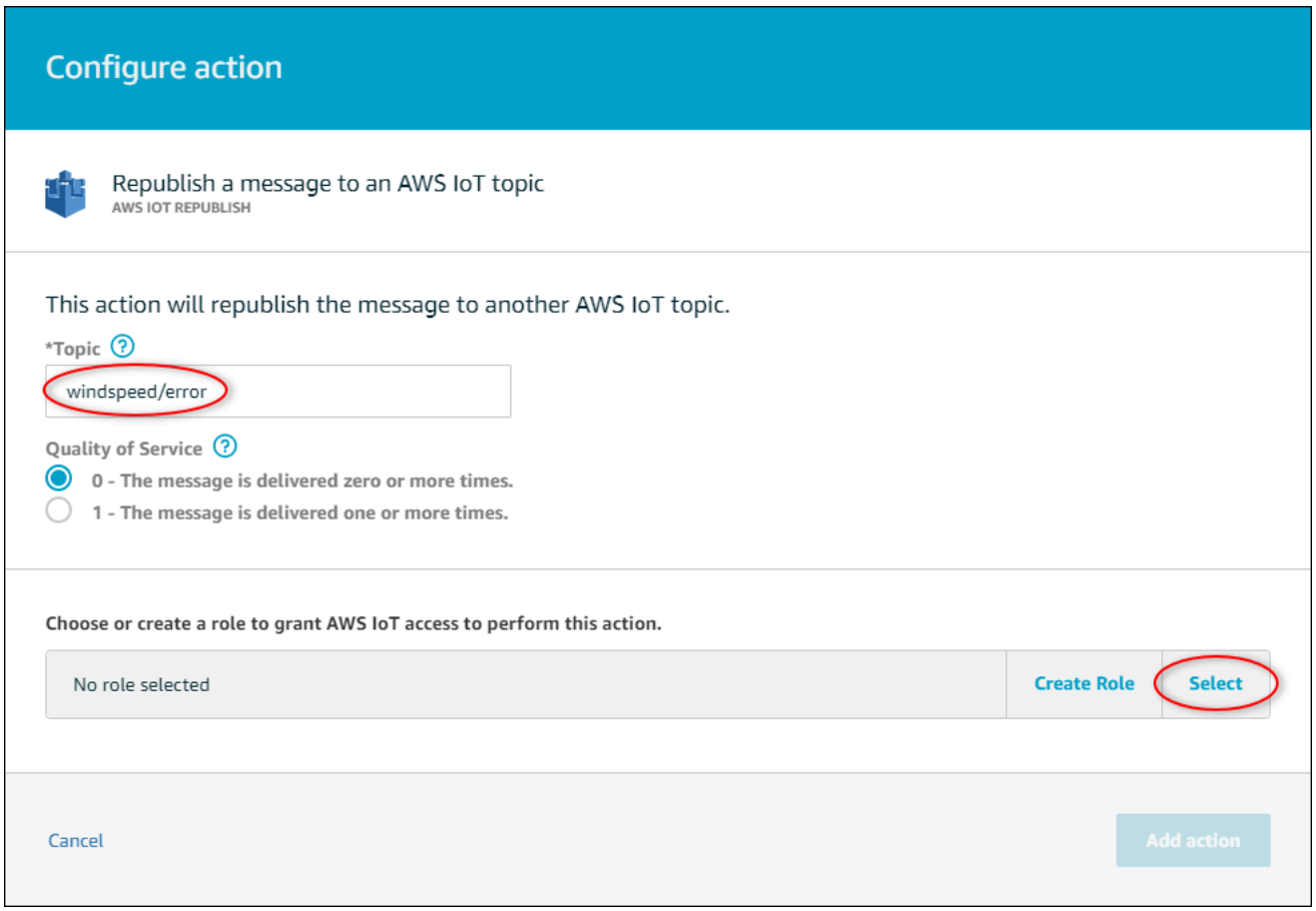
1. Accédez à la console AWS IoT.
2. Dans le panneau de navigation de gauche, choisissez Act (Agir) puis Rules (Règles).
3. Choisissez la règle que vous avez créée précédemment.



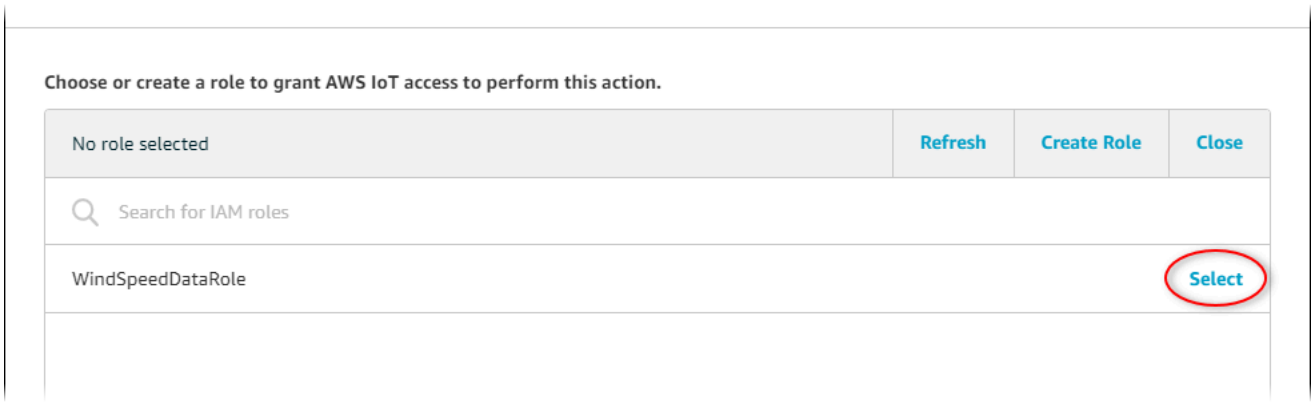
4. Sous Error action (Action d'erreur), choisissez Add action (Ajouter une action).
5. Choisissez Republier un message dans un AWS IoT sujet.



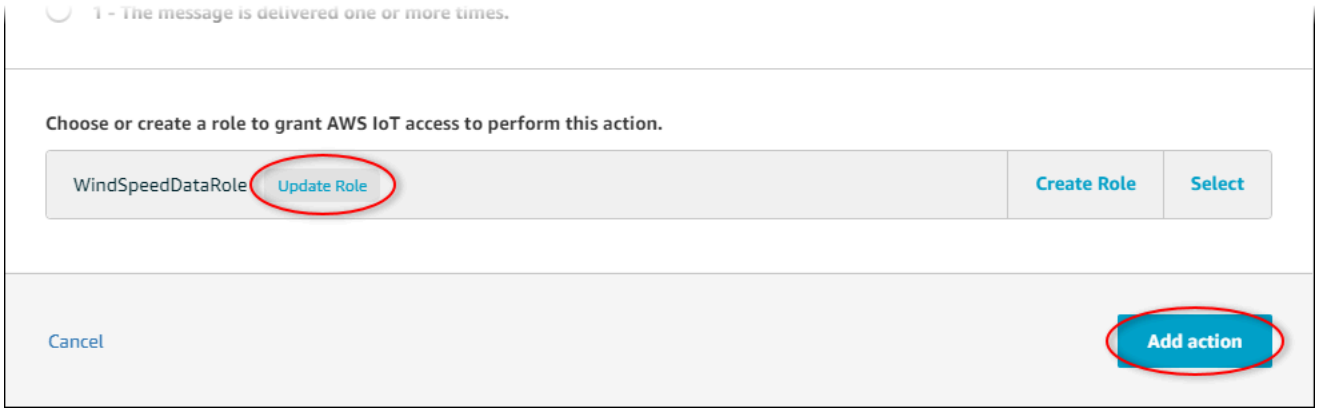
6. En bas de la page, choisissez Configure action (Configurer l'action).
7. Dans Sujet, entrez **`windspeed/error`**. AWS IoT Core republiera les messages d'erreur dans cette rubrique.



8. Choisissez Sélectionner pour autoriser AWS IoT Core à exécuter l'action d'erreur en utilisant le rôle que vous avez créé précédemment.
9. Choisissez Select (Sélectionner) en regard de votre rôle.



10. Choisissez Update Role (Mettre à jour le rôle) pour ajouter les autorisations supplémentaires au rôle.



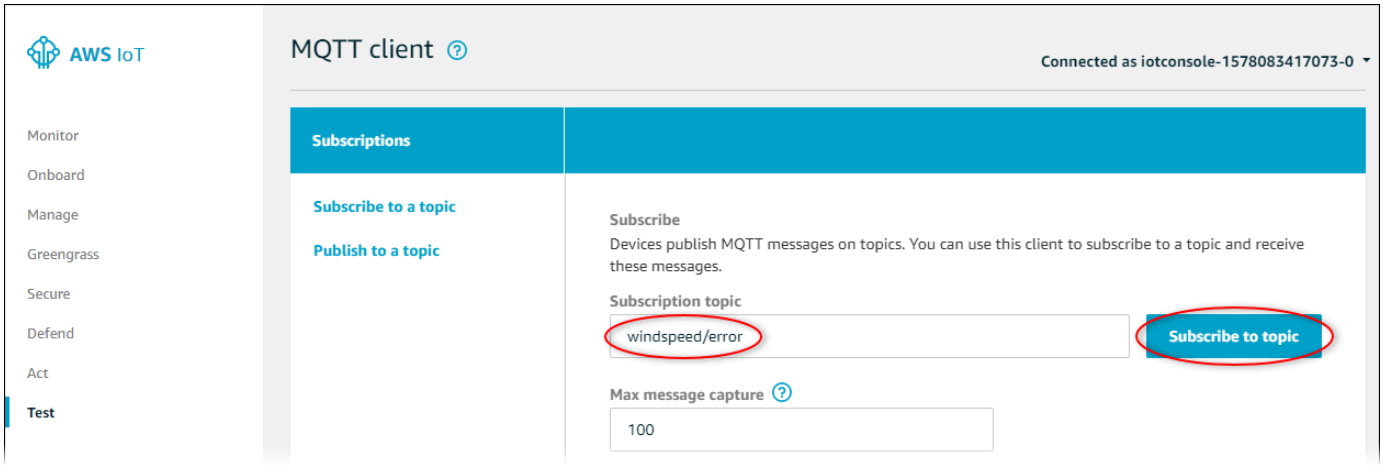
11. Choisissez Add action (Ajouter une action) pour terminer l'ajout de l'action d'erreur.
12. Cliquez sur la flèche de retour en haut à gauche de la console pour revenir à la page d'accueil de la console AWS IoT Core.

Après avoir configuré l'action d'erreur de republication, vous pouvez afficher les messages d'erreur dans le client de test MQTT dans AWS IoT Core.

Dans la procédure suivante, vous vous abonnez à la rubrique d'erreur dans le client de test MQTT.

Pour vous abonner à la rubrique d'action d'erreur

1. Dans la page de navigation de gauche de la console AWS IoT Core, choisissez Test.
2. Dans le champ Subscription topic (Rubrique Abonnement) saisissez **`windspeed/error`** et choisissez Subscribe to topic (S'abonner à la rubrique).



3. Vérifiez les messages d'erreur qui s'affichent et explorez la zone `failures` d'un message d'erreur pour diagnostiquer les problèmes courants suivants :

   - Fautes de frappe dans l'instruction de requête de règle

- Autorisations de rôle insuffisantes

Si aucune erreur ne s'affiche, vérifiez que votre règle est activée et que vous vous êtes abonné à la même rubrique que celle que vous avez configurée dans l'action d'erreur de republication. Si, malgré cela, aucune erreur ne s'affiche, vérifiez que les ressources de votre parc éolien de démonstration existent toujours et que vous avez activé les notifications sur les propriétés de vitesse du vent. Si vos ressources de démonstration ont expiré et ont disparu AWS IoT SiteWise, vous pouvez créer une nouvelle démo et mettre à jour l'énoncé de la requête de règle pour refléter le modèle d'actif et les identifiants de propriété mis à jour.

AWS IoT SiteWise points de terminaison et quotas

Les sections suivantes décrivent les points de terminaison et les quotas pour AWS IoT SiteWise.

Table des matières

- AWS IoT SiteWise points de terminaison
- AWS IoT SiteWise quotas

AWS IoT SiteWise points de terminaison

Pour vous connecter par programmation AWS IoT SiteWise, vous utilisez un point de terminaison. Les AWS SDK et AWS Command Line Interface (AWS CLI) utilisent automatiquement le point de terminaison par défaut dans une AWS région. Pour plus d'informations sur les régions où cette option AWS IoT SiteWise est disponible, consultez la section AWS IoT SiteWise Points de terminaison et quotas dans le Références générales AWS.

AWS IoT SiteWise prend en charge les points de terminaison suivants.

Utilisez ce point de terminaison pour accéder aux opérations d'API du plan de données suivantes : BatchPutAssetPropertyValueGetAssetPropertyAggregatesGetAssetPropertyValue,, GetAssetPropertyValueHistoryet GetInterpolatedAssetPropertyValues. Remplacez *`region`* par votre AWS région.

AWS IoT SiteWise propose ce point de terminaison consolidé pour les opérations d'API du plan de contrôle que vous utilisez pour gérer les modèles d'actifs, les actifs, les passerelles SiteWise Edge, les balises et les configurations de comptes. Remplacez *`region`* par votre AWS région.

> **Note**
>
> - Par défaut, AWS IoT SiteWise utilise le point de terminaison consolidé lorsque vous appelez les opérations d'API du plan de contrôle prises en charge.
> - Nous vous recommandons d'utiliser le point de terminaison consolidé pour les opérations d'API du plan de contrôle prises en charge.
> - Vous ne pouvez pas utiliser le point de terminaison consolidé pour accéder aux opérations de l'API SiteWise Monitor.

Les opérations d'API du plan de contrôle prises en charge incluent AssociateAssetsCreateAssetCreateAssetModelDeleteAssetDeleteAssetModel,, DeleteDashboard, DescribeAsset, DescribeAssetModel, DescribeAssetProperty, DescribeDashboard, DescribeLoggingOptions, DisassociateAssets, ListAssetModels, ListAssetRelationships,, ListAssets, ListAssociatedAssets, PutLoggingOptions, UpdateAsset, UpdateAssetModel, UpdateAssetProperty, CreateGateway, DeleteGateway, DescribeGateway, DescribeGatewayCapabilityConfiguration, ListGateways, UpdateGatewayUpdateGatewayCapabilityConfiguration, DescribeStorageConfiguration, PutStorageConfiguration, DescribeDefaultEncryptionConfiguration, ListTagsForResource, PutDefaultEncryptionConfiguration, TagResource, et UntagResource.

Le point de terminaison VPC de l'interface pour les opérations d'API du plan de contrôle prend uniquement en charge le point de terminaison consolidé. Pour plus d'informations, consultez Points de terminaison d'un VPC .

Utilisez ce point de terminaison pour accéder aux opérations d'API suivantes : DescribeStorageConfigurationPutStorageConfigurationDescribeDefaultEncryptionConfiguration, ListTagsForResource, PutDefaultEncryptionConfiguration, TagResource, et UntagResource. Remplacez *region* par votre AWS région.

Utilisez ce point de terminaison pour accéder aux opérations d'API suivantes : AssociateAssetsCreateAssetCreateAssetModelDeleteAsset, DeleteAssetModel, DeleteDashboard, DescribeAsset, DescribeAssetModel, DescribeAssetProperty, DescribeDashboard,, DescribeLoggingOptions, DisassociateAssets, ListAssetModels, ListAssetRelationships, ListAssets, ListAssociatedAssets, PutLoggingOptions, UpdateAsset UpdateAssetModel, et UpdateAssetProperty. Remplacez *region* par votre AWS région.

Utilisez ce point de terminaison pour accéder aux opérations d'API suivantes : CreateGatewayDeleteGatewayDescribeGateway, DescribeGatewayCapabilityConfiguration, ListGateways, UpdateGateway, et UpdateGatewayCapabilityConfiguration. Remplacez *region* par votre AWS région.

Utilisez ce point de terminaison pour accéder aux opérations d'API suivantes : BatchAssociateProjectAssetsBatchDisassociateProjectAssetsCreateAccessPolicyCreateDashboard, CreatePortal, CreateProject, DeleteAccessPolicy, DeletePortal, DeleteProject, DescribeAccessPolicy,, DescribePortal, DescribeProject, ListAccessPolicies, ListDashboards,

ListPortals, ListProjectAssets, ListProjects, UpdateAccessPolicy , UpdateDashboardUpdatePortal, et UpdateProject. Remplacez *region* par votre AWS région.

AWS IoT SiteWise quotas

Les tableaux suivants décrivent les quotas dans AWS IoT SiteWise. Pour plus d'informations sur les quotas et sur la manière de demander des augmentations de quotas, consultez la section sur les quotas de AWS service dans le Références générales AWS. Pour plus d'informations sur les AWS IoT SiteWise quotas, consultez la section sur les quotas de AWS IoT SiteWise service dans le Références générales AWS.

Quotas pour les actifs et les modèles d'actifs

Ressource	Quota	Ajustable	Remarques
Nombre de modèles d'actifs par région et par AWS compte	1 000	Oui	
Nombre d'actifs par modèle d'actifs	10 000	Oui	
Nombre d'actifs enfants par actif parent	2000	Oui	
Profondeur de l'arbre hiérarchique du modèle d'actifs	30	Oui	
Nombre de définitions hiérarchiques par modèle d'actif	30	Oui	
Nombre de propriétés au niveau racine par modèle d'actif	500	Oui	Ce nombre maximum de `assetModelProperties` pour chaque modèle d'actif. Ce

Ressource	Quota	Ajustable	Remarques
			décompte n'inclut pascomposite ModelProp erties . Ce quota s'applique également à tout actif unique créé à partir de ce modèle d'actif.
Nombre de propriétés par modèle d'actif	5000	Oui	Le nombre maximum de propriétés d'un modèle d'actif de type ASSET_MOD EL ouCOMPONENT _MODEL . Ce nombre est déterminé en combinant les propriétés du modèle d'actif racine et de tout modèle composite inclus component-model-based ou en ligne. Ce quota s'applique également à tout actif unique créé à partir de ce modèle d'actif.

Ressource	Quota	Ajustable	Remarques
Nombre de propriétés par modèle composite	100	Oui	Nombre maximal de propriétés autorisées pour les modèles composites. En outre, le nombre maximum de propriétés autorisées pour un modèle d'actif de type `COMPONENT_MODEL` .
Profondeur de l'arborescence des propriétés par modèle d'actif	10	Non	Par exemple, un modèle avec une propriété de transformation C qui consomme une propriété de transformation B qui consomme une propriété de mesure A a une profondeur de 3.
Nombre de modèles d'actifs par arborescence de hiérarchie	100	Oui	

Ressource	Quota	Ajustable	Remarques
Nombre de propriétés directement dépendantes par modèle d'actif	20	Non	Ce quota limite le nombre de propriétés pouvant dépendre directement d'une propriété unique, tel que défini dans les expressions de formule de propriété. Le nombre de propriétés dépendantes d'un modèle d'actif doit être supérieur au nombre de propriétés directement dépendantes par modèle d'actif. Vous devez demander une augmentation du quota pour les deux si la limite du nombre de propriétés directement dépendantes par modèle d'actif est supérieure à la limite du nombre de propriétés dépendantes par modèle d'actif.

Ressource	Quota	Ajustable	Remarques
Nombre de propriétés dépendantes par modèle d'actif	30	Non	Ce quota limite le nombre de propriétés pouvant dépendre directement ou indirectement d'une propriété unique, tel que défini dans les expressions de formule de propriété.
Nombre de modèles composites par modèle d'actif	50	Oui	Le nombre maximum de modèles composites autorisés sur un seul modèle d'actif.
Profondeur du modèle composite	2	Oui	Profondeur maximale de l'arbre du modèle composite par modèle d'actif, y compris les modèles en ligne et component-model-based composites.
Nombre de modèles d'actifs uniques utilisant le même modèle de composant	20	Oui	Nombre maximal de modèles d'actifs uniques dotés d'au moins un modèle component-model-based composite faisant directement référence à un modèle d'actif spécifique de type COMPONENT_MODEL.

Ressource	Quota	Ajustable	Remarques
Nombre de variables de propriété par expression de formule de propriété	10	Non	Par exemple, il existe deux variables de propriété, `power` et `temp`, dans l'expression `avg(power) + max(temp)` . Cela s'applique également aux résultats des calculs de transformation.
Nombre de fonctions par expression de formule de propriété	10	Non	Par exemple, il existe deux fonctions, `avg` et `max`, dans l'expression `avg(power) + max(temp)` .

Quotas pour les données sur les ressources

Ressource	Quota	Ajustable	Remarques
Taux de demande pour les opérations d'API de données des ressources	1000 demandes par seconde, par région et par AWS compte	Oui	Ce quota s'applique aux opérations d'API telles que `GetAssetPropertyValue` et `BatchPutAssetPropertyValue` .
Nombre de points de données par seconde par qualité des données par propriété d'actif	10 points de données	Non	Ce quota s'applique au nombre maximum de points de données timestamp-quality-value (TQV) avec

Ressource	Quota	Ajustable	Remarques
			le même horodatage en secondes par qualité de données pour chaque propriété d'actif. Vous pouvez stocker jusqu'à ce nombre de points de données de bonne qualité, de qualité incertaine et de mauvaise qualité par seconde pour chaque propriété d'actif.
Nombre d'`BatchPutAssetPropertyValue` entrées ingérées par seconde par propriété d'actif, par région et par AWS compte.	10 entrées par propriété d'actif	Non	Ce quota s'applique aux `BatchPutAssetPropertyValue` entrées provenant de toutes les sources, y compris les passerelles SiteWise Edge, AWS IoT Core les règles et les appels d'API.
Taux de points de données ingérés	5000 points de données par seconde par région et par AWS compte	Oui	Points de données Timestamp-quality-value (TQV).

Ressource	Quota	Ajustable	Remarques
Tarif de demande pour `BatchGetAssetPropertyAggregates`	200	Oui	Le nombre maximum de `BatchGetAssetPropertyAggregates` demandes par seconde que vous pouvez effectuer sur ce compte dans la région actuelle.
Tarif de demande pour `BatchGetAssetPropertyValue`	500	Oui	Le nombre maximum de `BatchGetAssetPropertyValue` demandes par seconde que vous pouvez effectuer sur ce compte dans la région actuelle.
Tarif de demande pour `BatchGetAssetPropertyValueHistory`	200	Oui	Le nombre maximum de `BatchGetAssetPropertyValueHistory` demandes par seconde que vous pouvez effectuer sur ce compte dans la région actuelle.

Ressource	Quota	Ajustable	Remarques
Nombre d'`BatchPutAssetPropertyValue` entrées ingérées par seconde par propriété d'actif, par région et par AWS compte.	10 entrées par propriété d'actif	Non	Ce quota s'applique aux `BatchPutAssetPropertyValue` entrées provenant de toutes les sources, y compris les passerelles SiteWise Edge, AWS IoT Core les règles et les appels d'API.
Taux de `GetAssetPropertyAggregates` demandes et de requêtes de `BatchGetAssetPropertyAggregates` saisie par propriété d'actif	50	Non	Nombre total maximum de `GetAssetPropertyAggregates` demandes et d'`BatchGetAssetPropertyAggregates` entrées pour chaque propriété d'actif par seconde dans ce compte dans la région actuelle.

Ressource	Quota	Ajustable	Remarques
Taux de `GetAssetPropertyValue` demandes et de requêtes de `BatchGetAssetPropertyValue` saisie par propriété d'actif	500	Non	Nombre total maximum de `GetAssetPropertyValue` demandes et d'`BatchGetAssetPropertyValue` entrées pour chaque propriété d'actif par seconde dans ce compte dans la région actuelle.
Taux de `GetAssetPropertyValueHistory` demandes et de requêtes de `BatchGetAssetPropertyValueHistory` saisie par propriété d'actif	30	Non	Nombre total maximum de `GetAssetPropertyValueHistory` demandes et d'`BatchGetAssetPropertyValueHistory` entrées pour chaque propriété d'actif par seconde dans ce compte dans la région actuelle.

Ressource	Quota	Ajustable	Remarques
Taux de `GetInterpolatedAssetPropertyValues` demandes	500	Oui	Le nombre maximum de `GetInterpolatedAssetPropertyValues` demandes par seconde que vous pouvez effectuer sur ce compte dans la région actuelle.
Nombre de résultats par `GetInterpolatedAssetPropertyValues` demande	10	Oui	Le nombre maximum de résultats à renvoyer par `GetInterpolatedAssetPropertyValues` demande paginée.

Ressource	Quota	Ajustable	Remarques
Taux de points de données extraits de et `GetAssetPropertyValueHistory` `BatchGetAssetPropertyValueHistory`	100 Mo de réponse en lecture par seconde, par région et par AWS compte.	Oui	Débit maximal (Mo/seconde) des points de données récupérés par seconde, par région et par compte sur et. AWS `GetAssetPropertyValueHistory` `BatchGetAssetPropertyValueHistory` La charge utile de réponse évaluée pour ce quota utilise des champs Timestamp-Quality-Value (TQV) pour chaque point de données et arrondit la taille en octets de chaque demande d'API au prochain incrément de 4 Ko. Les points de données T imestamp-quality-value (TQV) récupérés par seconde varient en fonction du type de données : • Nombre entier : jusqu'à 5 millions

Ressource	Quota	Ajustable	Remarques
			de TQV par seconde • Double : jusqu'à 4 millions de TQV par seconde • Booléen : jusqu'à 6 millions de TQV par seconde • Chaîne : varie en fonction de la taille de chaque valeur de chaîne.

Quotas pour les passerelles SiteWise Edge

Ressource	Quota	Ajustable
Nombre de passerelles SiteWise Edge par région et par compte AWS	100	Oui
Nombre de sources OPC-UA par passerelle Edge SiteWise	100	Non

Quotas pour AWS IoT SiteWise Monitor

Ressource	Quota	Ajustable
Nombre de portails par région et par AWS compte	100	Oui
Nombre de projets par portail	100	Oui
Nombre de tableaux de bord par projet	100	Oui

Ressource	Quota	Ajustable
Nombre de ressources racine par projet	1	Non
Nombre de visualisations par tableau de bord	10	Oui
Nombre de métriques par visualisation du tableau de bord	5	Oui
Nombre de seuils par visualisation du tableau de bord	12	Non

Quotas pour l'importation et l'exportation AWS IoT SiteWise groupées de métadonnées

Ressource	Description	Quota	Ajustable
Nombre de tâches de transfert de métadonnées en file d'attente	Nombre maximal de tâches de transfert de `PENDING` métadonnées dans la file d'attente.	10	Oui
Taille du fichier d'importation des tâches de transfert de métadonnées	Taille maximale du fichier importé (en Mo).	100 Mo	Oui
AWS IoT SiteWise quota de ressources pour une tâche de transfert de métadonnées	Le nombre maximum de ressources importées ou exportées dans une seule tâche. Une ressource inclut des actifs et des modèles d'actifs.	5000	Non

Quotas pour l'importation AWS IoT SiteWise en masse de données

Ressource	Quota	Ajustable
Nombre de tâches d'importation en bloc en cours	100	Non
Taille du fichier CSV	10 Go	Non
Taille du fichier de parquet non compressé	256 Mo	Non
Taille du CSV fichier pour l'ingestion en mémoire tampon	256 Mo	Non
Taille du groupe de rangées de parquet non compressé	64 MO	Non
Nombre de mesures uniques par groupe de rangées de parquet	2000	Oui
Nombre de jours entre l'horodatage antérieur et actuel pour l'ingestion en mémoire tampon	30	Oui
Taux de demande `CreateBulkImportJobs` pour chaque région dans chaque AWS compte	10	Oui
Taux de demande `ListBulkImportJobs` pour chaque région dans chaque AWS compte	50	Oui
Taux de demande `DescribeBulkImport`	50	Oui

Ressource	Quota	Ajustable
`Jobs` pour chaque région dans chaque AWS compte		

Quotas pour la détection des anomalies

Les quotas de détection des anomalies sont partagés entre Amazon Lookout for Equipment AWS IoT SiteWise et Amazon Lookout for Equipment. Pour plus d'informations, consultez la section Quotas d'utilisation de Lookout for Equipment.

Historique du document pour le guide de AWS IoT SiteWise l'utilisateur

Le tableau suivant décrit la documentation de cette version de AWS IoT SiteWise.

- Version de l'API : 2019-12-02

Modification	Description	Date
Ajout de la prise en charge de l'exécution d' SiteWise Edge sur Siemens Industrial Edge	AWS IoT SiteWise prend désormais en charge l'exécution d' SiteWise Edge sur les appareils Siemens Industrial Edge.	26 novembre 2023
Support supplémentaire pour le stockage à chaud	AWS IoT SiteWise prend désormais en charge le stockage à chaud, un niveau de stockage entièrement géré qui permet aux clients de stocker et d'accéder facilement en toute sécurité aux données industrielles.	15 novembre 2023
Ajout de la prise en charge des identifiants uniques définis par l'utilisateur	AWS IoT SiteWise prend désormais en charge l'utilisation d'identifiants uniques définis par l'utilisateur pour les actifs, les modèles d'actifs, les propriétés et les hiérarchies.	15 novembre 2023
Ajout de la prise en charge de la détection d'anomalies à plusieurs variables dans les actifs industriels	AWS IoT SiteWise prend désormais en charge la détection des anomalies multidimensionnelles des actifs industriels en intégrant	15 novembre 2023

	les données historiques et en temps réel des équipemen ts à Amazon Lookout for Equipment.	
Support supplémentaire pour une ingestion rentable et évolutive de données de séries chronologiques dans AWS IoT SiteWise	AWS IoT SiteWise prend désormais en charge l'ingesti on rentable et évolutive des données chronologiques nécessaires aux cas d'utilisa tion analytiques.	15 novembre 2023
Ajout de la prise en charge de l'importation, de l'exportation et de la mise à jour en masse	AWS IoT SiteWise prend désormais en charge l'importa tion, l'exportation et la mise à jour en masse des métadonné es des équipements industrie ls.	15 novembre 2023
Ajout de la prise en charge des composants du modèle d'actifs	AWS IoT SiteWise prend désormais en charge les composants du modèle Asset pour aider les clients industrie ls à créer des composants réutilisables.	15 novembre 2023
Ajout de la prise en charge de l'application de tableau de bord IoT	AWS IoT SiteWise prend désormais en charge une application de tableau de bord open source dans laquelle vous pouvez visualiser et interagir avec les données opérationnelles.	15 novembre 2023

Mise à jour des rôles liés à un service pour AWS IoT SiteWise	AWS IoT SiteWise possède de nouveaux rôles liés aux services et peut exécuter une requête de recherche de métadonnées dans la AWS IoT TwinMaker base de données.	6 novembre 2023
Balisage mis à jour pour les ressources AWS IoT SiteWise de flux de données	Ajout du support pour le balisage des ressources de flux de données.	18 août 2022
Passerelles SiteWise Edge mises à jour	Vous pouvez désormais configurer l'éditeur pour contrôler les données envoyées de la périphérie vers le cloud et l'ordre dans lequel elles sont envoyées vers le cloud.	12 janvier 2022
Mise à jour de la AWS IoT SiteWise démo	Vous pouvez désormais utiliser la démo pour créer un portail SiteWise Monitor.	10 janvier 2022
Gestion du stockage actualisée	Vous pouvez désormais définir une période de conservation pour contrôler la durée de conservation de vos données dans le hot tier.	29 novembre 2021
Support supplémentaire pour la gestion des flux de données	Vous pouvez désormais ingérer des données AWS IoT SiteWise avant de créer des modèles d'actifs et des actifs.	24 novembre 2021

Hiérarchies de modèles d'actifs mises à jour	Un modèle d'actif enfant peut désormais être associé à plusieurs modèles d'actifs parents.	28 octobre 2021
Lancement de la région	Lancé AWS IoT SiteWise en AWS GovCloud (ouest des États-Unis).	29 septembre 2021
Fonctions mises à jour	Ajout des fonctionnalités suivantes • Dans les métriques, vous pouvez utiliser des expressions imbriquées dans les fonctions d'agrégation et les fonctions temporelles. • Dans les transformations, vous pouvez utiliser la fonction pretrigger () pour récupérer la valeur d'une variable avant la mise à jour de la propriété qui a déclenché le calcul de transformation en cours.	10 août 2021
Intervalle de temps métrique personnalisé	Ajout de la prise en charge des intervalles de temps personnalisés et des décalages dans les métriques.	3 août 2021
Utilisation AWS IoT SiteWise sur le bord	La fonction de traitement des bords est désormais disponible pour tous.	29 juillet 2021

Exportation de données vers Amazon S3	AWS IoT SiteWise peut désormais exporter des données vers Amazon S3.	27 Juillet 2021
Points de terminaison VPC ()AWS PrivateLink	Le point de terminaison VPC de l'interface pour les opérations de l'API du plan de contrôle est désormais généralement disponible.	15 juillet 2021
Transforme	Les transformations peuvent désormais saisir plusieurs variables de propriétés d'actifs.	8 juillet 2021
Mise à jour de la fonction timestamp ()	Dans les transformations, vous pouvez désormais fournir une variable comme argument à la `timestamp()` fonction.	16 juin 2021
Disponibilité générale des alarmes	La fonction d'alarmes est désormais disponible pour tous.	27 mai 2021
Sortie de la version 2 de l'adaptateur de protocole Modbus-TCP	La version 2 du connecteur adaptateur de protocole Modbus-TCP est disponible. Cette version a ajouté la prise en charge des chaînes sources codées en ASCII, UTF8 et ISO8859.	24 mai 2021

Quotas de service actualisés	Ajout des quotas suivants pour l'GetInterpolatedAssetPropertyValuesAPI : taux de `GetInterpolatedAssetPropertyValues` demandes, nombre de résultats par `GetInterpolatedAssetPropertyValues` demande et nombre de jours entre la date de début passée et la date d'aujourd'hui pour`GetInterpolatedAssetPropertyValues` .	29 avril 2021
Expressions de formule mises à jour	Les opérateurs et fonctions suivants ont été ajoutés : • Les opérateurs suivants ont été ajoutés : `<` `>` `<=`,`,>=`,`==`,`!=`,`!`,`and`,`or`, et`not`. • Ajout de la fonction de comparaison suivante : `neq(x, y)` • Les fonctions de chaîne suivantes ont été ajoutées : `join()``format()`, et`f''`.	22 avril 2021
Points de terminaison VPC ()AWS PrivateLink	Ajout d'informations sur la façon d'établir une connexion privée entre votre cloud privé virtuel (VPC) et les API du plan de AWS IoT SiteWise contrôle en créant un point de terminaison VPC d'interface.	16 mars 2021

Fédération IAM	Les administrateurs et utilisateurs de votre portail SiteWise Monitor peuvent désormais se connecter aux portails qui leur sont assignés avec leurs informations d'identification IAM.	16 mars 2021
Lancement de la région	Lancé AWS IoT SiteWise en Chine (Pékin).	3 février 2021
Sortie de la version 10 du SiteWise connecteur IoT	La version 10 du SiteWise connecteur IoT est disponible. Cette version est configurée `StreamManager` pour améliorer la gestion lorsque la connexion source est perdue puis rétablie. Cette version accepte également les valeurs OPC-UA avec un `ServerTimestamp` lorsque non `SourceTimestamp` est disponible.	22 janvier 2021
Fonctions de date et d'heure	AWS IoT SiteWise prend désormais en charge les fonctions de date et d'heure.	21 janvier 2021
Syntaxe des fonctions	Vous pouvez désormais utiliser la syntaxe UFCS (Uniform Function Call Syntax) pour les AWS IoT SiteWise fonctions.	11 janvier 2021

Intégration à Grafana	Ajout d'informations sur la façon de visualiser les AWS IoT SiteWise données dans les tableaux de bord Grafana.	15 décembre 2020

AWS IoT SiteWise sortie de fonctionnalités	Vous pouvez désormais surveiller vos données à l'aide d'alarmes, traiter les données industrielles en périphérie, utiliser des sources Modbus TCP et EtherNet/IP pour votre passerelle SiteWise Edge, filtrer les données entrantes avec des zones mortes, etc. • Ajout de la section Surveillance des données avec alarmes que vous pouvez utiliser pour définir, configurer et répondre aux alarmes AWS IoT SiteWise. • Ajout de la section Traitement Edge que vous pouvez utiliser pour configurer le traitement de vos données industrielles sur vos appareils Edge. • Les sections Modbus TCP et EtherNet/IP ont été ajoutées à la documentation source de la passerelle SiteWise Edge. • Ajout de la section source et destination que vous pouvez utiliser pour personnaliser l'endroit où vous envoyez vos données industrielles entrantes. • Ajout de la section de filtrage OPC-UA que vous pouvez utiliser pour	15 décembre 2020

	contrôler la fréquence et le type de données envoyées à votre passerelle SiteWise Edge depuis votre serveur local industriel.	
AWS IoT SiteWise prend désormais en charge les CMK gérées par le client.	AWS IoT SiteWise prend désormais en charge le chiffrement avec des CMK gérées par le client.	24 novembre 2020
Sortie de la version 8 du SiteWise connecteur IoT	La version 8 du SiteWise connecteur IoT est disponible. Cette version améliore la stabilité lorsque le connecteur est confronté à une connectivité réseau intermittente.	19 novembre 2020
Utilisation de chaînes et de conditions dans les expressions de formule	Ajout d'informations sur la façon d'utiliser des chaînes et des fonctions conditionnelles dans les expressions de formule pour les transformations et les métriques.	16 novembre 2020
Ingestion de données à l'aide du gestionnaire de AWS IoT Greengrass flux	Ajout d'informations sur la façon d'ingérer de gros volumes de données IoT à partir de sources de données locales à l'aide d'un appareil AWS IoT Greengrass périphérique.	16 septembre 2020

Points de terminaison VPC ()AWS PrivateLink	Ajout d'informations sur la façon d'établir une connexion privée entre votre cloud privé virtuel (VPC) et les API de AWS IoT SiteWise données en créant un point de terminaison VPC d'interface.	4 septembre 2020
Sortie de la version 7 du SiteWise connecteur IoT	La version 7 du SiteWise connecteur IoT est disponibl e. Cette version résout un problème lié aux métriques de la passerelle SiteWise Edge.	14 août 2020
Création d'utilisateurs IAM Identity Center à partir de la console AWS IoT SiteWise	Ajout d'informations sur la façon dont vous pouvez créer des utilisateurs IAM Identity Center dans la AWS IoT SiteWise console. Vous pouvez désormais créer des utilisateurs IAM Identity Center lorsque vous attribuez des utilisateurs à un portail nouveau ou existant. Mise à jour du didacticiel sur la visualisation et le partage de données de parcs éoliens pour utiliser cette fonctionnalité. Cette modification réduit le nombre d'étapes du didacticiel.	4 août 2020
Résolution améliorée des problèmes liés à la passerelle SiteWise Edge	Ajout d'informations supplémentaires sur le dépannage d'une passerell e SiteWise Edge et l'exporta tion du certificat client OPC-UA pour une source.	18 juin 2020

Documentation des tâches liées à la console	Ajout de la documentation des tâches de la console pour Modélisation des ressources industrielles, Interrogation des données de propriété de ressource et Interaction avec d'autres services. Vous pouvez suivre ces instructions pour effectuer des tâches dans la console AWS IoT SiteWise .	11 juin 2020
Tutoriel d'analyse des données exportées	Ajout d'un didacticiel que vous pouvez suivre pour apprendre à utiliser Amazon Athena pour analyser les données d'actifs que vous avez exportées vers S3 à l'aide du modèle de fonctionnalité AWS CloudFormation d'exportation.	27 mai 2020
Amélioré à l'aide d'expressions de formule	Ajout d'informations détaillées sur le comportement des propriétés des AWS IoT SiteWise formules et ajout d'un exemple expliquant comment compter les points de données filtrés.	18 mai 2020

Sortie de la version 6 du SiteWise connecteur IoT	La version 6 du SiteWise connecteur IoT est disponible. Cette version ajoute la prise en charge des CloudWatch métriques et de la découverte automatique des nouvelles balises OPC-UA. Cela signifie que vous n'avez pas besoin de redémarrer votre passerelle SiteWise Edge lorsque les balises de vos sources OPC-UA changent. Cette version du connecteur nécessite le gestionnaire de flux et le logiciel AWS IoT Greengrass Core v1.10.0 ou supérieur.	29 avril 2020

AWS IoT SiteWise sortie de fonctionnalités	AWS IoT SiteWise sortie de fonctionnalité. Vous pouvez désormais gérer les passerelles SiteWise Edge avec l'API, ajouter votre logo aux portails, consulter les statistiques des passerelles SiteWise Edge, etc. • La section Exportation de données vers Amazon S3 a été ajoutée avec un AWS CloudFormation modèle que vous pouvez utiliser pour exporter de nouvelles valeurs de données vers un compartiment S3. • Ajout de la section Configuration des sources de données qui améliore la documentation des sources de passerelle SiteWise Edge et inclut les nouvelles API de passerelle SiteWise Edge. • Ajout de la section des métriques de passerelle SiteWise Edge qui décrit les CloudWatch métriques publiées par les passerelles SiteWise Edge. • Ajout de la section Configuration d'une passerelle SiteWise Edge sur Amazon EC2 avec un AWS CloudFormation	29 avril 2020

	modèle que vous pouvez utiliser pour configurer rapidement les dépendances d'une passerelle SiteWise Edge sur une instance Amazon EC2. • Ajout de la section sur les rôles des services de portail qui décrit la nouvelle fonctionnalité d'autorisation des portails SiteWise Monitor. • Mise à jour de la documentation du portail pour les rôles de service du portail et les logos du portail. • La section Marquage de vos AWS IoT SiteWise ressources a été ajoutée. • Mise à jour de la section Création de tableaux de bord (CLI) pour la nouvelle structure de définition de tableau de bord. • Ajout de la section Sécurité.	
Ingestion de données depuis AWS IoT Events	Ajout d'informations sur la façon d'ingérer des données à partir du AWS IoT Events moment où un événement se produit.	20 avril 2020

Visualisation et partage de données de parcs éoliens dans le didacticiel SiteWise Monitor	Ajout d'un didacticiel que vous pouvez suivre pour apprendre à visualiser et AWS IoT SiteWise Monitor à partager les données des actifs.	12 mars 2020
AWS IoT SiteWise concepts	Ajout d'un glossaire de AWS IoT SiteWise concepts que vous pouvez utiliser pour en savoir plus sur le service et ses termes courants.	5 mars 2020
Instructions AWS IoT Greengrass d'installation supprimées	Les instructions d'installation du logiciel AWS IoT Greengras s Core ont été supprimées du guide de AWS IoT SiteWise l'utilisateur. Le guide du AWS IoT Greengrass développeur propose un script de configura tion de l'appareil et des instructions à configurer AWS IoT Greengrass sur d'autres plateformes telles qu'Amazon EC2 et Docker.	14 février 2020
Amélioration de l'ingestion de données à l'aide de règles AWS IoT Core	Ajout d'informations détaillée s sur la façon d'utiliser et de résoudre les problèmes liés à l'action de la AWS IoT SiteWise règle, que vous pouvez utiliser pour ingérer des données provenant de messages MQTT via. AWS IoT Core	14 février 2020

Sortie de la version 5 du SiteWise connecteur IoT	La version 5 du SiteWise connecteur IoT est disponible. Cette version corrige un problème de compatibilité avec le logiciel AWS IoT Greengrass Core v1.9.4.	12 février 2020
Sortie de la version 4 du SiteWise connecteur IoT	La version 4 du SiteWise connecteur IoT est disponible. Cette version résout un problème lié à la reconnexion du serveur OPC-UA.	7 février 2020
Modélisation restructurée des actifs industriels	Restructuration de la section sur la mise à jour des ressources et des modèles en plusieurs rubriques dans la section sur la modélisation des ressources industrielles. • État des ressources et des modèles • Mappage des flux de données industrielles avec des propriétés de ressources • Mise à jour des valeurs d'attribut • Association et dissociation de ressources • Mise à jour des ressources et des modèles • Suppression des ressources et des modèles	4 février 2020

Tutoriel sur l'ingestion de données depuis AWS IoT des objets	Ajout d'un didacticiel que vous pouvez suivre pour apprendre à configurer une action de AWS IoT SiteWise règle pour ingérer des données provenant d'un parc d' AWS IoT objets nouveau ou existant.	4 février 2020
Restructuration de la récupération des données depuis AWS IoT SiteWise	Restructuration de la section Extraction des données en deux sections de niveau supérieur : Interaction avec les valeurs et les agrégats des propriétés des actifs et interaction avec d'autres services. AWS	21 janvier 2020
Publication de mises à jour de la valeur des propriétés dans le didacticiel Amazon DynamoDB	Ajout d'un didacticiel que vous pouvez suivre pour apprendre à utiliser les notifications de valeur de propriété pour stocker les données des actifs dans DynamoDB.	8 janvier 2020
Utilisation d'expressions de formule	Ajout de la référence d'expression de formule pour l'organisation des constantes et des fonctions disponibles pour une utilisation dans les propriétés de transformation et de métriques Restructuration de la section sur les propriétés de ressource en rubriques distinctes pour chaque type de propriété.	7 janvier 2020

Utilisation des filtres de nœuds OPC-UA	Ajout d'informations sur l'utilisation des filtres de nœuds OPC-UA pour améliorer les performances de la passerelle SiteWise Edge lors de l'ajout de sources de passerelle SiteWise Edge.	3 janvier 2020
Mise à niveau d'un connecteur	Ajout d'informations sur la mise à niveau d'une passerelle SiteWise Edge lorsqu'une nouvelle version du connecteur est publiée.	30 décembre 2019
Sortie de la version 3 du SiteWise connecteur IoT	La version 3 du SiteWise connecteur IoT est disponible. Cette version supprime l'exigence d'autorisations iot:*.	17 décembre 2019
Sortie de la version 2 du SiteWise connecteur IoT	La version 2 du SiteWise connecteur IoT est disponible. Cette version ajoute la prise en charge de plusieurs ressources secrètes OPC-UA.	10 décembre 2019
Création de tableaux de bord ()AWS CLI	Ajout d'informations sur la création d'un tableau de bord à AWS IoT SiteWise Monitor l'aide du AWS CLI.	6 décembre 2019

AWS IoT SiteWise sortie de la version 2	Aperçu publié pour la version 2 de AWS IoT SiteWise. Vous pouvez désormais ingérer des données via OPC-UA, MQTT et HTTP, modéliser vos données dans des hiérarchies d'actifs et visualiser vos données avec Monitor. SiteWise • Réécriture de la section relative à la modélisation des ressources pour les modifications apportées aux ressources, aux modèles de ressources et aux hiérarchies de ressources. • Mise à jour de la section d'ingestion de données pour inclure les étapes AWS IoT Greengrass du connecteur et les sections d'ingestion de données non liées à la passerelle. • Ajout de la AWS IoT SiteWise Monitorsection et d'un guide d'application distinct qui montre comment utiliser l'application Web SiteWise Monitor. • Ajout des sections Interrogez les données de AWS IoT SiteWise et Interaction avec d'autres AWS services. • Réécriture de la section relative à la mise en route	2 décembre 2019

	pour correspondance avec l'expérience de démonstration mise à jour.	
AWS IoT SiteWise sortie de la version 1	Aperçu initial publié pour la version 1 de AWS IoT SiteWise.	25 février 2019

Glossaire AWS

Pour connaître la terminologie la plus récente d'AWS, consultez le Glossaire AWS dans la Référence Glossaire AWS.

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.