aws

Guide de l’utilisateur

EventBridge Planificateur

EventBridge Planificateur: Guide de l’utilisateur

Table of Contents

Qu'est-ce que le EventBridge planificateur Amazon ?

Amazon EventBridge Scheduler est un planificateur sans serveur qui vous permet de créer, d'exécuter et de gérer des tâches à partir d'un service géré central. Hautement évolutif, EventBridge Scheduler vous permet de planifier des millions de tâches pouvant appeler plus de 270AWS services et plus de 6 000 opérations d'API. Sans avoir à provisionner et à gérer l'infrastructure, ni à intégrer plusieurs services, EventBridge Scheduler vous permet de respecter des calendriers à grande échelle et de réduire les coûts de maintenance.

EventBridge Scheduler fournit vos tâches de manière fiable, grâce à des mécanismes intégrés qui ajustent vos calendriers en fonction de la disponibilité des cibles en aval. Avec EventBridge Scheduler, vous pouvez créer des plannings à l'aide d'expressions cron et rate pour des modèles récurrents, ou configurer des invocations ponctuelles. Vous pouvez configurer des créneaux horaires flexibles pour la livraison, définir des limites de nouvelles tentatives et définir la durée de rétention maximale pour les déclencheurs ayant échoué.

Rubriques

Principales fonctionnalités de EventBridge Scheduler

EventBridge Le planificateur propose les fonctionnalités clés suivantes que vous pouvez utiliser pour configurer des cibles et adapter vos calendriers.

- Cibles modélisées : le EventBridge planificateur prend en charge les cibles modélisées pour effectuer des opérations d'API courantes à l'aide d'Amazon SQS, Amazon SNS, Lambda et EventBridge. Avec des cibles prédéfinies, vous pouvez configurer rapidement vos calendriers à l'aide de la console EventBridge EventBridge Scheduler, du SDK Scheduler ou duAWS CLI.
- Cibles universelles : le EventBridge planificateur fournit un paramètre cible universel (UTP) que vous pouvez utiliser pour créer des déclencheurs personnalisés qui ciblent plus de 270AWS services et plus de 6 000 opérations d'API selon un calendrier. Avec UTP, vous pouvez configurer vos déclencheurs personnalisés à l'aide de la console EventBridge EventBridge Scheduler, du SDK Scheduler ou duAWS CLI.
- Fenêtres horaires flexibles : le EventBridge planificateur prend en charge des fenêtres horaires flexibles, ce qui vous permet de disperser vos calendriers et d'améliorer la fiabilité de vos

déclencheurs pour les cas d'utilisation qui ne nécessitent pas d'invocation planifiée précise de cibles.

- Réessais : le EventBridge planificateur fournit des at-least-once événements aux cibles, ce qui signifie qu'au moins une diffusion aboutit à une réponse de la part de la cible. EventBridge Le planificateur vous permet de définir le nombre de nouvelles tentatives de votre calendrier en cas d'échec d'une tâche. EventBridge Le planificateur réessaie les tâches ayant échoué avec des tentatives différées afin d'améliorer la fiabilité de votre calendrier et de garantir la disponibilité des cibles.

Accès au EventBridge planificateur

Vous pouvez utiliser EventBridge Scheduler via la console EventBridge Scheduler, le SDK EventBridge Scheduler ou directement à l'aide de l'API EventBridge Scheduler.AWS CLI

Configuration d'Amazon EventBridge Scheduler

Avant de pouvoir utiliser le EventBridge planificateur, vous devez suivre les étapes suivantes.

Rubriques

Inscrivez-vous à AWS

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

Pour s'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 souscrivez à un Compte AWS, un Utilisateur racine d'un compte AWS est créé. Par défaut, seul l'utilisateur root a accès à l'ensemble des Services AWS et des ressources de ce compte. En tant que bonne pratique de sécurité, attribuer un accès administratif à un utilisateur administratif, et utilisez uniquement l'utilisateur root pour effectuer tâches nécessitant un accès utilisateur root.

Créer un utilisateur IAM

Afin de créer un utilisateur administrateur, choisissez l'une des options suivantes :

Choisissez un moyen de gérer votre administrateur	Pour	Bit	Vous pouvez également
Dans IAM Identity Center (Recommandé)	Utiliser des identifiants à court terme pour accéder à AWS. Telles sont les meilleures pratiques en matière de sécurité. Pour plus d'informations sur les bonnes pratiques, consultez Security best practices in IAM (Bonnes pratiques de sécurité dans IAM) dans le Guide de l'utilisateur IAM.	Suivre les instructions de la section Mise en route dans le AWS IAM Identity Center Guide de l'utilisateur.	Configuration de l'accès par programmation en Configurant le AWS CLI à utiliser AWS IAM Identity Centerdans le AWS Command Line Interface Guide de l'utilisateur.
Dans IAM (Non recommandé)	Utiliser des identifiants à long terme pour accéder à AWS.	Suivre les instructions relatives à la Création de votre premier groupe utilisateur administrateur et utilisateur IAM dans le Guide de l'utilisateur IAM.	Configuration de l'accès par programmation via la Gestion des clés d'accès pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Utiliser des politiques gérées

À l'étape précédente, vous avez configuré un utilisateur IAM avec les informations d'identification nécessaires pour accéder à vos AWS ressources. Dans la plupart des cas, pour utiliser le

EventBridge planificateur en toute sécurité, nous vous recommandons de créer des utilisateurs, des groupes ou des rôles distincts dotés uniquement des autorisations nécessaires pour utiliser EventBridge le planificateur. EventBridge Le planificateur prend en charge les politiques gérées suivantes pour les cas d'utilisation courants.

- the section called "`AmazonEventBridgeSchedulerFullAccess`"— Accorde un accès complet au EventBridge planificateur à l'aide de la console et de l'API.
- the section called "`AmazonEventBridgeSchedulerReadOnlyAccess`"— Accorde un accès en lecture seule au planificateur. EventBridge

Vous pouvez associer ces politiques gérées à vos principaux IAM de la même manière que vous les avez associées à l'`AdministratorAccess`étape précédente. Pour plus d'informations sur la gestion de l'accès au EventBridge planificateur à l'aide de politiques IAM basées sur l'identité, consultez. the section called "Utilisation de politiques basées sur l'identité"

Configurer le rôle d'exécution

Un rôle d'exécution est un rôle IAM que EventBridge Scheduler assume afin d'interagir avec d'autres personnes en votre Services AWS nom. Vous associez des politiques d'autorisation à ce rôle pour autoriser le EventBridge planificateur à appeler des cibles.

Vous pouvez également créer un nouveau rôle d'exécution lorsque vous utilisez la console pour créer un nouveau calendrier. Si vous utilisez la console, EventBridge Scheduler crée un rôle en votre nom avec des autorisations en fonction de la cible que vous avez choisie. Lorsque EventBridge Scheduler crée un rôle pour vous, la politique de confiance du rôle inclut des clés de condition qui limitent les principaux autorisés à assumer le rôle en votre nom. Cela permet d'éviter toute confusion potentielle en matière de sécurité des adjoints.

Les étapes suivantes décrivent comment créer un nouveau rôle d'exécution et comment accorder à EventBridge Scheduler l'accès pour invoquer une cible. Cette rubrique décrit les autorisations pour les cibles modélisées les plus populaires. Pour plus d'informations sur l'ajout d'autorisations pour d'autres cibles, consultezthe section called "Utilisation de cibles modélisées".

Pour créer un rôle d'exécution à l'aide du AWS CLI

1. Copiez la politique JSON de prise de rôle suivante et enregistrez-la localement sous le nom de`Scheduler-Execution-Role.json`. Cette politique de confiance permet à EventBridge Scheduler d'assumer le rôle en votre nom.

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

> **Important**
>
> Pour configurer un rôle d'exécution dans un environnement de production, nous vous recommandons de mettre en œuvre des mesures de protection supplémentaires afin d'éviter toute confusion liée aux adjoints. Pour plus d'informations et un exemple de politique, consultezthe section called “Prévention de l'adjoint confus”.

2. À partir du AWS Command Line Interface (AWS CLI), entrez la commande suivante pour créer un nouveau rôle. *SchedulerExecutionRole*Remplacez-le par le nom que vous souhaitez attribuer à ce rôle.

```
$ aws iam create-role --role-name SchedulerExecutionRole --assume-role-policy-
document file://Scheduler-Execution-Role.json
```

En cas de succès, vous verrez le résultat suivant :

```
{
    "Role": {
        "Path": "/",
        "RoleName": "Scheduler-Execution-Role",
        "RoleId": "BR1L2DZK3K4CTL5ZF9EIL",
        "Arn": "arn:aws:iam::123456789012:role/SchedulerExecutionRole",
        "CreateDate": "2022-03-10T18:45:01+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
```

```
                {
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "scheduler.amazonaws.com"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }
    }
}
```

3. Pour créer une nouvelle politique permettant au EventBridge Scheduler d'invoquer une cible, choisissez l'une des cibles communes suivantes. Copiez la politique d'autorisation JSON et enregistrez-la localement sous forme de `.json` fichier.

   Amazon SQS – SendMessage

   Ce qui suit permet au EventBridge planificateur d'appeler l'`sqs:SendMessage`action sur toutes les files d'attente Amazon SQS de votre compte.

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

   Amazon SNS – Publish

   Ce qui suit permet au EventBridge planificateur de lancer l'`sns:Publish`action sur toutes les rubriques Amazon SNS de votre compte.

   ```
   {
       "Version": "2012-10-17",
       "Statement": [
   ```

```
        {
            "Action": [
                "sns:Publish"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Lambda – Invoke

Ce qui suit permet au EventBridge Scheduler d'appeler l'`lambda:InvokeFunction`action sur toutes les fonctions Lambda de votre compte.

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

4. Exécutez la commande suivante pour créer la nouvelle politique d'autorisation. *PolicyName*Remplacez-le par le nom que vous souhaitez donner à cette politique.

```
$ aws iam create-policy --policy-name PolicyName --policy-document file://
PermissionPolicy.json
```

En cas de succès, vous verrez le résultat suivant. Notez l'ARN de la politique. Vous utiliserez cet ARN à l'étape suivante pour associer la politique à notre rôle d'exécution.

```
{
    "Policy": {
        "PolicyName": "PolicyName",
        "CreateDate": "2022-03-015T19:31:18.620Z",
        "AttachmentCount": 0,
```

```
        "IsAttachable": true,
        "PolicyId": "ZXR6A36LTYANPAI7NJ5UV",
        "DefaultVersionId": "v1",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:policy/PolicyName",
        "UpdateDate": "2022-03-015T19:31:18.620Z"
    }
}
```

5. Exécutez la commande suivante pour associer la politique à votre rôle d'exécution. *your-policy-arn*Remplacez-le par l'ARN de la politique que vous avez créée à l'étape précédente. *SchedulerExecutionRole*Remplacez-le par le nom de votre rôle d'exécution.

```
$ aws iam attach-role-policy --policy-arn your-policy-arn --role-
name SchedulerExecutionRole
```

   L'`attach-role-policy`opération ne renvoie pas de réponse sur la ligne de commande.

Définissez un objectif

Avant de créer un planning EventBridge Scheduler, vous devez invoquer au moins une cible pour votre planning. Vous pouvez utiliser une AWS ressource existante ou en créer une nouvelle. Les étapes suivantes montrent comment créer une nouvelle file d'attente Amazon SQS standard avec. AWS CloudFormation

Pour créer une nouvelle file d'attente Amazon SQS

1. Copiez le AWS CloudFormation modèle JSON suivant et enregistrez-le localement sous le nom de`SchedulerTargetSQS.json`.

```
{
   "AWSTemplateFormatVersion": "2010-09-09",
   "Resources": {
      "MyQueue": {
         "Type": "AWS::SQS::Queue",
         "Properties": {
            "QueueName": "MyQueue"
             }
         }
      },
```

```
   "Outputs": {
      "QueueName": {
         "Description": "The name of the queue",
         "Value": {
            "Fn::GetAtt": [
               "MyQueue",
               "QueueName"
            ]
         }
      },
      "QueueURL": {
         "Description": "The URL of the queue",
         "Value": {
            "Ref": "MyQueue"
         }
      },
      "QueueARN": {
         "Description": "The ARN of the queue",
         "Value": {
            "Fn::GetAtt": [
               "MyQueue",
               "Arn"
            ]
         }
      }
   }
}
```

2. À partir duAWS CLI, exécutez la commande suivante pour créer une AWS CloudFormation pile à partir du `Scheduler-Target-SQS.json` modèle.

```
$ aws cloudformation create-stack --stack-name Scheduler-Target-SQS --template-body
 file://Scheduler-Target-SQS.json
```

En cas de succès, vous verrez le résultat suivant :

```
{
    "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/Scheduler-
Target-SQS/1d2af345-a121-12eb-abc1-012e34567890"
}
```

3. Exécutez la commande suivante pour afficher les informations récapitulatives de votre AWS CloudFormation stack. Ces informations incluent l'état de la pile et les sorties spécifiées dans le modèle.

```
$ aws cloudformation describe-stacks --stack-name Scheduler-Target-SQS
```

En cas de succès, la commande crée la file d'attente Amazon SQS et renvoie le résultat suivant :

```
{
    "Stacks": [
        {
            "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/
Scheduler-Target-SQS/1d2af345-a121-12eb-abc1-012e34567890",
            "StackName": "Scheduler-Target-SQS",
            "CreationTime": "2022-03-17T16:21:29.442000+00:00",
            "RollbackConfiguration": {},
            "StackStatus": "CREATE_COMPLETE",
            "DisableRollback": false,
            "NotificationARNs": [],
            "Outputs": [
                {
                    "OutputKey": "QueueName",
                    "OutputValue": "MyQueue",
                    "Description": "The name of the queue"
                },
                {
                    "OutputKey": "QueueARN",
                    "OutputValue": "arn:aws:sqs:us-west-2:123456789012:MyQueue",
                    "Description": "The ARN of the queue"
                },
                {
                    "OutputKey": "QueueURL",
                    "OutputValue": "https://sqs.us-
west-2.amazonaws.com/123456789012/MyQueue",
                    "Description": "The URL of the queue"
                }
            ],
            "Tags": [],
            "EnableTerminationProtection": false,
            "DriftInformation": {
                "StackDriftStatus": "NOT_CHECKED"
            }
```

```
        }
    ]
}
```

Plus loin dans ce guide, vous utiliserez la valeur `QueueARN` pour configurer la file d'attente en tant que cible pour EventBridge Scheduler.

Quelle est la prochaine étape ?

Une fois l'étape de configuration terminée, utilisez le guide de démarrage pour créer votre premier EventBridge planificateur Scheduler et invoquer une cible.

Commencer à utiliser EventBridge Scheduler

Cette rubrique décrit la création d'un nouveau calendrier du EventBridge planificateur. Vous utilisez la console EventBridge Scheduler AWS Command Line Interface (AWS CLI) ou les AWS kits SDK pour créer un calendrier avec un modèle de cible Amazon SQS. Vous allez ensuite configurer la journalisation, configurer les nouvelles tentatives et définir une durée de rétention maximale pour les tâches ayant échoué. Après avoir créé le calendrier, vous allez vérifier qu'il invoque correctement la cible et envoie un message à la file d'attente cible.

> **Note**
>
> Pour suivre ce guide, nous vous recommandons de configurer les utilisateurs IAM avec les autorisations minimales requises décrites dansthe section called "Utilisation de politiques basées sur l'identité". Après avoir créé et configuré un utilisateur, exécutez la commande suivante pour définir vos informations d'accès. Vous aurez besoin de votre identifiant de clé d'accès et de votre clé d'accès secrète pour configurer leAWS CLI.
>
> ```
> $ aws configure
> AWS Access Key ID [None]: AKIAIOSFODNN7EXAMPLE
> AWS Secret Access Key [None]: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
> Default region name [None]: us-west-2
> Default output format [None]: json
> ```
>
> Pour plus d'informations sur les différentes manières de définir vos informations d'identification, consultez la section Paramètres de configuration et priorité dans le Guide de l'AWS Command Line Interfaceutilisateur de la version 2.

Rubriques

Prérequis

Avant de suivre les étapes décrites dans cette section, vous devez effectuer les opérations suivantes :

- Effectuez les tâches décrites dans Configuration

Création d'un calendrier à l'aide de la console EventBridge Scheduler

Pour créer un nouveau calendrier à l'aide de la console

1. Connectez-vous auAWS Management Console, puis cliquez sur le lien suivant pour ouvrir la section EventBridge Planificateur de la EventBridge console : https://us-west-2.console.aws.amazon.com/scheduler/home?region=us-west-2#home

   > **Note**
   >
   > Vous pouvez changer de région Région AWS en utilisant le sélecteur AWS Management Console de région.

2. Sur la page Planifications, choisissez Créer une planification.
3. Sur la page Spécifier le détail de la planification, dans la section Nom et description de la planification, procédez comme suit :

   a. Pour Nom de la planification, saisissez un nom à attribuer à votre planification. Par exemple, **`MyTestSchedule`**

   b. Dans Description (facultatif), entrez une description pour votre planning. Par exemple, **`My first schedule`**.

   c. Pour le groupe de planification, choisissez un groupe de planification dans les options du menu déroulant. Si vous n'avez encore créé aucun groupe de planning, vous pouvez choisir le `default` groupe correspondant à votre planning. Pour créer un nouveau groupe de planning, cliquez sur le lien « Créez votre propre planning » dans la description de la console. Vous utilisez des groupes de planifications pour leur ajouter des balises.

4. Dans la section Schéma de planification, procédez comme suit :

a. Pour Occurrence, choisissez l'une des options de modèle suivantes. Les options de configuration changent en fonction du modèle que vous sélectionnez.

   - Calendrier ponctuel : un calendrier ponctuel n'invoque un objectif qu'une seule fois, à la date et à l'heure que vous spécifiez.

     Pour Date et heure, entrez une date valide dans le `YYYY/MM/DD` format. Spécifiez ensuite un horodatage au format 24 heureshh`:mm`. Enfin, choisissez un fuseau horaire dans les options du menu déroulant.
   - Calendrier récurrent : un calendrier récurrent invoque un objectif à un taux que vous spécifiez à l'aide d'une cron expression ou d'une expression de taux.

     Choisissez la planification basée sur Cron pour configurer une planification à l'aide d'une cron expression. Pour utiliser une expression de taux, choisissez la planification basée sur le taux et entrez un nombre positif pour la valeur, puis choisissez une unité dans les options du menu déroulant.

   Pour plus d'informations sur l'utilisation des expressions cron et rate, consultezTypes d'horaires.

b. Pour la fenêtre horaire flexible, choisissez Désactivé pour désactiver l'option, ou choisissez l'une des fenêtres temporelles prédéfinies dans la liste déroulante. Par exemple, si vous choisissez15 minutes et que vous définissez une planification récurrente pour invoquer son objectif une fois par heure, la planification s'exécute dans les 15 minutes suivant le début de chaque heure.

5.
> **Note**
>
> La fonctionnalité de fenêtre horaire flexible n'est pas disponible pour les horaires ponctuels.

Si vous avez choisi Calendrier récurrent à l'étape précédente, dans la section Période, spécifiez un fuseau horaire et définissez éventuellement une date et une heure de début, ainsi qu'une date et une heure de fin pour le calendrier. Un calendrier récurrent sans date de début commence dès qu'il est créé et disponible. Un planning récurrent sans date de fin continuera à invoquer son objectif indéfiniment.

6. Choisissez Suivant.

7. Sur la page Sélectionner une cible, procédez comme suit :

   a. Sélectionnez des cibles modélisées et choisissez une API cible. Pour cet exemple, nous allons choisir la cible modélisée Amazon SQS. **`SendMessage`**

   b. SendMessageDans la section, pour la file d'attente SQS, choisissez un ARN de file d'attente Amazon SQS existant, par exemple `arn:aws:sqs:us-west-2:123456789012:TestQueue` dans la liste déroulante. Pour créer une nouvelle file d'attente, choisissez Create new SQS Queue pour accéder à la console Amazon SQS. Après avoir créé une file d'attente, revenez à la console du EventBridge planificateur et actualisez le menu déroulant. Le nouvel ARN de votre file d'attente apparaît et peut être sélectionné.

   c. Pour Target, entrez la charge utile que EventBridge Scheduler doit envoyer à la cible. Pour cet exemple, nous allons envoyer le message suivant à la file d'attente cible : **`Hello, it's EventBridge Scheduler.`**

8. Choisissez Suivant, puis sur la page Paramètres - facultatif, procédez comme suit :

9.
   a. Dans la section État de la planification, pour Activer la planification, activez ou désactivez la fonctionnalité à l'aide du commutateur. Par défaut, le EventBridge planificateur active votre planning.

   b. Dans la section Action une fois le planning terminé, configurez l'action que le EventBridge planificateur exécute une fois le planning terminé :

      - Choisissez SUPPRIMER si vous souhaitez que le planning soit automatiquement supprimé. Pour les plannings ponctuels, cela se produit une fois que le planning a invoqué la cible une fois. Pour les plannings récurrents, cela se produit après le dernier appel planifié du planning. Pour plus d'informations sur la suppression automatique, consultezthe section called “Suppression une fois le planning terminé”.
      - Choisissez AUCUNE, ou ne choisissez aucune valeur, si vous ne souhaitez pas que le EventBridge planificateur prenne des mesures une fois le planning terminé.

   c. Dans la section Politique de rétentatives et file d'attente de lettres mortes (DLQ), pour la politique de réessai, activez Réessayer pour configurer une politique de nouvelles tentatives adaptée à votre calendrier. Avec les politiques de nouvelle tentative, si un calendrier ne parvient pas à invoquer sa cible, le EventBridge planificateur le réexécute. Si elle est configurée, vous devez définir la durée de rétention maximale et les nouvelles tentatives pour la planification.

d. Pour Âge maximum de l'événement (facultatif), entrez le nombre maximum d'heures et de minutes pendant lequel le EventBridge planificateur doit conserver un événement non traité.

> **Note**
>
> La valeur maximale est de 24 heures.

e. Pour Nombre maximum de tentatives, entrez le nombre maximum de fois que le EventBridge planificateur réessaie le calendrier si la cible renvoie une erreur.

> **Note**
>
> La valeur maximale est 185 nouvelles tentatives.

f. Pour la file d'attente des lettres mortes (DLQ), choisissez l'une des options suivantes :

- Aucun — Choisissez cette option si vous ne souhaitez pas configurer de DLQ.
- Sélectionnez une file d'attente Amazon SQS dans mon AWS compte en tant que DLQ : choisissez cette option, puis sélectionnez un ARN de file d'attente dans la liste déroulante, configurez un DLQ Compte AWS identique à celui dans lequel vous créez le planning.
- Spécifiez une file d'attente Amazon SQS dans un autre AWS compte en tant que DLQ : choisissez cette option, puis entrez l'ARN de la file d'attente configurée en tant que DLQ, si la file d'attente se trouve dans un autre compte. Compte AWS Vous devez saisir l'ARN exact de la file d'attente pour pouvoir utiliser cette option.

g. Dans la section Chiffrement, choisissez Personnaliser les paramètres de chiffrement (avancés) pour utiliser une clé KMS gérée par le client afin de chiffrer votre entrée cible. Si vous choisissez cette option, entrez un ARN de clé KMS existant ou choisissez Créer une clé AWS KMS pour accéder à la AWS KMS console. Pour plus d'informations sur la façon dont EventBridge Scheduler chiffre vos données au repos, consultez. the section called "Chiffrement au repos"

h. Pour Autorisations, choisissez Utiliser le rôle existant, puis sélectionnez le rôle que vous avez créé lors de la procédure de configuration dans la liste déroulante. Vous pouvez également choisir Accéder à la console IAM pour créer un nouveau rôle.

   Si vous souhaitez que le EventBridge planificateur crée un nouveau rôle d'exécution pour vous, choisissez plutôt Créer un nouveau rôle pour ce calendrier. Ensuite, saisissez un nom

pour Nom du rôle. Si vous choisissez cette option, le EventBridge planificateur ajoute au rôle les autorisations requises pour votre cible modélisée.

10. Choisissez Suivant.
11. Sur la page Examiner et créer une planification, examinez les détails de votre planification. Dans chaque section, choisissez Modifier pour revenir à cette étape et modifier ses détails.
12. Choisissez Créer un calendrier pour terminer la création de votre nouveau calendrier. Vous pouvez consulter la liste de vos planifications nouvelles et existantes sur la page Planifications. Sous la colonne État, vérifiez que votre nouvelle planification est activée.
13. Pour vérifier que votre planning invoque la cible Amazon SQS, ouvrez la console Amazon SQS et procédez comme suit :

    a. Choisissez la file d'attente cible dans la liste des files d'attente.

    b. Choisissez Send and receive messages (Envoyer et recevoir des messages).

    c. Sur la page Envoyer et recevoir des messages, sous Recevoir des messages, choisissez Rechercher des messages pour récupérer les messages de test que votre planning a envoyés à la file d'attente cible.

Créez un calendrier à l'aide du AWS CLI

L'exemple suivant montre comment utiliser la AWS CLI commande pour `create-schedule`créer un planning EventBridge Scheduler avec un modèle de cible Amazon SQS. Remplacez les valeurs d'espace réservé pour les paramètres suivants par vos informations :

- --name — Entrez un nom pour le calendrier.
- RoleArn— Entrez l'ARN du rôle d'exécution que vous souhaitez associer au planning.
- Arn — Entrez l'ARN de la cible. Dans ce cas, la cible est une file d'attente Amazon SQS.
- Entrée — Entrez un message que le EventBridge planificateur envoie à la file d'attente cible.

```
$ aws scheduler create-schedule --name sqs-templated-schedule --schedule-expression
 'rate(5 minutes)' \
--target '{"RoleArn": "ROLE_ARN", "Arn": "QUEUE_ARN", "Input": "TEST_PAYLOAD" }' \
--flexible-time-window '{ "Mode": "OFF"}'
```

Créez un calendrier à l'aide des SDK du EventBridge planificateur

Dans l'exemple suivant, vous utilisez les SDK du EventBridge planificateur pour créer un calendrier du EventBridge planificateur avec un modèle de cible Amazon SQS.

Example SDK Python

```
import boto3
scheduler = boto3.client('scheduler')

flex_window = { "Mode": "OFF" }

sqs_templated = {
    "RoleArn": "<ROLE_ARN>",
    "Arn": "<QUEUE_ARN>",
    "Input": "Message for scheduleArn: '<aws.scheduler.schedule-arn>', scheduledTime:
 '<aws.scheduler.scheduled-time>'"
}

scheduler.create_schedule(
    Name="sqs-python-templated",
    ScheduleExpression="rate(5 minutes)",
    Target=sqs_templated,
    FlexibleTimeWindow=flex_window)
```

Example Kit SDK Java

```
package com.example;

import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.scheduler.SchedulerClient;
import software.amazon.awssdk.services.scheduler.model.*;


public class MySchedulerApp {

    public static void main(String[] args) {

        final SchedulerClient client = SchedulerClient.builder()
                .region(Region.US_WEST_2)
                .build();
```

```
        Target sqsTarget = Target.builder()
                .roleArn("<ROLE_ARN>")
                .arn("<QUEUE_ARN>")
                .input("Message for scheduleArn: '<aws.scheduler.schedule-arn>',
 scheduledTime: '<aws.scheduler.scheduled-time>'")
                .build();

        CreateScheduleRequest createScheduleRequest = CreateScheduleRequest.builder()
                .name("<SCHEDULE NAME>")
                .scheduleExpression("rate(10 minutes)")
                .target(sqsTarget)
                .flexibleTimeWindow(FlexibleTimeWindow.builder()
                        .mode(FlexibleTimeWindowMode.OFF)
                        .build())
                .build();

        client.createSchedule(createScheduleRequest);
        System.out.println("Created schedule with rate expression and an Amazon SQS
 templated target");
    }
}
```

Quelle est la prochaine étape ?

- Pour plus d'informations sur la gestion de votre planning à l'aide de la console ou du SDK du EventBridge planificateurAWS CLI, consultez. Gestion d'un planning
- Pour plus d'informations sur la configuration de cibles modélisées et sur l'utilisation du paramètre de cible universel, consultezGestion des cibles.
- Pour plus d'informations sur les types de données et les opérations d'API du EventBridge planificateur, consultez la référence de l'API du EventBridge planificateur.

Types de planification sur le EventBridge planificateur

La rubrique suivante décrit les différents types d'horaires pris en charge par Amazon EventBridge Scheduler, ainsi que la façon dont EventBridge Scheduler gère l'heure d'été et la planification dans différents fuseaux horaires. Vous pouvez choisir entre trois types de planification lors de la configuration de votre calendrier : les programmes basés sur les taux, les programmes basés sur des crons et les programmes ponctuels.

Les programmes basés sur les taux et ceux basés sur le cron sont des programmes récurrents. Vous configurez chaque type de planification récurrente à l'aide d'une expression de planification correspondant au type de planification que vous souhaitez configurer et en spécifiant le fuseau horaire dans lequel le EventBridge planificateur évalue l'expression.

Un calendrier ponctuel est un calendrier qui n'appelle une cible qu'une seule fois. Vous configurez un calendrier ponctuel en spécifiant l'heure, la date et le fuseau horaire dans lesquels le EventBridge planificateur évalue le calendrier.

> **Note**
>
> Tous les types de planification sur EventBridge Scheduler invoquent leurs cibles avec une précision de 60 secondes. Cela signifie que si vous définissez votre planning pour qu'il s'exécute à`1:00`, il invoquera l'API cible entre `1:00:00` et`1:00:59`.

Utilisez les sections suivantes pour en savoir plus sur la configuration des expressions de planification pour chaque type de planification récurrente et sur la façon de configurer une planification ponctuelle dans le EventBridge planificateur.

Rubriques

Horaires basés sur les tarifs

Un calendrier basé sur des taux commence après la date de début que vous spécifiez pour votre programme et s'exécute à un rythme régulier que vous définissez jusqu'à la date de fin du calendrier. Vous pouvez configurer les cas d'utilisation de la planification récurrente les plus courants à l'aide d'une planification basée sur les taux. Par exemple, si vous souhaitez un calendrier qui invoque son objectif toutes les 15 minutes, une fois toutes les deux heures ou une fois tous les cinq jours, vous pouvez utiliser un calendrier basé sur les taux pour y parvenir. Vous configurez une planification basée sur les taux à l'aide d'une expression de taux.

Dans le cas des programmes basés sur des taux, vous utilisez la `StartDate`propriété pour définir la première occurrence du calendrier. Si vous ne fournissez pas de `StartDate` calendrier basé sur le taux, votre calendrier commence à invoquer l'objectif immédiatement.

Les expressions de taux comportent deux champs obligatoires séparés par un espace blanc, comme indiqué ci-dessous.

Syntaxe

```
rate(value unit)
```

value

Nombre positif.

unité

L'unité de temps pendant laquelle vous souhaitez que votre emploi du temps invoque son objectif.

Entrées valides : `minutes` | `hours` | `days`

Exemples

L'exemple suivant montre comment utiliser des expressions de taux avec la AWS CLI `create-schedule` commande pour configurer une planification basée sur le taux. Cet exemple crée un planning qui s'exécute toutes les cinq minutes et envoie un message à une file d'attente Amazon SQS, en utilisant le type de cible modélisé. `SqsParameters`

Dans la mesure où cet exemple ne définit pas de valeur pour le `--start-date` paramètre, le calendrier commence à appeler sa cible immédiatement après sa création et son activation.

```
$ aws scheduler create-schedule --schedule-expression 'rate(5 minutes)' --
name schedule-name \
--target '{"RoleArn": "role-arn", "Arn": "QUEUE_ARN", "Input": "TEST_PAYLOAD" }' \
--flexible-time-window '{ "Mode": "OFF"}'
```

Horaires basés sur CRON

Une expression cron crée un calendrier récurrent précis qui s'exécute à un moment précis de votre choix. EventBridge Le planificateur prend en charge la configuration des horaires basés sur le cron en temps universel coordonné (UTC) ou dans le fuseau horaire que vous spécifiez lors de la création de votre calendrier. Avec les plannings basés sur des crons, vous pouvez mieux contrôler le moment et la fréquence d'exécution de votre planning. Utilisez des programmes basés sur des crons lorsque vous avez besoin d'un calendrier de récurrence personnalisé qui n'est pas pris en charge par l'une des expressions de taux du EventBridge planificateur. Par exemple, vous pouvez créer un calendrier basé sur des crons qui s'exécute à 8 h 00. PST le premier lundi de chaque mois par exemple. Vous configurez un calendrier basé sur cron à l'aide d'une expression cron.

Une expression cron se compose de cinq champs obligatoires séparés par des espaces : minutes day-of-month, heures day-of-week, mois et un champ facultatif, année, comme indiqué ci-dessous.

Syntaxe

```
cron(minutes hours day-of-month month day-of-week year)
```

Champ	Valeurs	Caractères génériques
Minutes	0-59	, - * /
Heures	0-23	, - * /
D ay-of-month	1-31	, - * ? / L W
Mois	1-12 ou JAN-DEC	, - * /
D ay-of-week	1-7 ou DIM-SAM	, - * ? L #
Année	1970-2199	, - * /

Caractères génériques

- Le caractère générique , (virgule) inclut des valeurs supplémentaires. Dans le champ Month, JAN,FEB,MAR englobe January, February et March.
- Le caractère générique - (tiret) spécifie des plages. Dans le champ Day, 1-15 englobe les jours 1 à 15 du mois spécifié.
- Le caractère générique * (astérisque) inclut toutes les valeurs du champ. Dans le champ Hours (Heures), * inclut toutes les heures. Vous ne pouvez pas utiliser * à la fois dans les ay-of-week champs D ay-of-month et D. Si vous l'utilisez dans un champ, vous devez utiliser ? dans l'autre.
- Le caractère générique / (barre oblique) spécifie les incréments. Dans le champ Minutes, vous pouvez entrer 1/10 pour spécifier toutes les dix minutes, à partir de la première minute de l'heure (par exemple, les 11e, 21e, 31e minutes, et ainsi de suite).
- Le caractère générique ? (point d'interrogation) indique l'un ou l'autre. Dans le ay-of-month champ D, vous pouvez saisir 7 et si un jour de la semaine vous convient, vous pouvez saisir ? dans le ay-of-week champ D.
- Le caractère générique L dans les ay-of-week champs D ay-of-month ou D indique le dernier jour du mois ou de la semaine.
- Le **`W`** caractère générique dans le ay-of-month champ D indique un jour de la semaine. Dans le ay-of-month champ D, **`3W`** indique le jour de la semaine le plus proche du troisième jour du mois.
- Le caractère générique # dans le ay-of-week champ D indique une certaine instance du jour de la semaine spécifié dans un délai d'un mois. Par exemple, 3#2 correspond au deuxième mardi du mois : le 3 fait référence à mardi, car c'est le troisième jour de chaque semaine, et le 2 fait référence à la deuxième journée de ce type dans le mois.

> **Note**
>
> Si vous utilisez un caractère « # », vous ne pouvez définir qu'une seule expression dans le day-of-week champ. Par exemple, `"3#1,6#3"` n'est pas valide, car il est interprété comme deux expressions.

Exemples

L'exemple suivant montre comment utiliser des expressions cron avec la AWS CLI `create-schedule` commande pour configurer un planning basé sur cron. Cet exemple crée un calendrier qui s'exécute à 10 h 15 UTC+0 le dernier vendredi de chaque mois pendant les années 2022 à

2023, et envoie un message à une file d'attente Amazon SQS, en utilisant le type de cible modélisé. `SqsParameters`

```
$ aws scheduler create-schedule --schedule-expression "cron(15 10 ? * 6L 2022-2023)" --
name schedule-name \
--target '{"RoleArn": "role-arn", "Arn": "QUEUE_ARN", "Input": "TEST_PAYLOAD" }' \
--flexible-time-window '{ "Mode": "OFF"}'
```

Planifications ponctuelles

Un calendrier ponctuel n'invoquera une cible qu'une seule fois à la date et à l'heure que vous spécifiez à l'aide d'une date valide et d'un horodatage. EventBridge Le planificateur prend en charge la planification en temps universel coordonné (UTC) ou dans le fuseau horaire que vous spécifiez lors de la création de votre calendrier.

> **Note**
>
> Un calendrier ponctuel est toujours pris en compte dans le quota de votre compte une fois qu'il a été exécuté et que son objectif a été atteint. Nous vous recommandons de supprimer vos programmes ponctuels une fois leur exécution terminée.

Vous configurez un calendrier ponctuel à l'aide d'une expression at. Une expression at correspond à la date et à l'heure auxquelles vous souhaitez que EventBridge Scheduler appelle votre calendrier, comme indiqué ci-dessous.

Syntaxe

```
at(yyyy-mm-ddThh:mm:ss)
```

Lorsque vous configurez un calendrier ponctuel, le EventBridge planificateur ignore le `StartDate` et `EndDate` que vous spécifiez pour le calendrier.

Exemples

L'exemple suivant montre comment utiliser des expressions at avec la AWS CLI `create-schedule` commande pour configurer un calendrier ponctuel. Cet exemple crée un calendrier qui s'exécute une

fois à 13 h UTC-8 le 20 novembre 2022 et envoie un message à une file d'attente Amazon SQS, en utilisant le type de cible modélisé. `SqsParameters`

```
$ aws scheduler create-schedule --schedule-expression "at(2022-11-20T13:00:00)" --
name schedule-name \
--target '{"RoleArn": "role-arn", "Arn": "QUEUE_ARN", "Input": "TEST_PAYLOAD" }' \
--schedule-expression-timezone "America/Los_Angeles"
--flexible-time-window '{ "Mode": "OFF"}'
```

Fuseaux horaires sur le EventBridge planificateur

EventBridge Le planificateur prend en charge la configuration de calendriers ponctuels et basés sur des crons dans tous les fuseaux horaires que vous spécifiez. EventBridge Le planificateur utilise la base de données de fuseaux horaires gérée par l'Internet Assigned Numbers Authority (IANA).

Avec leAWS CLI, vous pouvez définir le fuseau horaire dans lequel vous souhaitez que EventBridge Scheduler évalue votre planning à l'aide du `--schedule-expression-timezone` paramètre. Par exemple, la commande suivante crée un calendrier basé sur un cron qui invoque un modèle de cible Amazon SQS dans America/New_York tous les **`SendMessage`** jours à 8 h 30.

```
$ aws scheduler create-schedule --schedule-expression "cron(30 8 * * ? *)" --name
 schedule-in-est \
    --target '{"RoleArn": "role-arn", "Arn": "QUEUE_ARN", "Input": "This schedule runs
 in the America/New_York time zone." }' \
    --schedule-expression-timezone "America/New_York"
    --flexible-time-window '{ "Mode": "OFF"}'
```

Heure d'été sur EventBridge Scheduler

EventBridge Le planificateur ajuste automatiquement votre emploi du temps en fonction de l'heure d'été. Lorsque le temps avance au printemps, si une expression cron tombe sur une date et une heure inexistantes, votre appel de calendrier est ignoré. Lorsque le temps recule à l'automne, votre emploi du temps ne s'exécute qu'une seule fois et ne répète pas son invocation. Les invocations suivantes se produisent normalement à la date et à l'heure spécifiées.

EventBridge Le planificateur ajuste votre emploi du temps en fonction du fuseau horaire que vous spécifiez lorsque vous créez le calendrier. Si vous configurez un horaire dans America/New_York, celui-ci s'ajuste lorsque l'heure change dans ce fuseau horaire, tandis qu'un horaire dans America/Los_Angeles est ajusté trois heures plus tard lorsque l'heure change sur la côte ouest.

Pour les horaires basés sur des taux `days` dont l'unité `days` représente, par exemple`rate(1 days)`, une durée de 24 heures au compteur. Cela signifie que lorsque l'heure d'été réduit un jour à 23 heures ou le prolonge à 25 heures, EventBridge Scheduler évalue toujours l'expression du taux 24 heures après le dernier appel du calendrier.

> **Note**
>
> Certains fuseaux horaires ne respectent pas l'heure d'été, conformément aux règles et réglementations locales. Si vous créez un horaire dans un fuseau horaire qui ne respecte pas l'heure d'été, le EventBridge planificateur ne l'ajuste pas. Les ajustements de l'heure d'été ne s'appliquent pas aux horaires en temps universel coordonné (UTC).

Exemple

Imaginons un scénario dans lequel vous créez un calendrier en utilisant l'expression cron suivante dans America/Los_Angeles :. `cron(30 2 * * ? *)` Ce programme fonctionne tous les jours à 2 h 30 dans le fuseau horaire indiqué.

- Printemps avancé — Lorsque le temps passe de 1 h 59 à 3 h 00 au printemps, le EventBridge planificateur ignore l'invocation du calendrier ce jour-là et reprend l'exécution du calendrier normalement le jour suivant.
- Solution de rechange — Lorsque le temps recule à l'automne de 2 h 59 à 2 h 00, le EventBridge planificateur exécute l'horaire une seule fois à 2 h 30 avant le changement de temps, mais ne répète pas l'invocation de l'horaire à 2 h 30 après le changement d'heure.

Gestion d'un planning

Un calendrier est la principale ressource que vous créez, configurez et gérez à l'aide d'Amazon EventBridge Scheduler.

Chaque planification possède une expression de planification qui détermine quand et à quelle fréquence elle s'exécute. EventBridge Le planificateur prend en charge trois types de plannings : les plannings rate, cron et les plannings ponctuels. Pour plus d'informations sur les différents types de planification, consultezTypes d'horaires.

Lorsque vous créez un planning, vous configurez une cible que le planning doit invoquer. Une cible est une opération d'API que EventBridge Scheduler appelle en votre nom à chaque exécution de votre planning. EventBridge Le planificateur prend en charge deux types de cibles : les cibles modélisées appellent des opérations d'API communes à des groupes principaux de services, et le paramètre de cible universel (UTP) que vous pouvez utiliser pour appeler plus de 6 000 opérations sur plus de 270 services. Pour plus d'informations sur la configuration des cibles, consultezGestion des cibles.

Vous configurez la manière dont votre calendrier gère les échecs lorsque le EventBridge planificateur ne parvient pas à transmettre un événement à une cible avec succès, en utilisant deux mécanismes principaux : une politique de nouvelles tentatives et une file d'attente de lettres mortes (DLQ). Une politique de nouvelle tentative détermine le nombre de fois que le EventBridge planificateur doit réessayer un événement ayant échoué, ainsi que la durée pendant laquelle un événement non traité doit être conservé. Un DLQ est un outil standard utilisé par le planificateur de EventBridge files d'attente Amazon SQS pour transmettre les événements ayant échoué, une fois que la politique de nouvelle tentative a été épuisée. Vous pouvez utiliser un DLQ pour résoudre les problèmes liés à votre calendrier ou à sa cible en aval. Pour plus d'informations sur, voirthe section called "Configuration d'une file d'attente de lettre morte".

Dans cette section, vous trouverez des exemples de gestion de vos plannings du EventBridge planificateur à l'aide de la console, du SDK AWS CLI et du EventBridge planificateur.

Rubriques

- Supprimer un planning
- Quelle est la prochaine étape ?

Modification de l'état du planning

Un EventBridge planning de planificateur possède deux états : activé et désactivé. L'exemple suivant permet `UpdateSchedule` de désactiver un calendrier qui se déclenche toutes les cinq minutes et invoque une cible Lambda.

Lors de l'utilisation`UpdateSchedule`, vous devez fournir tous les paramètres requis. EventBridge Le planificateur remplace votre emploi du temps par les informations que vous fournissez. Si vous ne spécifiez aucun paramètre que vous avez défini précédemment, sa valeur par défaut est. `null`

Example AWS CLI

```
$ aws scheduler update-schedule --name lambda-universal --schedule-expression 'rate(5
 minutes)' \
--target '{"RoleArn": "ROLE_ARN", "Arn":"arn:aws:scheduler:::aws-sdk:lambda:invoke"
 "Input": "{\"FunctionName\":\"arn:aws:lambda:REGION:123456789012:function:HelloWorld
\",\"InvocationType\":\"Event\",\"Payload\":\"{\\\"message\\\":\\\"testing function\\
\"}\"}" }' \
--flexible-time-window '{ "Mode": "OFF"}' \
--state DISABLED
```

```
{
    "ScheduleArn": "arn:aws:scheduler:us-west-2:123456789012:schedule/default/lambda-
universal"
}
```

L'exemple suivant utilise le SDK Python et l'`UpdateSchedule`opération pour désactiver un calendrier qui cible Amazon SQS à l'aide d'un modèle de cible.

Example Kit de développement logiciel pour Python

```
import boto3
scheduler = boto3.client('scheduler')

sqs_templated = {
    "RoleArn": "<ROLE_ARN>",
```

```
    "Arn": "<QUEUE_ARN>",
    "Input": "{}"}

flex_window = { "Mode": "OFF" }

scheduler.update_schedule(Name="your-schedule",
    ScheduleExpression="rate(5 minutes)",
    Target=sqs_templated,
    FlexibleTimeWindow=flex_window,
    State='DISABLED')
```

Configuration de fenêtres horaires flexibles

Lorsque vous configurez votre emploi du temps avec une fenêtre horaire flexible, le EventBridge planificateur invoque la cible dans le créneau horaire que vous avez défini. Cela est utile dans les cas qui ne nécessitent pas une invocation planifiée précise des cibles. La définition d'un créneau horaire flexible améliore la fiabilité de votre emploi du temps en répartissant vos invocations cibles.

Par exemple, si vous configurez une fenêtre horaire flexible de 15 minutes pour un calendrier exécuté toutes les heures, l'objectif est invoqué dans les 15 minutes suivant l'heure planifiée. Les exemples suivantsAWS CLI, ainsi que ceux du SDK EventBridge Scheduler, permettent `UpdateSchedule` de définir une fenêtre horaire flexible de 15 minutes pour un planning exécuté une fois par heure.

> **Note**
>
> Vous devez indiquer si vous souhaitez définir un créneau horaire flexible ou non. Si vous ne souhaitez pas définir cette option, spécifiez`OFF`. Si vous définissez la valeur sur`FLEXIBLE`, vous devez alors spécifier une fenêtre de temps maximale pendant laquelle votre planification sera exécutée.

Example AWS CLI

```
$ aws scheduler update-schedule --name lambda-universal --schedule-expression 'rate(1
 hour)' \
--target '{"RoleArn": "ROLE_ARN", "Arn":"arn:aws:scheduler:::aws-sdk:lambda:invoke"
 "Input": "{\"FunctionName\":\"arn:aws:lambda:REGION:123456789012:function:HelloWorld
\",\"InvocationType\":\"Event\",\"Payload\":\"{\\\"message\\\":\\\"testing function\\
\"}\"}" }' \
```

```
--flexible-time-window '{ "Mode": "FLEXIBLE", "MaximumWindowInMinutes": 15} \
```

```
{
    "ScheduleArn": "arn:aws:scheduler:us-west-2:123456789012:schedule/lambda-universal"
}
```

Example Kit de développement logiciel pour Python

```
import boto3
scheduler = boto3.client('scheduler')

sqs_templated = {
    "RoleArn": "<ROLE_ARN>",
    "Arn": "<QUEUE_ARN>",
    "Input": "{}"}

flex_window = { "Mode": "FLEXIBLE", "MaximumWindowInMinutes": 15}

scheduler.update_schedule(Name="your-schedule",
    ScheduleExpression="rate(1 hour)",
    Target=sqs_templated,
    FlexibleTimeWindow=flex_window)
```

Configuration d'une file d'attente lettres mortes pour un calendrier

Amazon EventBridge Scheduler prend en charge les files d'attente mortes (DLQ) à l'aide Amazon Simple Queue Service. Lorsqu'un calendrier ne parvient pas à appeler sa cible, EventBridge Scheduler envoie une charge utile JSON contenant les détails de l'appel et toute réponse reçue de la cible à une file d'attente standard Amazon SQS que vous spécifiez.

La rubrique suivante fait référence à ce JSON en tant qu'événement lettre morte. Un événement lettre morte vous permet de résoudre les problèmes liés à votre calendrier ou à vos objectifs. Si vous configurez une politique de nouvelles tentatives en fonction de votre calendrier, EventBridge Scheduler envoie l'événement lettre morte correspondant à l'épuisement du nombre maximum de tentatives que vous avez défini.

Les rubriques suivantes décrivent comment configurer une file d'attente Amazon SQS en tant que DLQ adaptée à votre emploi du temps, définir les autorisations dont le EventBridge planificateur a besoin pour envoyer des messages à Amazon SQS et recevoir des événements inactifs provenant du DLQ.

Rubriques

Créez une file d'attente Amazon SQS.

Avant de configurer une DLQ pour votre planning, vous devez créer une file d'attente Amazon SQS standard. Pour obtenir les instructions sur la création d'une file d'attente à l'aide de la console Amazon SQS, veuillez consulter la section Création d'une file d'attente Amazon SQS dans le guide du développeur Amazon Simple Queue Service.

> **Note**
>
> EventBridge Le planificateur ne prend pas en charge l'utilisation d'une file d'attente FIFO comme DLQ de votre calendrier.

Utilisez laAWS CLI commande suivante pour créer une file d'attente standard.

```
$ aws sqs create-queue --queue-name queue-name
```

Si l'opération aboutit, vous verrez le`QueueURL` dans la sortie.

```
{
    "QueueUrl": "https://sqs.us-west-2.amazonaws.com/123456789012/scheduler-dlq-test"
}
```

Après avoir créé la file d'attente, notez l'ARN de la file d'attente. Vous aurez besoin de l'ARN lorsque vous spécifierez un DLQ pour votre planning EventBridge Scheduler. Vous pouvez trouver l'ARN de votre file d'attente dans la console Amazon SQS ou à l'aide de la `get-queue-attributes`AWS CLIcommande.

```
$ aws sqs get-queue-attributes --queue-url your-dlq-url --attribute-names QueueArn
```

En cas de succès, vous verrez l'ARN de la file d'attente dans la sortie.

```
{
    "Attributes": {
        "QueueArn": "arn:aws:sqs:us-west-2:123456789012:scheduler-dlq-test"
    }
}
```

Dans la section suivante, vous allez ajouter les autorisations requises à votre rôle d'exécution du planning pour permettre à EventBridge Scheduler de transmettre des événements lettre morte à Amazon SQS.

Configurer les autorisations de rôle d'exécution

Pour permettre à EventBridge Scheduler de transmettre des événements lettre morte à Amazon SQS, votre rôle d'exécution du planning doit respecter la politique d'autorisation suivante. Pour plus d'informations sur l'association d'une nouvelle politique d'autorisation à votre rôle d'exécution du planning, consultez la section Configuration du rôle d'exécution.

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

> **Note**
>
> Votre rôle d'exécution du planning est peut-être déjà associé aux autorisations requises si vous utilisez EventBridge Scheduler pour appeler une cible d'API Amazon SQS.

Dans la section suivante, vous allez utiliser la console du EventBridge planificateur et définir un DLQ pour votre planning.

Spécifier une file d'attente de lettres mortes mortes mortes mortes mortes

Pour spécifier un DLQ, utilisez la console EventBridge Scheduler ouAWS CLI pour mettre à jour un calendrier existant ou en créer un nouveau.

Console

Pour spécifier un DLQ à l'aide de la console

1. Connectez-vous auAWS Management Console, puis cliquez sur le lien suivant pour ouvrir la section EventBridge Planificateur de EventBridge la console : https://console.aws.amazon.com/scheduler/home
2. Dans la console du EventBridge planificateur, créez un nouveau calendrier ou choisissez un calendrier existant dans votre liste de programmes à modifier.
3. Sur la page Paramètres, pour la file d'attente aux lettres mortes (DLQ), effectuez l'une des opérations suivantes :
   - Choisissez Sélectionner une file d'attente Amazon SQS dans monAWS compte en tant que DLQ, puis choisissez l'ARN de file d'attente pour votre DLQ dans la liste déroulante.
   - Choisissez Spécifier une file d'attente Amazon SQS dans d'autresAWS comptes en tant que DLQ, puis saisissez l'ARN de la file d'attente pour votre DLQ. Si vous choisissez une file d'attente dans un autreAWS compte, la console EventBridge Scheduler ne pourra pas afficher les ARN de la file d'attente dans une liste déroulante.
4. Vérifiez vos sélections, puis choisissez Créer un calendrier ou Enregistrer un calendrier pour terminer la configuration d'un DLQ.
5. (Facultatif) Pour afficher les détails de la DLQ d'un calendrier, choisissez le nom du calendrier dans la liste, puis choisissez l'onglet File d'attente aux lettres mortes sur la page de détail du calendrier.

AWS CLI

Pour mettre à jour un calendrier existant à l'aide duAWS CLI

- Utilisez la `update-schedule`commande pour mettre à jour votre calendrier. Spécifiez la file d'attente Amazon SQS que vous avez créée précédemment en tant que DLQ. Spécifiez l'ARN du rôle IAM auquel vous avez associé les autorisations Amazon SQS requises en

tant que rôle d'exécution. Remplacez toutes les autres valeurs d'espace réservé par vos informations.

```
$ aws scheduler update-schedule --name existing-schedule \
    --schedule-expression 'rate(5 minutes)' \
    --target '{"DeadLetterConfig": {"Arn": "DLQ_ARN"}, "RoleArn": "ROLE_ARN",
 "Arn":"QUEUE_ARN", "Input": "Hello world!" }' \
    --flexible-time-window '{ "Mode": "OFF"}'
```

Pour créer un nouveau calendrier avec un DLQ à l'aide duAWS CLI

- Utilisez la `create-schedule`commande pour créer un calendrier. Remplacez toutes les valeurs d'espace réservé par vos informations.

```
$ aws scheduler create-schedule --name new-schedule \
    --schedule-expression 'rate(5 minutes)' \
    --target '{"DeadLetterConfig": {"Arn": "DLQ_ARN"}, "RoleArn": "ROLE_ARN",
 "Arn":"QUEUE_ARN", "Input": "Hello world!" }' \
    --flexible-time-window '{ "Mode": "OFF"}'
```

Dans la section suivante, vous allez utiliser leAWS CLI pour recevoir un événement de lettres mortes de la part du DLQ.

Récupérez l'événement de lettres mortes mortes mortes

Utilisez la `receive-message`commande, comme indiqué ci-dessous, pour récupérer un événement lettre morte dans le DLQ. Vous pouvez définir le nombre de messages à récupérer à l'aide de l'`--max-number-of-messages`attribut.

```
$ aws sqs receive-message --queue-url your-dlq-url --attribute-names All --message-
attribute-names All --max-number-of-messages 1
```

Si l'opération aboutit, vous verrez des résultats similaires à ce qui suit.

```
{
    "Messages": [
        {
            "MessageId": "2aeg3510-fe3a-4f5a-ab6a-6906560eaf7e",
```

```
            "ReceiptHandle": "AQEBkNKTdOMrWgHKPoITRBwrPoK3eCSZIcZwVqCY0BZ
+FfTcORFpopJbtCqj36VbBTlHreM8+qM/m5jcwqSlAlGmIJO/hYmMgn/
+dwIty9izE7HnpvRhhEyHxbeTZ5V05RbeasYaBdNyi9WLcnAHviDh6MebLXXNWoFyYNsxdwJuG0f/
w3htX6r3dxpXvvFNPGoQb8ihY37+u0gtsbuIwhLtUSmE8rbldEEwiUfi3IJ1zEZpUS77n/k1GWrMrnYg0Gx/
BuaLzOrFi2F738XI/
Hnh45uv3ca6OYwS1ojPQ1LtX2URg1haV5884FYlaRvY8jRlpCZabTkYRTZKSXG5KNgYZnHpmsspii6JNkjitYVFKPo0H91w
            "MD5OfBody": "07adc3fc889d6107d8bb8fda42fe0573",
            "Body": "{\"MessageBody\":\"Hello, world!\",\"QueueUrl\":\"https://sqs.us-
west-2.amazonaws.com/123456789012/does-not-exist\"}",
            "Attributes": {
                "SenderId": "AROA2DZE3W4CTL5ZR7EIN:ff00212d8c453aaaae644bc6846d4723",
                "ApproximateFirstReceiveTimestamp": "1652499058144",
                "ApproximateReceiveCount": "2",
                "SentTimestamp": "1652490733042"
            },
            "MD5OfMessageAttributes": "f72c1d78100860e00403d849831d4895",
            "MessageAttributes": {
                "ERROR_CODE": {
                    "StringValue": "AWS.SimpleQueueService.NonExistentQueue",
                    "DataType": "String"
                },
                "ERROR_MESSAGE": {
                    "StringValue": "The specified queue does not exist for this wsdl
 version.",
                    "DataType": "String"
                },
                "EXECUTION_ID": {
                    "StringValue": "ad06616e51cdf74a",
                    "DataType": "String"
                },
                "EXHAUSTED_RETRY_CONDITION": {
                    "StringValue": "MaximumEventAgeInSeconds",
                    "DataType": "String"
                }
                "IS_PAYLOAD_TRUNCATED": {
                    "StringValue": "false",
                    "DataType": "String"
                },
                "RETRY_ATTEMPTS": {
                    "StringValue": "0",
                    "DataType": "String"
                },
                "SCHEDULED_TIME": {
                    "StringValue": "2022-05-14T01:12:00Z",
```

```
                    "DataType": "String"
                },
                "SCHEDULE_ARN": {
                    "StringValue": "arn:aws:scheduler:us-west-2:123456789012:schedule/
DLQ-test",
                    "DataType": "String"
                },
                "TARGET_ARN": {
                    "StringValue": "arn:aws:scheduler:::aws-sdk:sqs:sendMessage",
                    "DataType": "String"
                }
            }
        }
    ]
}
```

Notez les attributs suivants dans l'événement lettre morte pour vous aider à identifier et à résoudre les causes possibles de l'échec de l'inovcation cible.

- **`ERROR_CODE`**— Contient le code d'erreur que EventBridge Scheduler reçoit de l'API de service de la cible. Dans l'exemple précédent, le code d'erreur renvoyé par Amazon SQS est`AWS.SimpleQueueService.NonExistentQueue`. Si le calendrier ne parvient pas à appeler une cible en raison d'un problème avec le EventBridge planificateur, le code d'erreur suivant s'affichera à la place :`AWS.Scheduler.InternalServerError`.
- **`ERROR_MESSAGE`**— Contient le message d'erreur que EventBridge Scheduler reçoit de l'API de service de la cible. Dans l'exemple précédent, le message d'erreur renvoyé par Amazon SQS est`The specified queue does not exist for this wsdl version`. Si le planning échoue en raison d'un problème avec EventBridge Scheduler, le message d'erreur suivant s'affichera à la place :`Unexpected error occurred while processing the request`.
- **`TARGET_ARN`**— L'ARN de la cible invoquée par votre planning, au format ARN de service suivant :`arn:aws:scheduler:::aws-sdk:`*`service`*`:`*`apiAction`*.
- **`EXHAUSTED_RETRY_CONDITION`**— Indique pourquoi l'événement a été transmis au DLQ. Cet attribut sera présent si l'erreur provenant de l'API cible est une erreur réessayable et non une erreur permanente. L'attribut peut contenir les valeurs`MaximumRetryAttempts` si EventBridge Scheduler l'a envoyé au DLQ après avoir dépassé le nombre maximum de tentatives que vous avez configuré pour le calendrier`MaximumEventAgeInSeconds`, ou si l'événement est antérieur à l'âge maximum que vous avez configuré dans le calendrier et ne parvient toujours pas à être diffusé.

Dans l'exemple précédent, nous pouvons déterminer, sur la base du code d'erreur et du message d'erreur, que la file d'attente cible que nous avons spécifiée pour le planning n'existe pas.

Supprimer un planning

Vous pouvez supprimer un planning soit en configurant la suppression automatique, soit en supprimant manuellement un planning individuel. Consultez les rubriques suivantes pour savoir comment supprimer un planning à l'aide des deux méthodes, et pourquoi vous pouvez choisir une méthode plutôt qu'une autre.

Rubriques

Suppression une fois le planning terminé

Configurez la suppression automatique une fois la planification terminée si vous souhaitez éviter d'avoir à gérer individuellement les ressources de votre planification dans le EventBridge planificateur. Dans les applications où vous créez des milliers de programmes à la fois et que vous avez besoin de flexibilité pour augmenter le nombre de vos programmes à la demande, la suppression automatique peut vous empêcher d'atteindre le quota de votre compte pour le nombre de programmes dans une région donnée.

Lorsque vous configurez la suppression automatique d'un calendrier, le EventBridge planificateur supprime le calendrier après son dernier appel cible. Pour les plannings ponctuels, cela se produit une fois que le planning a invoqué sa cible une fois. Pour les programmes récurrents que vous configurez avec des expressions rate, ou cron, votre calendrier est supprimé après son dernier appel. Le dernier appel d'un programme récurrent est celui qui se produit le plus près de celui que `EndDate`vous avez spécifié. Si vous configurez une planification avec suppression automatique mais que vous ne spécifiez pas de valeur pour`EndDate`, le EventBridge planificateur ne supprime pas automatiquement la planification.

Vous pouvez configurer la suppression automatique lorsque vous créez un planning pour la première fois, ou mettre à jour les préférences d'un planning existant. Les étapes suivantes décrivent comment configurer la suppression automatique pour un planning existant.

AWS Management Console

1. Ouvrez la console du EventBridge planificateur à l'adresse https://console.aws.amazon.com/scheduler/.
2. Dans la liste des programmes, sélectionnez le programme que vous souhaitez modifier, puis choisissez Modifier.
3. Dans la liste de navigation de gauche, choisissez Réglages.
4. Dans la section Action une fois le planning terminé, sélectionnez SUPPRIMER dans la liste déroulante, puis enregistrez vos modifications.

AWS CLI

1. Ouvrez une nouvelle fenêtre d'invite.
2. Utilisez la AWS CLI commande update-schedule pour mettre à jour un planning existant, comme indiqué ci-dessous. La commande définit la valeur `--action-after-completion` à`DELETE`. Cet exemple suppose que vous avez défini votre configuration cible localement dans un fichier JSON. Pour mettre à jour une planification, vous devez fournir la cible, ainsi que tout autre paramètre de planification que vous souhaitez configurer pour votre planification existante.

   Il s'agit d'un programme récurrent avec un taux d'une invocation par heure. Par conséquent, vous spécifiez une date de fin lors de la définition du `--action-after-completion` paramètre.

```
$ aws scheduler update-schedule --name schedule-name
 \
--action-after-completion 'DELETE' \
--schedule-expression 'rate(1 hour)' \
--end-date '2024-01-01T00:00:00'
--target file://target-configuration.json \
--flexible-time-window '{ "Mode": "OFF"}' \
```

Suppression manuelle

Lorsque vous n'avez plus besoin d'un planning, vous pouvez le supprimer à l'aide de l'`DeleteSchedule`opération.

Example AWS CLI

```
$ aws scheduler delete-schedule --name your-schedule
```

Example Kit de développement logiciel pour Python

```
import boto3
scheduler = boto3.client('scheduler')

scheduler.delete_schedule(Name="your-schedule")
```

Quelle est la prochaine étape ?

- Pour plus d'informations sur la façon dont vous pouvez configurer des cibles modélisées pour Lambda et Step Functions, et pour en savoir plus sur l'utilisation du paramètre cible universel, consultez. Gestion des cibles
- Pour plus d'informations sur les types de données et les opérations d'API du EventBridge planificateur, consultez la référence de l'API du EventBridge planificateur.

Gestion d'un groupe de planning

Un groupe de plannings est une ressource Amazon EventBridge Scheduler que vous utilisez pour organiser vos plannings.

Vous êtes Compte AWS livré avec un groupe de `default` planificateurs. Vous pouvez associer un nouveau planning au `default` groupe ou aux groupes de plannings que vous créez et gérez. Vous pouvez créer jusqu'à 500 groupes de planning dans votreCompte AWS. Avec EventBridge Scheduler, vous organisez des groupes de plannings, plutôt que des plannings individuels, en appliquant des tags.

Une balise est une étiquette composée d'une clé sensible aux majuscules et minuscules et d'une valeur que vous définissez. Vous pouvez créer des balises pour classer les plannings selon des critères tels que l'objectif, le propriétaire ou l'environnement. Par exemple, vous pouvez identifier l'environnement auquel appartiennent vos plannings avec la balise suivante :`environment:`*`production`*.

> **Important**
>
> N'ajoutez pas de données d'identification personnelle (PII) ou d'autres informations confidentielles ou sensibles dans les étiquettes. Les étiquettes accessibles à de nombreux services AWS, y compris la facturation. Les étiquettes ne sont pas destinées à être utilisées pour des données privées ou sensibles.

Un groupe de planification possède deux états possibles : ACTIF et DELETING.

Lorsque vous créez un groupe pour la première fois, c'est `ACTIVE` par défaut. Vous pouvez ajouter des horaires à un `ACTIVE` groupe. Lorsque vous supprimez un groupe, l'état change `DELETING` jusqu'à ce que le EventBridge planificateur termine la suppression des plannings associés. Une fois que le EventBridge planificateur a supprimé les horaires du groupe, celui-ci n'est plus disponible dans votre compte.

Utilisez les rubriques suivantes pour créer un groupe de planification et lui appliquer une balise. Vous allez également associer un planning au groupe. Enfin, vous allez supprimer le groupe.

Rubriques

Création d'un groupe de planification

Utilisez les groupes de planification et le balisage pour organiser les plannings ayant un objectif commun ou appartenant au même environnement. Dans les étapes suivantes, vous allez créer un nouveau groupe de planification et l'étiqueter à l'aide d'une balise. Vous associez ensuite un nouveau planning à ce groupe.

> **Note**
>
> Une fois que vous avez créé un groupe, vous ne pouvez pas supprimer un programme de ce groupe, ni l'associer à un autre groupe. Vous ne pouvez associer un planning à un groupe que lorsque vous le créez pour la première fois.

Première étape : créer un nouveau groupe de planification

Les rubriques suivantes décrivent comment créer un nouveau groupe de planification et l'étiqueter avec la balise suivante :`environment:development`.

AWS Management Console

Pour créer un nouveau groupe à l'aide du AWS Management Console

1. Connectez-vous à la EventBridge console Amazon AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/events/.
2. Dans le volet de navigation de gauche, choisissez Schedule groups.
3. Sur la page Groupes de planification, choisissez Créer un groupe de planification.
4. Dans la section Détails du groupe de planification, dans Nom, entrez le nom du groupe. Par exemple, **`TestGroup`**.
5. Dans la section Tags, procédez comme suit :

   a. Sélectionnez Add new tag (Ajouter une nouvelle balise).

b. Pour Clé, entrez le nom que vous souhaitez attribuer à cette clé. Pour ce didacticiel, pour étiqueter l'environnement auquel appartient ce groupe de planification, entrez**`environment`**.

c. Pour Valeur - facultatif, entrez la valeur que vous souhaitez attribuer à cette clé. Pour ce didacticiel, entrez la valeur **`development`** de votre clé d'environnement.

> **Note**
>
> Vous pouvez ajouter des balises supplémentaires à votre groupe après l'avoir créé.

6. Pour terminer, choisissez Créer un groupe de planification. Votre nouveau groupe apparaît dans la liste des groupes de planification.
7. (Facultatif) Pour modifier un groupe ou gérer ses balises, cochez la case correspondant au nouveau groupe et choisissez Modifier.

> **Note**
>
> Vous ne pouvez pas modifier le groupe `default` de planification.

AWS CLI

Pour créer un nouveau groupe à l'aide du AWS CLI

1. Ouvrez une nouvelle fenêtre d'invite de commandes.
2. À partir du AWS Command Line Interface (AWS CLI), entrez la `create-schedule-group`commande suivante pour créer un nouveau groupe. Cette commande crée un groupe avec une seule balise :`environment:development`. Vous pouvez utiliser cette balise ou un système de balisage similaire pour étiqueter vos groupes de planification en fonction de l'environnement auquel ils appartiennent.

   Remplacez le nom du programme, la clé et la valeur du tag par vos informations.

```
$ aws scheduler create-schedule-group --name TestGroup --tags
 Key=environment,Value=development
```

Par défaut, votre nouveau groupe est dans l'`ACTIVE`état. Vous pouvez désormais associer de nouveaux horaires au nouveau groupe que vous avez créé.

Deuxième étape : associer un planning au groupe

Suivez les étapes ci-dessous pour associer un nouveau planning au groupe que vous avez créé à l'étape précédente.

AWS Management Console

Pour associer un planning à un groupe à l'aide du AWS Management Console

1. Connectez-vous à la EventBridge console Amazon AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/events/.
2. Dans le volet de navigation de gauche, choisissez Schedules dans le volet de navigation de gauche.
3. Dans le tableau Programmes, choisissez Créer un calendrier pour créer un nouveau calendrier.
4. Sur la page Spécifier les détails du calendrier, pour le groupe de planification, sélectionnez le nom de votre nouveau groupe dans la liste déroulante. Par exemple, sélectionnez`TestGroup`.
5. Spécifiez un modèle de planification, un objectif, des paramètres, puis passez en revue votre sélection sur la page Réviser et enregistrer le calendrier. Pour plus d'informations sur la configuration d'un nouveau calendrier, consultezDémarrer.
6. Pour terminer et enregistrer votre planning, choisissez Enregistrer le planning.

AWS CLI

Pour associer un planning à un groupe à l'aide du AWS CLI

1. Ouvrez une nouvelle fenêtre d'invite de commandes.
2. À partir du AWS Command Line Interface (AWS CLI), entrez la `create-schedule`commande suivante. Cela crée un calendrier et l'associe au groupe de l'étape précédente, nommé`sqs-test-schedule`. Ce calendrier utilise le type de cible Amazon SQS modélisé pour appeler `SendMessage` l'opération. Remplacez le nom du programme, la cible et le nom du groupe par vos informations.

```
$ aws scheduler create-schedule --name sqs-test-schedule --schedule-expression
 'rate(5 minutes)' \
--target '{"RoleArn": "ROLE_ARN", "Arn": "QUEUE_ARN", "Input": "TEST_PAYLOAD" }'
 \
--group-name TestGroup
--flexible-time-window '{ "Mode": "OFF"}'
```

Votre nouveau planning est désormais associé au groupe d'`TestGroup`horaires.

Supprimer un groupe de planification

Dans ce qui suit, vous découvrirez comment supprimer un groupe de planification à l'aide du AWS Management Console et duAWS Command Line Interface. Lorsque vous supprimez un groupe, celui-ci est conservé jusqu'à ce `DELETING` que le EventBridge planificateur supprime tous les plannings du groupe. Une fois que le EventBridge planificateur a supprimé les horaires du groupe, celui-ci n'est plus disponible dans votre compte.

> **Note**
>
> Une fois que vous avez créé un groupe, vous ne pouvez pas supprimer un programme de ce groupe, ni l'associer à un autre groupe. Vous ne pouvez associer un planning à un groupe que lorsque vous le créez pour la première fois.

AWS Management Console

Pour supprimer un groupe à l'aide du AWS Management Console

1. Connectez-vous à la EventBridge console Amazon AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/events/.
2. Dans le volet de navigation de gauche, choisissez Schedule groups dans le volet de navigation de gauche.
3. Sur la page Planifier des groupes, dans la liste des groupes existants dans le groupe actuelRégion AWS, recherchez le groupe que vous souhaitez supprimer. Si le groupe que vous recherchez ne s'affiche pas, choisissez-en un autreRégion AWS.

> **Note**
>
> Vous ne pouvez ni supprimer ni modifier le groupe par défaut.

4. Cochez la case correspondant au groupe que vous souhaitez supprimer.
5. Choisissez Delete (Supprimer).
6. Dans la boîte de dialogue Supprimer le groupe de planification, entrez le nom du groupe pour confirmer votre choix, puis choisissez Supprimer.
7. Dans la liste des groupes de planification, la colonne État change pour indiquer que votre groupe est en train de supprimer. Le groupe reste dans cet état jusqu'à ce que le EventBridge planificateur supprime tous les plannings associés au groupe.
8. Pour actualiser la liste et confirmer que le groupe a été supprimé, cliquez sur l'icône Actualiser.

AWS CLI

Pour supprimer un groupe à l'aide du AWS CLI

1. Ouvrez une nouvelle fenêtre d'invite de commandes.
2. À partir du AWS Command Line Interface (AWS CLI), entrez la `delete-schedule-group`commande suivante pour supprimer le groupe de planification. Remplacez la valeur pour `--name` par vos informations.

```
$ aws scheduler delete-schedule-group --name TestGroup
```

   En cas de succès, cette AWS CLI opération ne renvoie aucune réponse.
3. Pour vérifier que le groupe est dans `DELETING` cet état, exécutez la `get-schedule-group`commande suivante.

```
$ aws scheduler get-schedule-group --name TestGroup
```

   En cas de réussite, vous recevez un résultat similaire à ce qui suit :

```
{
    "Arn": "arn:aws::scheduler:us-west-2:123456789012:schedule-group/TestGroup",
    "CreationDate": "2023-01-01T09:00:00.000000-07:00",
```

```
    "LastModificationDate": "2023-01-01T09:00:00.000000-07:00",
    "Name": "TestGroup",
    "State": "DELETING"
}
```

EventBridge Le planificateur supprime le groupe après avoir supprimé les plannings associés au groupe. Si vous vous `get-schedule-group` présentez à nouveau, vous recevrez la `ResourceNotFoundException` réponse suivante :

```
An error occurred (ResourceNotFoundException) when calling the GetScheduleGroup
 operation: Schedule group TestGroup does not exist.
```

Ressources connexes

Pour plus d'informations sur les groupes de planification, consultez les ressources suivantes :

- CreateScheduleGroupopération dans le EventBridge Scheduler API Reference.
- DeleteScheduleGroupopération dans le EventBridge Scheduler API Reference.

Gestion des cibles

Les rubriques suivantes décrivent comment utiliser des cibles modélisées et universelles avec EventBridge Scheduler et fournissent une liste desAWS services pris en charge que vous pouvez configurer à l'aide du paramètre cible universel de EventBridge Scheduler.

Les cibles modélisées sont un ensemble d'opérations d'API courantes sur un groupe deAWS services principaux tels qu'Amazon SQS, Lambda et Step Functions. Par exemple, vous pouvez cibler l'opération d'API Invoke de Lambda en fournissant l'ARN de la fonction, ou l'`SendMessage`opération Amazon SQS avec l'ARN de file d'attente de la cible.

La cible universelle est un ensemble de paramètres personnalisables qui vous permet d'invoquer un ensemble plus large d'opérations d'API pour de nombreuxAWS services. Par exemple, vous pouvez utiliser le paramètre cible universel (UTP) du EventBridge planificateur pour créer une nouvelle file d'attente Amazon SQS à l'aide de cette `CreateQueue`opération.

Pour configurer des cibles modélisées ou universelles, votre calendrier doit être autorisé à appeler l'opération d'API que vous configurez comme cible. Pour ce faire, vous devez associer les autorisations requises au rôle d'exécution de votre calendrier. Par exemple, pour cibler l'`SendMessage`opération Amazon SQS, le rôle d'exécution doit être autorisé à effectuer l'`sqs:SendMessage`action. Dans la plupart des cas, vous pouvez ajouter les autorisations nécessaires à l'aide des politiquesAWS gérées prises en charge par le service cible. Toutefois, vous pouvez également créer vos propres politiques gérées par le client ou ajouter des autorisations en ligne à une politique existante associée au rôle d'exécution. Les rubriques suivantes présentent des exemples d'ajout d'autorisations pour les types de cibles modélisés et universels.

Pour de plus amples informations sur la configuration d'un rôle d'exécution pour un calendrier, consultezthe section called “Configurer le rôle d'exécution”.

Rubriques

Utilisation de cibles modélisées

Les cibles modélisées sont un ensemble d'opérations d'API communes à un groupe de AWS services principaux, tels qu'Amazon SQS, Lambda et Step Functions. Par exemple, vous pouvez cibler le `Invoke`fonctionnement de Lambda en fournissant la fonction ARN, ou le `SendMessage`fonctionnement d'Amazon SQS en utilisant l'ARN de la file d'attente. Pour configurer une cible modélisée, vous devez également accorder des autorisations au rôle d'exécution du calendrier pour effectuer l'opération d'API ciblée.

Pour configurer un modèle de cible par programmation à l'aide du AWS CLI ou de l'un des SDK du EventBridge planificateur, vous devez spécifier l'ARN du rôle d'exécution, l'ARN de la ressource cible, une entrée facultative que vous souhaitez que le EventBridge Scheduler fournisse à la cible et, pour certaines cibles modèles, un ensemble unique de paramètres avec des options de configuration supplémentaires pour cette cible. Lorsque vous spécifiez l'ARN d'une ressource cible modélisée, EventBridge Scheduler suppose automatiquement que vous souhaitez appeler l'opération d'API prise en charge pour ce service. Si vous souhaitez que EventBridge Scheduler cible une opération d'API différente pour le service, vous devez configurer la cible en tant que cible universelle.

Vous trouverez ci-dessous une liste complète de toutes les cibles modélisées prises en charge EventBridge par Scheduler et, le cas échéant, l'ensemble unique de paramètres associés à chaque cible. Cliquez sur le lien correspondant à chaque ensemble de paramètres pour voir les champs obligatoires et facultatifs dans la référence de l'API du EventBridge planificateur.

- CodeBuild – `StartBuild`
- CodePipeline – `StartPipelineExecution`
- Amazon ECS — `RunTask`
  - Paramètres: `EcsParameters`
- EventBridge – `PutEvents`
  - Paramètres: `EventBridgeParameters`
- Amazon Inspector — `StartAssessmentRun`
- Kinesis : `PutRecord`
  - Paramètres: `KinesisParameters`
- Firehose — **`PutRecord`**
- Lambda – `Invoke`
- SageMaker – `StartPipelineExecution`

  - Paramètres: SageMakerPipelineParameters
- Amazon SNS — **Publish**
- Amazon SQS : SendMessage
  - Paramètres: SqsParameters
- Step Functions — StartExecution

Utilisez les exemples suivants pour savoir comment configurer différentes cibles modélisées et les autorisations IAM requises pour chaque cible décrite.

Amazon SQS **SendMessage**

Example Politique d'autorisation pour le rôle d'exécution

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

Example AWS CLI

```
$ aws scheduler create-schedule --name sqs-templated --schedule-expression 'rate(5
 minutes)' \
--target '{"RoleArn": "ROLE_ARN", "Arn":"QUEUE_ARN", "Input": "Message for scheduleArn:
 '<aws.scheduler.schedule-arn>', scheduledTime: '<aws.scheduler.scheduled-time>'" }' \
--flexible-time-window '{ "Mode": "OFF"}'
```

Example Kit de développement logiciel pour Python

```
import boto3
scheduler = boto3.client('scheduler')
```

```
flex_window = { "Mode": "OFF" }

sqs_templated = {
    "RoleArn": "<ROLE_ARN>",
    "Arn": "<QUEUE_ARN>",
    "Input": "Message for scheduleArn: '<aws.scheduler.schedule-arn>', scheduledTime:
 '<aws.scheduler.scheduled-time>'"
}

scheduler.create_schedule(
    Name="sqs-python-templated",
    ScheduleExpression="rate(5 minutes)",
    Target=sqs_templated,
    FlexibleTimeWindow=flex_window)
```

Example Kit SDK Java

```
package com.example;

import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.scheduler.SchedulerClient;
import software.amazon.awssdk.services.scheduler.model.*;


public class MySchedulerApp {

    public static void main(String[] args) {

        final SchedulerClient client = SchedulerClient.builder()
                .region(Region.US_WEST_2)
                .build();

        Target sqsTarget = Target.builder()
                .roleArn("<ROLE_ARN>")
                .arn("<QUEUE_ARN>")
                .input("Message for scheduleArn: '<aws.scheduler.schedule-arn>',
 scheduledTime: '<aws.scheduler.scheduled-time>'")
                .build();

        CreateScheduleRequest createScheduleRequest = CreateScheduleRequest.builder()
                .name("<SCHEDULE NAME>")
                .scheduleExpression("rate(10 minutes)")
                .target(sqsTarget)
```

```
                .flexibleTimeWindow(FlexibleTimeWindow.builder()
                        .mode(FlexibleTimeWindowMode.OFF)
                        .build())
                .build();

        client.createSchedule(createScheduleRequest);
        System.out.println("Created schedule with rate expression and an Amazon SQS
 templated target");
    }
}
```

Lambda **Invoke**

Example Politique d'autorisation pour le rôle d'exécution

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

Example AWS CLI

```
$ aws scheduler create-schedule --name lambda-templated-schedule --schedule-expression
 'rate(5 minutes)' \
--target '{"RoleArn": "ROLE_ARN", "Arn":"FUNCTION_ARN", "Input": "{ \"Payload\":
 \"TEST_PAYLOAD\" }" }' \
--flexible-time-window '{ "Mode": "OFF"}'
```

Example Kit de développement logiciel pour Python

```
import boto3
scheduler = boto3.client('scheduler')

flex_window = { "Mode": "OFF" }
```

```
lambda_templated = {
    "RoleArn": "<ROLE_ARN>",
    "Arn": "<LAMBDA_ARN>",
    "Input": "{ 'Payload': 'TEST_PAYLOAD' }"}
}

scheduler.create_schedule(
    Name="lambda-python-templated",
    ScheduleExpression="rate(5 minutes)",
    Target=lambda_templated,
    FlexibleTimeWindow=flex_window)
```

Example Kit SDK Java

```
package com.example;

import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.scheduler.SchedulerClient;
import software.amazon.awssdk.services.scheduler.model.*;


public class MySchedulerApp {

    public static void main(String[] args) {

        final SchedulerClient client = SchedulerClient.builder()
                .region(Region.US_WEST_2)
                .build();

        Target lambdaTarget = Target.builder()
                .roleArn("<ROLE_ARN>")
                .arn("<Lambda ARN>")
                .input("{ 'Payload': 'TEST_PAYLOAD' }")
                .build();

        CreateScheduleRequest createScheduleRequest = CreateScheduleRequest.builder()
                .name("<SCHEDULE_NAME>")
                .scheduleExpression("rate(10 minutes)")
                .target(lambdaTarget)
                .flexibleTimeWindow(FlexibleTimeWindow.builder()
                        .mode(FlexibleTimeWindowMode.OFF)
                        .build())
```

```
                .clientToken("<Token GUID>")
                .build();

        client.createSchedule(createScheduleRequest);
        System.out.println("Created schedule with rate expression and Lambda templated
 target");
    }
}
```

Step Functions **`StartExecution`**

Example Politique d'autorisation pour le rôle d'exécution

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

Example AWS CLI

```
$ aws scheduler create-schedule --name sfn-templated-schedule --schedule-expression
 'rate(5 minutes)' \
--target '{"RoleArn": "ROLE_ARN", "Arn":"STATE_MACHINE_ARN", "Input": "{ \"Payload\":
 \"TEST_PAYLOAD\" }" }' \
--flexible-time-window '{ "Mode": "OFF"}'
```

Example Kit de développement logiciel pour Python

```
import boto3
scheduler = boto3.client('scheduler')

flex_window = { "Mode": "OFF" }

sfn_templated= {
```

```
    "RoleArn": "<ROLE_ARN>",
    "Arn": "<STATE_MACHINE_ARN>",
    "Input": "{ 'Payload': 'TEST_PAYLOAD' }"
}

scheduler.create_schedule(Name="sfn-python-templated",
    ScheduleExpression="rate(5 minutes)",
    Target=sfn_templated,
    FlexibleTimeWindow=flex_window)
```

Example Kit SDK Java

```
package com.example;

import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.scheduler.SchedulerClient;
import software.amazon.awssdk.services.scheduler.model.*;


public class MySchedulerApp {

    public static void main(String[] args) {

        final SchedulerClient client = SchedulerClient.builder()
                .region(Region.US_WEST_2)
                .build();

        Target stepFunctionsTarget = Target.builder()
                .roleArn("<ROLE_ARN>")
                .arn("<STATE_MACHINE_ARN>")
                .input("{ 'Payload': 'TEST_PAYLOAD' }")
                .build();

        CreateScheduleRequest createScheduleRequest = CreateScheduleRequest.builder()
                .name("<SCHEDULE_NAME>")
                .scheduleExpression("rate(10 minutes)")
                .target(stepFunctionsTarget)
                .flexibleTimeWindow(FlexibleTimeWindow.builder()
                        .mode(FlexibleTimeWindowMode.OFF)
                        .build())
                .clientToken("<Token GUID>")
                .build();
```

```
        client.createSchedule(createScheduleRequest);
        System.out.println("Created schedule with rate expression and Step Function
 templated target");
    }
}
```

Utiliser des cibles universelles

Une cible universelle est un ensemble personnalisable de paramètres qui vous permet d'invoquer un ensemble plus large d'opérations d'API pour de nombreux AWS services. Par exemple, vous pouvez utiliser un paramètre cible universel (UTP) pour créer une nouvelle file d'attente Amazon SQS à l'`CreateQueue`aide de cette opération.

Pour configurer une cible universelle pour votre planning à l'aide du AWS CLI ou de l'un des SDK du EventBridge planificateur, vous devez spécifier les informations suivantes :

- RoleArn— L'ARN du rôle d'exécution que vous souhaitez utiliser pour la cible. Le rôle d'exécution que vous spécifiez doit être autorisé à appeler l'opération d'API que vous souhaitez cibler dans votre planning.
- Arn — L'ARN complet du service, y compris l'opération d'API que vous souhaitez cibler, au format suivant :`arn:aws:scheduler:::aws-sdk:`*`service`*`:`*`apiAction`*.

  Par exemple, pour Amazon SQS, le nom du service que vous spécifiez est. `arn:aws:scheduler:::aws-sdk:`**`sqs:sendMessage`**
- Entrée — Un JSON bien formé que vous spécifiez avec les paramètres de demande que EventBridge Scheduler envoie à l'API cible. Les paramètres et la forme du JSON que vous définissez `Input` sont déterminés par l'API de service invoquée par votre planning. Pour trouver ces informations, consultez la référence d'API du service que vous souhaitez cibler.

Actions non prises en charge

EventBridge Le planificateur ne prend pas en charge les actions d'API en lecture seule, telles que les `GET` opérations courantes, qui commencent par la liste de préfixes suivante :

```
get
describe
list
poll
```

```
receive
search
scan
query
select
read
lookup
discover
validate
batchGet
batchDescribe
batchRead
transactGet
adminGet
adminList
testMigration
retrieve
testConnection
translateDocument
isAuthorized
isAuthorizedWithToken
invokeModel
```

Par exemple, l'ARN du service pour l'action d'`GetQueueUrl`API serait le suivant : `arn:aws:scheduler:::aws-sdk:sqs:`**`getQueueURL`** Comme l'action de l'API commence par le `get` préfixe, EventBridge Scheduler ne prend pas en charge cette cible. De même, l'`ListBrokers`action Amazon MQ n'est pas prise en charge en tant que cible car elle commence par le préfixe. `list`

Exemples d'utilisation de la cible universelle

Les paramètres que vous transmettez dans le `Input` champ de planification dépendent des paramètres de demande acceptés par l'API de service que vous souhaitez invoquer. Par exemple, pour cibler Lambda `Invoke`, vous pouvez définir les paramètres répertoriés dans la référence d'AWS LambdaAPI. Cela inclut la charge utile JSON facultative que vous pouvez transmettre à une fonction Lambda.

Pour déterminer les paramètres que vous pouvez définir pour les différentes API, consultez la référence des API pour ce service. À l'instar de Lambda`Invoke`, certaines API acceptent les paramètres d'URI, ainsi que la charge utile du corps de la requête. Dans ce cas, vous spécifiez les paramètres du chemin de l'URI ainsi que la charge utile JSON dans votre planning`Input`.

Les exemples suivants montrent comment utiliser la cible universelle pour appeler des opérations d'API courantes avec Lambda, Amazon SQS et Step Functions.

Example Lambda

```
$ aws scheduler create-schedule --name lambda-universal-schedule --schedule-expression
 'rate(5 minutes)' \
--target '{"RoleArn": "ROLE_ARN", "Arn":"arn:aws:scheduler:::aws-sdk:lambda:invoke"
 "Input": "{\"FunctionName\":\"arn:aws:lambda:REGION:123456789012:function:HelloWorld
\",\"InvocationType\":\"Event\",\"Payload\":\"{\\\"message\\\":\\\"testing function\\
\"}\"}" }' \
--flexible-time-window '{ "Mode": "OFF"}'
```

Example Amazon SQS

```
import boto3
scheduler = boto3.client('scheduler')

flex_window = { "Mode": "OFF" }

sqs_universal= {
    "RoleArn": "<ROLE_ARN>",
    "Arn": "arn:aws:scheduler:::aws-sdk:sqs:sendMessage",
    "Input": "{\"MessageBody\":\"My message\",\"QueueUrl\":\"<QUEUE_URL>\"}"}
}

scheduler.create_schedule(
    Name="sqs-sdk-test",
    ScheduleExpression="rate(5 minutes)",
    Target=sqs_universal,
    FlexibleTimeWindow=flex_window)
```

Example Step Functions

```
package com.example;

import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.scheduler.SchedulerClient;
import software.amazon.awssdk.services.scheduler.model.*;


public class MySchedulerApp {
```

```
    public static void main(String[] args) {

        final SchedulerClient client = SchedulerClient.builder()
                .region(Region.US_WEST_2)
                .build();

        Target stepFunctionsUniversalTarget = Target.builder()
                .roleArn("<ROLE_ARN>")
                .arn("arn:aws:scheduler:::aws-sdk:sfn:startExecution")
                .input("{\"Input\":\"{}\",\"StateMachineArn\":\"<STATE_MACHINE_ARN>
\"}")
                .build();

        CreateScheduleRequest createScheduleRequest = CreateScheduleRequest.builder()
                .name("<SCHEDULE_NAME>")
                .scheduleExpression("rate(10 minutes)")
                .target(stepFunctionsUniversalTarget)
                .flexibleTimeWindow(FlexibleTimeWindow.builder()
                        .mode(FlexibleTimeWindowMode.OFF)
                        .build())
                .clientToken("<Token GUID>")
                .build();

        client.createSchedule(createScheduleRequest);
        System.out.println("Created schedule with rate expression and Step Function
 universal target");
    }
}
```

Ajouter des attributs de contexte

Utilisation des mots clés suivants dans la charge utile que vous transmettez à la cible pour collecter des métadonnées relatives au planning. EventBridge Le planificateur remplace chaque mot clé par sa valeur respective lorsque votre calendrier invoque la cible.

- **<aws.scheduler.schedule-arn>**— L'ARN du planning.
- **<aws.scheduler.scheduled-time>**— L'heure que vous avez spécifiée pour que le planning invoque sa cible, par exemple,`2022-03-22T18:59:43Z`.
- **<aws.scheduler.execution-id>**— L'identifiant unique que EventBridge Scheduler attribue à chaque tentative d'invocation d'une cible, par exemple,. `d32c5kddcf5bb8c3`

- **<aws.scheduler.attempt-number>**— Un compteur qui identifie le numéro de tentative pour l'invocation en cours, par exemple,1.

Cet exemple montre comment créer un calendrier qui se déclenche toutes les cinq minutes et invoque l'opération Amazon `SendMessage` SQS en tant que cible universelle. Le corps du message inclut la valeur pour`schedule-time`.

Example AWS CLI

```
$ aws scheduler create-schedule --name your-schedule \
    --schedule-expression 'rate(5 minutes)' \
    --target '{"RoleArn": "ROLE_ARN", \
        "Arn": "arn:aws:scheduler:::aws-sdk:sqs:sendMessage", \
        "Input": "{\"MessageBody\":\"<aws.scheduler.scheduled-time>\",\"QueueUrl\":
\"https://sqs.us-west-2.amazonaws.com/123456789012/scheduler-cli-test\"}"}' \
    --flexible-time-window '{ "Mode": "OFF"}'
```

Example Kit de développement logiciel pour Python

```
import boto3
scheduler = boto3.client('scheduler')

sqs_universal= {
    "RoleArn": "<ROLE_ARN>",
    "Arn": "arn:aws:scheduler:::aws-sdk:sqs:sendMessage",
    "Input": "{\"MessageBody\":\"<aws.scheduler.scheduled-time>\",\"QueueUrl\":
\"https://sqs.us-west-2.amazonaws.com/123456789012/scheduler-cli-test\"}"
}

flex_window = { "Mode": "OFF" }


scheduler.update_schedule(Name="your-schedule",
    ScheduleExpression="rate(5 minutes)",
    Target=sqs_universal,
    FlexibleTimeWindow=flex_window)
```

Quelle est la prochaine étape ?

Pour plus d'informations sur les types de données et les opérations d'API du EventBridge planificateur, consultez la section Référence de l'API duEventBridge planificateur.

Sécurité dans Amazon EventBridge Scheduler

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures 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 cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon EventBridge Scheduler, consultez la section AWS Services concernés par programme de conformité AWS .
- 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 l'utilisation du EventBridge planificateur. Les rubriques suivantes expliquent comment configurer le EventBridge planificateur pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser les ressources de votre EventBridge planificateur.

Rubriques

Gestion de l'accès à Amazon EventBridge Scheduler

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 les ressources du EventBridge planificateur. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans EventBridge Scheduler.

Utilisateur du service : si vous utilisez le service EventBridge Scheduler 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 plus en plus de fonctionnalités du EventBridge planificateur 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 parvenez pas à accéder à une fonctionnalité dans le EventBridge planificateur, consultez. Résolution des problèmes d'identité et d'accès à Amazon EventBridge Scheduler

Administrateur du service — Si vous êtes responsable des ressources du EventBridge planificateur dans votre entreprise, vous avez probablement un accès complet au planificateur. EventBridge C'est à vous de déterminer les fonctionnalités et les ressources du EventBridge planificateur 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 EventBridge Scheduler, consultez. Comment fonctionne EventBridge Scheduler avec IAM

Administrateur IAM — Si vous êtes administrateur IAM, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès au EventBridge planificateur. Pour consulter des exemples de politiques basées sur l'identité du EventBridge planificateur que vous pouvez utiliser dans IAM, consultez. Utilisation 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, veuillez consulter 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 root pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur root et utilisez-les pour effectuer les tâches que seul l'utilisateur root peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

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 une seule 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 la section Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification du 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 la section 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 la section 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, veuillez consulter 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, une fonction 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, l'action que vous effectuez est susceptible de lancer 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.
  - Fonction du 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 la section 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 la section Quand créer un rôle IAM (au lieu d'un utilisateur) 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 Présentation 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 relatives à 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 la section 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 la section 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 Amazon S3. 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) vérifient quels principaux (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 Présentation 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 qui en résultent 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 la séance obtenue 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 remplace l'autorisation. Pour plus d'informations, consultez Politiques de session dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations obtenues 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.

Comment fonctionne EventBridge Scheduler avec IAM

Avant d'utiliser IAM pour gérer l'accès au EventBridge planificateur, découvrez quelles fonctionnalités IAM peuvent être utilisées avec le planificateur. EventBridge

Fonctionnalités IAM que vous pouvez utiliser avec Amazon Scheduler EventBridge

Fonctionnalité IAM	EventBridge Support du planificateur
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Oui
ACL	Non
ABAC (identifications dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Fonctions du service	Oui
Rôles liés à un service	Non

Pour obtenir une vue d'ensemble du fonctionnement du EventBridge planificateur et des autres AWS services avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le guide de l'utilisateur IAM.

Politiques basées sur l'identité pour Scheduler EventBridge

Prend en charge les politiques basées sur l'identité	Oui

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 la section Création de politiques IAM dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur l'identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour découvrir 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.

Exemples de politiques basées sur l'identité pour Scheduler EventBridge

Pour consulter des exemples de politiques basées sur l'identité du EventBridge planificateur, consultez. Utilisation de politiques basées sur l'identité

Politiques basées sur les ressources dans Scheduler EventBridge

Prend en charge les politiques basées sur les ressources	Non

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 Amazon S3. 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

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur l'identité à l'entité. Toutefois, si une politique basée sur les ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

Actions politiques pour EventBridge Scheduler

Prend en charge les actions de politique	Oui

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.

Pour consulter la liste des actions du EventBridge planificateur, consultez la section Actions définies par Amazon EventBridge Scheduler dans le Service Authorization Reference.

Les actions de stratégie dans le EventBridge planificateur utilisent le préfixe suivant avant l'action :

```
scheduler
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "scheduler:action1",
      "scheduler:action2"
]
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `List`, incluez l'action suivante :

```
"Action": [
   "scheduler:List*"
]
```

Ressources relatives aux politiques pour EventBridge Scheduler

Prend en charge les ressources de politique	Oui

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 pour lesquels 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": "*"
```

Pour consulter la liste des types de ressources du EventBridge planificateur et de leurs ARN, consultez la section Ressources définies par Amazon EventBridge Scheduler dans le manuel Service Authorization Reference. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par Amazon EventBridge Scheduler.

Pour consulter des exemples de politiques basées sur l'identité du EventBridge planificateur, consultez. Utilisation de politiques basées sur l'identité

Clés de conditions de politique pour EventBridge Scheduler

Prend en charge les clés de condition de politique spécifiques au service	Oui

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.

Pour consulter la liste des clés de condition du EventBridge planificateur, consultez la section Clés de condition pour Amazon EventBridge Scheduler dans la référence d'autorisation du service. Pour

savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez la section Actions définies par Amazon EventBridge Scheduler.

Pour consulter des exemples de politiques basées sur l'identité du EventBridge planificateur, consultez. Utilisation de politiques basées sur l'identité

ACL dans EventBridge le planificateur

Prend en charge les listes ACL	Non

Les listes de contrôle d'accès (ACL) vérifient quels principaux (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.

ABAC avec planificateur EventBridge

Prise en charge d'ABAC (identifications dans les politiques)	Partielle

Le contrôle d'accès basé sur les attributs (ABAC) est une politique d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

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`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (ABAC) ? dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès basé sur les attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec le EventBridge planificateur

Prend en charge les informations d'identification temporaires	Oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Autorisations principales interservices pour Scheduler EventBridge

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, l'action que vous effectuez est

susceptible de lancer 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 de service pour EventBridge Scheduler

Prend en charge les fonctions du service	Oui

Une fonction du 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.

> **Warning**
>
> La modification des autorisations associées à un rôle de service peut perturber les fonctionnalités du EventBridge planificateur. Modifiez les rôles de service uniquement lorsque le EventBridge planificateur fournit des instructions à cet effet.

Rôles liés à un service pour Scheduler EventBridge

Prend en charge les rôles liés à un service	Non

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.

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM. Recherchez un service dans le tableau qui inclut un `Yes` dans la

colonne Rôle lié à un service. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Utilisation de politiques basées sur l'identité

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier les ressources du EventBridge planificateur. 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 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.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par le EventBridge Scheduler, y compris le format des ARN pour chacun des types de ressources, consultez la section Actions, ressources et clés de condition pour Amazon EventBridge Scheduler dans le Service Authorization Reference.

Rubriques

- Bonnes pratiques en matière de politiques
- EventBridge Autorisations du planificateur
- AWS politiques gérées pour EventBridge Scheduler
- Politiques gérées par le client pour EventBridge Scheduler
- AWS mises à jour des politiques gérées

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer les ressources du EventBridge Scheduler 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 fonctions professionnelles dans le Guide de l'utilisateur IAM.

- Accorder des autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, n'accordez que les autorisations nécessaires à l'exécution de la 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 de plus amples 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 de plus amples 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.

EventBridge Autorisations du planificateur

Pour qu'un principal IAM (utilisateur, groupe ou rôle) puisse créer des horaires dans le EventBridge planificateur et accéder aux ressources du EventBridge planificateur via la console ou l'API, le

principal doit avoir un ensemble d'autorisations ajouté à sa politique d'autorisation. Vous pouvez configurer ces autorisations en fonction de la fonction du poste du principal. Par exemple, un utilisateur ou un rôle qui utilise uniquement la console du EventBridge planificateur pour consulter la liste des plannings existants n'a pas besoin des autorisations requises pour appeler l'opération d'`CreateSchedule`API. Nous vous recommandons de personnaliser vos autorisations basées sur l'identité afin de ne fournir que les accès les moins privilégiés.

La liste suivante présente les ressources du EventBridge planificateur et les actions prises en charge correspondantes.

- Schedule
  - `scheduler:ListSchedules`
  - `scheduler:GetSchedule`
  - `scheduler:CreateSchedule`
  - `scheduler:UpdateSchedule`
  - `scheduler:DeleteSchedule`
- Planifier un groupe
  - `scheduler:ListScheduleGroups`
  - `scheduler:GetScheduleGroup`
  - `scheduler:CreateScheduleGroup`
  - `scheduler:DeleteScheduleGroup`
  - `scheduler:ListTagsForResource`
  - `scheduler:TagResource`
  - `scheduler:UntagResource`

Vous pouvez utiliser les autorisations du EventBridge planificateur pour créer vos propres politiques gérées par les clients à utiliser avec EventBridge le planificateur. Vous pouvez également utiliser les politiques AWS gérées décrites dans la section suivante pour accorder les autorisations nécessaires pour les cas d'utilisation courants sans avoir à gérer vos propres politiques.

AWS politiques gérées pour EventBridge Scheduler

AWS répond à de nombreux cas d'utilisation courants en fournissant des politiques IAM autonomes qui AWS créent et administrent. Les politiques gérées, ou prédéfinies, accordent les autorisations nécessaires pour les cas d’utilisation courants, ce qui vous évite d’avoir à déterminer quelles

autorisations sont nécessaires. Pour plus d'informations, consultez Politiques gérées par AWS dans le Guide de l'utilisateur IAM. Les politiques AWS gérées suivantes que vous pouvez associer aux utilisateurs de votre compte sont spécifiques à EventBridge Scheduler :

- the section called "AmazonEventBridgeSchedulerFullAccess"— Accorde un accès complet au EventBridge planificateur à l'aide de la console et de l'API.
- the section called "AmazonEventBridgeSchedulerReadOnlyAccess"— Accorde un accès en lecture seule au planificateur. EventBridge

AmazonEventBridgeSchedulerFullAccess

La politique AmazonEventBridgeSchedulerFullAccess gérée accorde des autorisations pour utiliser toutes les actions du EventBridge planificateur pour les plannings et les groupes de plannings.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "scheduler:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "scheduler.amazonaws.com"
                }
            }
        }
    ]
}
```

AmazonEventBridgeSchedulerReadOnlyAccess

La politique AmazonEventBridgeSchedulerReadOnlyAccess gérée accorde des autorisations en lecture seule pour consulter les détails de vos plannings et de vos groupes de plannings.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "scheduler:ListSchedules",
                "scheduler:ListScheduleGroups",
                "scheduler:GetSchedule",
                "scheduler:GetScheduleGroup",
                "scheduler:ListTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

Politiques gérées par le client pour EventBridge Scheduler

Utilisez les exemples suivants pour créer vos propres politiques gérées par les clients pour EventBridge Scheduler. Les politiques gérées par le client vous permettent d'accorder des autorisations uniquement pour les actions et les ressources requises pour les applications et les utilisateurs de votre équipe conformément à la fonction du directeur.

Rubriques

- Exemple : CreateSchedule
- Exemple : GetSchedule
- Exemple : UpdateSchedule
- Exemple : DeleteScheduleGroup

Exemple : **`CreateSchedule`**

Lorsque vous créez un nouveau calendrier, vous choisissez de chiffrer vos données sur EventBridge Scheduler à l'aide d'une clé gérée par le client ou d'une Clé détenue par AWSclé gérée par le client.

La politique suivante permet à un directeur de créer un calendrier et d'appliquer le chiffrement à l'aide d'un Clé détenue par AWS. Avec un Clé détenue par AWS, AWS gère les ressources sur AWS Key Management Service (AWS KMS) pour vous afin que vous n'ayez pas besoin d'autorisations supplémentaires pour interagir avec AWS KMS.

```
{
```

```
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Action":
            [
                "scheduler:CreateSchedule"
            ],
            "Effect": "Allow",
            "Resource":
            [
                "arn:aws:scheduler:us-west-2:123456789012:schedule/my-group/my-
schedule-name"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::123456789012:role/*",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "scheduler.amazonaws.com"
                }
            }
        }
    ]
}
```

Utilisez la politique suivante pour autoriser un directeur à créer un calendrier et à utiliser une clé gérée par AWS KMS le client pour le chiffrement. Pour utiliser une clé gérée par le client, un mandant doit être autorisé à accéder aux AWS KMS ressources de votre compte. Cette politique accorde l'accès à une seule clé KMS spécifiée à utiliser pour chiffrer les données sur le EventBridge planificateur. Vous pouvez également utiliser un caractère générique (*) pour autoriser l'accès à toutes les clés d'un compte, ou à un sous-ensemble correspondant à un modèle de nom donné.

```
{
    "Version": "2012-10-17"
    "Statement":
    [
        {
            "Action":
            [
```

```
                "scheduler:CreateSchedule"
            ],
            "Effect": "Allow",
            "Resource":
            [
                "arn:aws:scheduler:us-west-2:123456789012:schedule/my-group/my-
schedule-name"
            ]
        },
        {
            "Action":
            [
                "kms:DescribeKey",
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Effect": "Allow",
            "Resource":
            [
                "arn:aws:kms:us-west-2:123456789012:key/my-key-id"
            ],
            "Conditions": {
                "StringLike": {
                    "kms:ViaService": "scheduler.amazonaws.com",
                    "kms:EncryptionContext:aws:scheduler:schedule:arn":
 "arn:aws:scheduler:us-west-2:123456789012:schedule/my-group/my-schedule-name"
            }
        }
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::123456789012:role/*",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "scheduler.amazonaws.com"
                }
            }
        }
    ]
}
```

Exemple : **`GetSchedule`**

Utilisez la politique suivante pour autoriser un directeur d'école à obtenir des informations sur un calendrier.

```
{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Action":
            [
                "scheduler:GetSchedule"
            ],
            "Effect": "Allow",
            "Resource":
            [
                "arn:aws:scheduler:us-west-2:123456789012:schedule/my-group/my-
schedule-name"
            ]
        }
    ]
}
```

Exemple : **`UpdateSchedule`**

Utilisez les politiques suivantes pour autoriser un directeur à mettre à jour un calendrier en déclenchant l'`scheduler:UpdateSchedule`action. De même`CreateSchedule`, la politique dépend du fait que le calendrier utilise une clé AWS KMS Clé détenue par AWS ou une clé gérée par le client pour le chiffrement. Pour un calendrier configuré avec un Clé détenue par AWS, appliquez la politique suivante :

```
{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Action":
            [
                "scheduler:UpdateSchedule"
            ],
            "Effect": "Allow",
```

```
            "Resource":
            [
                "arn:aws:scheduler:us-west-2:123456789012:schedule/my-group/my-
schedule-name"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::123456789012:role/*",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "scheduler.amazonaws.com"
                }
            }
        }
    ]
}
```

Pour un calendrier configuré avec une clé gérée par le client, appliquez la politique suivante. Cette politique inclut des autorisations supplémentaires qui permettent à un mandant d'accéder aux AWS KMS ressources de votre compte :

```
{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Action":
            [
                "scheduler:UpdateSchedule"
            ],
            "Effect": "Allow",
            "Resource":
            [
                "arn:aws:scheduler:us-west-2:123456789012:schedule/my-group/my-
schedule-name
        },
        {
            "Action":
            [
                "kms:DescribeKey",
                "kms:GenerateDataKey",
```

```
                "kms:Decrypt"
            ],
            "Effect": "Allow",
            "Resource":
            [
                "arn:aws:kms:us-west-2:123456789012:key/my-key-id"
            ],
            "Conditions": {
                "StringLike": {
                    "kms:ViaService": "scheduler.amazonaws.com",
                    "kms:EncryptionContext:aws:scheduler:schedule:arn":
 "arn:aws:scheduler:us-west-2:123456789012:schedule/my-group/my-schedule-name"
            }
        }
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::123456789012:role/*",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "scheduler.amazonaws.com"
                }
            }
        }
    ]
}
```

Exemple : **`DeleteScheduleGroup`**

Utilisez la politique suivante pour autoriser un directeur à supprimer un groupe de planification. Lorsque vous supprimez un groupe, vous supprimez également les plannings associés à ce groupe. Le principal qui supprime le groupe doit être autorisé à supprimer également les plannings associés à ce groupe. Cette politique accorde l'autorisation principale d'appeler l'`scheduler:DeleteScheduleGroup`action sur les groupes de planification spécifiés, ainsi que sur tous les programmes du groupe :

> **Note**
>
> EventBridge Le planificateur ne prend pas en charge la spécification d'autorisations au niveau des ressources pour des plannings individuels. Par exemple, la déclaration suivante n'est pas valide et ne doit pas être incluse dans votre police d'assurance :

```
    "Resource": "arn:aws:scheduler:us-west-2:123456789012:schedule/my-group/my-schedule-name"
```

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "scheduler:DeleteSchedule",
            "Resource": "arn:aws:scheduler:us-west-2:123456789012:schedule/my-group/*"
        },
        {
            "Effect": "Allow",
            "Action": "scheduler:DeleteScheduleGroup",
            "Resource": "arn:aws:scheduler:us-west-2:123456789012:schedule/my-group"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::123456789012:role/*",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "scheduler.amazonaws.com"
                }
            }
        }
    ]
}
```

AWS mises à jour des politiques gérées

Modification	Description	Date
the section called "AmazonEventBridgeSchedulerFullAccess"— Nouvelle politique gérée	EventBridge Le planificateur ajoute la prise en charge d'une nouvelle politique gérée qui accorde aux utilisateurs un accès complet à toutes les ressources, y compris les	10 novembre 2022

Modification	Description	Date
	plannings et les groupes de plannings.	
the section called "AmazonEventBridgeSchedulerReadOnlyAccess "— Nouvelle politique gérée	EventBridge Le planificateur ajoute la prise en charge d'une nouvelle politique gérée qui accorde aux utilisateurs un accès en lecture seule à toutes les ressources, y compris les plannings et les groupes de plannings.	10 novembre 2022
EventBridge Le planificateur a commencé à suivre les modifications	EventBridge Scheduler a commencé à suivre les modifications apportées à ses politiques AWS gérées.	10 novembre 2022

Prévention de l'adjoint confus

Le problème de l'adjoint confus est un problème de sécurité dans lequel une entité qui n'a pas l'autorisation d'effectuer une action peut contraindre une entité plus privilégiée à effectuer cette action. En AWS, l'usurpation d'identité interservices peut entraîner la confusion des 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 et ses autorisations utilisées pour agir sur les ressources d'un autre client auxquelles on ne serait pas autorisé d'accéder 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 vous recommandons d'utiliser les clés de contexte de condition `aws:SourceAccount`globale `aws:SourceArn`et les clés contextuelles dans votre rôle d'exécution de planification afin de limiter les autorisations que le EventBridge planificateur accorde à un autre service pour accéder à la ressource. 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.

Le moyen le plus efficace de se protéger du problème de l'adjoint désorienté consiste à utiliser la clé de contexte de condition globale `aws:SourceArn` avec l'ARN complet de la ressource. La condition suivante s'applique à un groupe de planification individuel : `arn:aws:scheduler:*:123456789012:schedule-group/your-schedule-group`

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:scheduler:*:123456789012:schedule-group/*`.

La valeur de `aws:SourceArn` doit être l'ARN du groupe de planification du EventBridge planificateur auquel vous souhaitez étendre cette condition.

> **Important**
>
> Ne limitez pas l'`aws:SourceArn`énoncé à un calendrier spécifique ou à un préfixe de nom de programme. L'ARN que vous spécifiez doit être un groupe de planification.

L'exemple suivant montre comment vous pouvez utiliser les clés de contexte de condition `aws:SourceAccount` globale `aws:SourceArn` et les clés de contexte dans la politique de confiance de votre rôle d'exécution pour éviter le problème de confusion des adjoints :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "scheduler.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "aws:SourceArn": "arn:aws:scheduler:us-
west-2:123456789012:schedule-group/your-schedule-group"
                }
            }
        }
    ]
```

```
}
```

Résolution des problèmes d'identité et d'accès à Amazon EventBridge Scheduler

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lors de l'utilisation de EventBridge Scheduler et d'IAM.

Rubriques

Je ne suis pas autorisé à effectuer une action dans le EventBridge planificateur

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `scheduler:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 scheduler:GetWidget on resource: my-example-widget
```

Dans ce cas, la stratégie de Mateo doit être mise à jour pour l'autoriser à accéder à la ressource *`my-example-widget`* à l'aide de l'action `scheduler:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle au EventBridge planificateur.

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 effectuer une action dans le EventBridge planificateur. Toutefois, l'action nécessite que le service ait des autorisations accordées par une fonction du 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 stratégies 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 autoriser des personnes extérieures à moi Compte AWS à accéder aux ressources de mon EventBridge planificateur

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 EventBridge Scheduler prend en charge ces fonctionnalités, consultez. Comment fonctionne EventBridge Scheduler 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 intercompte, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

Protection des données dans Amazon EventBridge Scheduler

Le modèle de responsabilité AWS partagée Le modèle s'applique à la protection des données dans Amazon EventBridge Scheduler. 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 en savoir plus 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 sécurité AWS .

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 en savoir plus 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 le EventBridge planificateur ou un autre outil à Services AWS l'aide de la console, de l'API ou AWS des AWS CLI SDK. Toutes les données que vous saisissez 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

Chiffrement au repos

Cette section décrit comment Amazon EventBridge Scheduler chiffre et déchiffre vos données au repos. Les données au repos sont des données stockées dans le EventBridge planificateur et dans les composants sous-jacents du service. EventBridge Le planificateur s'intègre à AWS Key Management Service (AWS KMS) pour chiffrer et déchiffrer vos données à l'aide d'un. AWS KMS key EventBridge Le planificateur prend en charge deux types de clés KMS : Clés détenues par AWSet les clés gérées par le client.

> **Note**
>
> EventBridge Le planificateur prend uniquement en charge l'utilisation de clés KMS de chiffrement symétriques.

Clés détenues par AWSsont des clés KMS qu'un AWS service possède et gère pour être utilisées dans plusieurs AWS comptes. Bien que les utilisations du Clés détenues par AWS EventBridge planificateur ne soient pas stockées dans votre AWS compte, le EventBridge planificateur les

utilise pour protéger vos données et vos ressources. Par défaut, EventBridge Scheduler chiffre et déchiffre toutes vos données à l'aide d'une clé propriétaire. AWS Vous n'avez pas besoin de gérer votre politique d'accès Clé détenue par AWS ou la sienne. Vous n'avez pas à payer de frais lorsque EventBridge Scheduler les utilise Clés détenues par AWS pour protéger vos données, et leur utilisation n'est pas prise en compte dans les AWS KMS quotas de votre compte.

Les clés gérées par le client sont des clés KMS stockées dans votre AWS compte que vous créez, détenez et gérez. Si votre cas d'utilisation spécifique nécessite que vous contrôliez et auditiez les clés de chiffrement qui protègent vos données sur EventBridge Scheduler, vous pouvez utiliser une clé gérée par le client. Si vous choisissez une clé gérée par le client, vous devez gérer votre politique en matière de clés. Les clés gérées par le client entraînent des frais mensuels et des frais pour une utilisation au-delà de l'offre gratuite. L'utilisation d'une clé gérée par le client compte également dans votre AWS KMS quota. Pour plus d'informations sur les tarifs, consultez la section AWS Key Management Service tarification.

Rubriques

- Artefacts de chiffrement
- Gestion des clés KMS
- CloudTrail exemple d'événement

Artefacts de chiffrement

Le tableau suivant décrit les différents types de données que EventBridge Scheduler chiffre au repos, ainsi que le type de clé KMS qu'il prend en charge pour chaque catégorie.

Type de données	Description	Clé détenue par AWS	clé gérée par le client
Charge utile (jusqu'à 256 Ko)	Les données que vous spécifiez dans le `TargetInput` paramètre du planning lorsque vous configurez le planning à livrer à la cible.	Pris en charge	Pris en charge
Identifiant et état	Le nom unique et l'état (activation,	Pris en charge	Non pris en charge

Type de données	Description	Clé détenue par AWS	clé gérée par le client
	désactivation) du planning.		
Planification d'une Configuration.	L'expression de planification, telle que l'expression rate ou cron pour les plannings récurrents, et l'horodatage pour les invocations ponctuelles, ainsi que la date de début, la date de fin et le fuseau horaire du planning.	Pris en charge	Non pris en charge
Configuration de la cible	Le nom de ressource Amazon (ARN) de la cible et d'autres détails de configuration liés à la cible.	Pris en charge	Non pris en charge
Configuration du comportement d'appel et de défaillance	Configuration flexible des fenêtres horaires, politique de nouvelles tentatives du calendrier et détails de la file d'attente en cas d'échec des livraisons.	Pris en charge	Non pris en charge

EventBridge Le planificateur utilise les clés gérées par le client uniquement pour chiffrer et déchiffrer la charge utile cible, comme décrit dans le tableau précédent. Si vous choisissez d'utiliser une clé gérée par le client, EventBridge Scheduler chiffre et déchiffre la charge utile deux fois : une fois en

utilisant la clé par défaut Clé détenue par AWS et une autre fois en utilisant la clé gérée par le client que vous spécifiez. Pour tous les autres types de données, EventBridge Scheduler utilise uniquement la valeur par défaut Clé détenue par AWS pour protéger vos données au repos.

Utilisez la the section called "Gestion des clés KMS" section suivante pour savoir comment vous devez gérer vos ressources IAM et vos politiques clés afin d'utiliser une clé gérée par le client avec EventBridge Scheduler.

Gestion des clés KMS

Vous pouvez éventuellement fournir une clé gérée par le client pour chiffrer et déchiffrer la charge utile que votre planning envoie à sa cible. EventBridge Le planificateur chiffre et déchiffre votre charge utile jusqu'à 256 Ko de données. L'utilisation d'une clé gérée par le client entraîne des frais mensuels et des frais supérieurs au niveau gratuit. L'utilisation d'un compte clé géré par le client dans le cadre de votre AWS KMS quota. Pour plus d'informations sur la tarification, consultez la section AWS Key Management Service tarification

EventBridge Le planificateur utilise les autorisations IAM associées au principal qui crée un calendrier pour chiffrer vos données. Cela signifie que vous devez associer les autorisations AWS KMS associées requises à l'utilisateur, ou au rôle, qui appelle l'API EventBridge Scheduler. En outre, EventBridge Scheduler utilise des politiques basées sur les ressources pour déchiffrer vos données. Cela signifie que le rôle d'exécution associé à votre calendrier doit également disposer des autorisations AWS KMS associées requises pour appeler l' AWS KMS API lors du déchiffrement des données.

> **Note**
>
> EventBridge Le planificateur ne prend pas en charge l'utilisation de subventions pour des autorisations temporaires.

Consultez la section suivante pour savoir comment gérer votre politique en matière de AWS KMS clés et les autorisations IAM requises pour utiliser une clé gérée par le client sur EventBridge Scheduler.

Rubriques

- Ajouter des autorisations IAM
- Gérer la politique clé

Ajouter des autorisations IAM

Pour utiliser une clé gérée par le client, vous devez ajouter les autorisations suivantes au principal IAM basé sur l'identité qui crée un calendrier, ainsi qu'au rôle d'exécution que vous associez au calendrier.

Autorisations basées sur l'identité pour les clés gérées par le client

Vous devez ajouter les AWS KMS actions suivantes à la politique d'autorisation associée à tout principal (utilisateurs, groupes ou rôles) qui appelle l'API EventBridge Scheduler lors de la création d'un calendrier.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "scheduler:*",

                # Required to pass the execution role
                "iam:PassRole",

                "kms:DescribeKey",
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
    ]
}
```

- **`kms:DescribeKey`**— Nécessaire pour valider que la clé que vous fournissez est une clé KMS de chiffrement symétrique.
- **`kms:GenerateDataKey`**— Nécessaire pour générer la clé de données que EventBridge Scheduler utilise pour effectuer le chiffrement côté client.
- **`kms:Decrypt`**— Nécessaire de déchiffrer la clé de données cryptée que EventBridge Scheduler stocke avec vos données cryptées.

Autorisations relatives aux rôles d'exécution pour les clés gérées par le client

Vous devez ajouter l'action suivante à la politique d'autorisation des rôles d'exécution de votre calendrier afin de permettre au EventBridge Scheduler d'appeler l' AWS KMS API lors du déchiffrement de vos données.

```
{
    "Version": "2012-10-17",
    "Statement" : [
    {
      "Sid" : "Allow EventBridge Scheduler to decrypt data using a customer managed
 key",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"

      ],
      "Resource": "arn:aws:kms:your-region:123456789012:key/your-key-id"
    }
  ]
}
```

- **`kms:Decrypt`**— Nécessaire de déchiffrer la clé de données cryptée que EventBridge Scheduler stocke avec vos données cryptées.

Si vous utilisez la console du EventBridge planificateur pour créer un nouveau rôle d'exécution lorsque vous créez un nouveau calendrier, le EventBridge planificateur associera automatiquement l'autorisation requise à votre rôle d'exécution. Toutefois, si vous choisissez un rôle d'exécution existant, vous devez ajouter les autorisations requises au rôle pour pouvoir utiliser les clés gérées par vos clients.

Gérer la politique clé

Lorsque vous créez une clé gérée par le client en utilisant AWS KMS, par défaut, votre clé possède la politique de clé suivante pour donner accès aux rôles d'exécution de vos plannings.

```
{
    "Id": "key-policy-1",
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "Provide required IAM Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        }
    ]
}
```

Vous pouvez éventuellement limiter la portée de votre politique clé afin de ne donner accès qu'au rôle d'exécution. Vous pouvez le faire si vous souhaitez utiliser votre clé gérée par le client uniquement avec les ressources de votre EventBridge planificateur. Utilisez l'exemple de politique clé suivant pour limiter les ressources du EventBridge planificateur qui peuvent utiliser votre clé.

```
{
    "Id": "key-policy-2",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Provide required IAM Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::695325144837:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:role/schedule-execution-role"
            },
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "*"
        }
    ]
}
```

CloudTrail exemple d'événement

AWS CloudTrail capture tous les événements des appels d'API. Cela inclut les appels d'API chaque fois que le EventBridge planificateur utilise votre clé gérée par le client pour déchiffrer vos données. L'exemple suivant montre une entrée d' CloudTrail événement qui montre que EventBridge Scheduler utilise l'`kms:Decrypt`action à l'aide d'une clé gérée par le client.


```
{
  "eventVersion": "1.08",
  "userIdentity": {
      "type": "AssumedRole",
      "principalId": "ABCDEABCD1AB12ABABAB0:70abcd123a123a12345a1aa12aa1bc12",
      "arn": "arn:aws:sts::123456789012:assumed-role/execution-
role/70abcd123a123a12345a1aa12aa1bc12",
      "accountId": "123456789012",
      "accessKeyId": "ABCDEFGHI1JKLMNOP2Q3",
      "sessionContext": {
          "sessionIssuer": {
              "type": "Role",
              "principalId": "ABCDEABCD1AB12ABABAB0",
              "arn": "arn:aws:iam::123456789012:role/execution-role",
              "accountId": "123456789012",
              "userName": "execution-role"
          },
          "webIdFederationData": {},
          "attributes": {
              "creationDate": "2022-10-31T21:03:15Z",
              "mfaAuthenticated": "false"
          }
      }
    },
    "eventTime": "2022-10-31T21:03:15Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "eu-north-1",
    "sourceIPAddress": "13.50.87.173",
    "userAgent": "aws-sdk-java/2.17.295 Linux/4.14.291-218.527.amzn2.x86_64 OpenJDK_64-
Bit_Server_VM/11.0.17+9-LTS Java/11.0.17 kotlin/1.3.72-release-468 (1.3.72) vendor/
Amazon.com_Inc. md/internal exec-env/AWS_ECS_FARGATE io/sync http/Apache cfg/retry-
mode/standard AwsCrypto/2.4.0",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-west-2:123456789012:key/2321abab-2110-12ab-a123-
a2b34c5abc67",
```

```
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "encryptionContext": {
            "aws:scheduler:schedule:arn": "arn:aws:scheduler:us-
west-2:123456789012:schedule/default/execution-role"
        }
    },
    "responseElements": null,
    "requestID": "request-id",
    "eventID": "event-id",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:123456789012:key/2321abab-2110-12ab-a123-
a2b34c5abc67"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
      "tlsVersion": "TLSv1.3",
      "cipherSuite": "TLS_AES_256_GCM_SHA384",
      "clientProvidedHostHeader": "kms.us-west-2.amazonaws.com"
  }
}
```

Chiffrement en transit

EventBridge Le planificateur chiffre vos données en transit lorsqu'elles circulent sur le réseau. Le protocole TLS (Transport Layer Security) chiffre vos données lorsque vous appelez une opération d'API du EventBridge planificateur, ainsi que lorsque le EventBridge planificateur appelle une API cible lorsqu'il appelle votre calendrier. Par défaut, EventBridge Scheduler utilise le protocole TLS 1.2 pour chiffrer vos données en transit. Il n'est pas nécessaire de configurer le chiffrement en transit, et vous ne pouvez pas choisir une autre version du protocole TLS lorsque vous utilisez le EventBridge planificateur.

Utilisation de l'API EventBridge Scheduler — Lorsque vous effectuez une opération d'API, telle que, EventBridge Scheduler chiffre l'intégralité de la requête HTTP`CreateSchedule`, y compris le corps

de la demande et les en-têtes. EventBridge Le planificateur chiffre également l'intégralité de l'objet de réponse que vous recevez de nos API.

Utilisation des API cibles : lorsque le EventBridge planificateur appelle votre calendrier, il appelle l'API cible que vous avez spécifiée lors de la création du calendrier. Lors de la transmission d'un événement à une cible, le EventBridge planificateur chiffre l'intégralité de la demande, y compris le corps de la demande et tous les en-têtes, ainsi que la réponse qu'il reçoit de la cible.

Validation de conformité pour Amazon EventBridge Scheduler

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. 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 Services AWS 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 : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

> **Note**
>
> Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- 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.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière

de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans plusieurs cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).

- Évaluation des ressources à l'aide des règles du 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— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience dans Amazon EventBridge Scheduler

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS 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.

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section Infrastructure AWS globale.

Outre l'infrastructure AWS mondiale, EventBridge Scheduler propose plusieurs fonctionnalités pour répondre à vos besoins en matière de résilience et de sauvegarde des données.

Sécurité de l'infrastructure dans Amazon EventBridge Scheduler

En tant que service géré, Amazon EventBridge Scheduler 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 au EventBridge Scheduler 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.

Surveillance et statistiques pour Amazon EventBridge Scheduler

La surveillance est un enjeu important pour assurer la sécurité et d'Amazon Scheduler et de vos autres solutions Amazon EventBridge Scheduler et de vos autresAWS solutions. AWSfournit les outils de surveillance suivants pour surveiller EventBridge Scheduler, signaler les incidents et prendre des mesures automatiques le cas échéant :

- Amazon CloudWatch surveille vosAWS ressources et les applications que vous exécutez surAWS en temps réel. Vous pouvez collecter et suivre les métriques, créer des tableaux de bord personnalisés, et définir des alarmes qui vous informent ou prennent des mesures lorsqu'une métrique spécifique atteint un seuil que vous spécifiez. Pour de plus amples informations, veuillez consulter le Guide de l' CloudWatch utilisateur Amazon Amazon Amazon Amazon Amazon Amazon Amazon Amazon
- AWS CloudTrail capture les appels d'API et les événements associés créés par ou au nom de votre compte AWS et envoie les fichiers journaux à un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes qui ont appelé AWS, l'adresse IP source à partir de laquelle les appels ont été émis, ainsi que le moment où les appels ont eu lieu. Pour de plus amples informations, veuillez consulter le Guide de l'utilisateur AWS CloudTrail.

Rubriques

Surveillance d'Amazon EventBridge Scheduler avec Amazon CloudWatch

Vous pouvez contrôler Amazon EventBridge Scheduler à l'aide de CloudWatch, qui collecte les données brutes et les transforme en métriques lisibles et disponibles presque en temps réel. EventBridge Le planificateur émet un ensemble de mesures pour tous les programmes et un ensemble supplémentaire de mesures pour les programmes auxquels est associée une file d'attente de lettres mortes (DLQ). Si vous configurez un DLQ pour votre calendrier, EventBridge Scheduler publie des mesures supplémentaires lorsque votre calendrier n'est plus soumis à la politique de nouvelles tentatives.

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 programme 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 de plus amples amples informations, veuillez consulter le Guide de CloudWatch l'utilisateur Amazon.

Rubriques

Conditions

Espace de noms

Un espace de noms est un conteneur pour les CloudWatch métriques d'unAWS service. Pour EventBridge Scheduler, l'espace de noms est`AWS/Scheduler`.

CloudWatch métriques

Une CloudWatch métrique représente un ensemble de points de données chronologiques qui sont spécifiques aux métriques CloudWatch.

Dimension

Une dimension est une paire nom-valeur qui fait partie de l'identité d'une métrique.

Unité

Une statistique possède une unité de mesure. Pour EventBridge Scheduler, les unités incluent Count.

Dimensions

Cette section décrit le regroupement des CloudWatch dimensions pour les métriques du EventBridge Scheduler dans CloudWatch.

Dimension	Description
ScheduleGroup	Le groupe de calendriers pour lequel vous souhaitez afficher les métriques CloudWatch. Si vous n'avez encore créé aucun groupe, EventBridge Scheduler associe vos plannings au `default` groupe.

Accès aux métriques

Cette section explique comment accéder aux mesures de performance CloudWatch pour un calendrier EventBridge de planification spécifique.

Pour consulter les métriques de performances pour une dimension

1. Ouvrez la page Metrics sur la CloudWatch console.
2. Utilisez le sélecteur deAWS région pour choisir la région pour votre programme
3. Choisissez l'espace de noms du planificateur.
4. Dans l'onglet Toutes les mesures, choisissez une dimension, par exemple, Planifier les mesures de groupe. Pour consulter les statistiques de tous les calendriers que vous avez créés dans la région sélectionnée, choisissez Mesures du compte.
5. Choisissez une CloudWatch métrique pour une dimension. Par exemple, InvocationAttemptCountou InvocationDroppedCount, choisissez Recherche graphique.
6. Cliquez sur l'onglet Indicateurs graphiques pour afficher les statistiques de performance des métriques EventBridge du Planificateur.

Répertorier les métriques

Les tableaux suivants répertorient les mesures pour tous les plannings du EventBridge Scheduler, ainsi que des métriques supplémentaires pour les plannings pour lesquels vous avez configuré un DLQ.

métriques pour toutes les métriques

Espace de noms	Mesure	Unité	Description
AWS/Scheduler	InvocationAttemptCount	Nombre	Émis à chaque tentative d'invocation. Utilisez cette métrique pour vérifier que EventBridge Scheduler tente d'appeler vos calendriers et pour voir à quel moment les appels approchent des quotas de votre compte.
AWS/Scheduler	TargetErrorCount	Nombre	Émis lorsque la cible renvoie une exception après que EventBridge Scheduler a appelé l'API cible. Utilisez-le pour vérifier si la livraison

Espace de noms	Mesure	Unité	Description
			à une cible échoue.
AWS/Scheduler	TargetErrorThrottledCount	Nombre	Émis lorsque l'invocation de la cible échoue en raison de la limitation de l'API par la cible. Utilisez-le pour diagnostiquer les échecs de livraison lorsque la raison sous-jacente est l'API cible, les appels de limitation effectués par EventBridge Scheduler.

Espace de noms	Mesure	Unité	Description
AWS/Scheduler	InvocationThrottleCount	Nombre	Émis lorsque EventBridge Scheduler limite l'invocation d'une cible parce qu'elle dépasse les quotas de service définis par EventBridge Scheduler. Utilisez-le pour déterminer à quel moment vous avez dépassé les quotas de votre EventBridge planificateur. Pour de plus amples informations sur les quotas de service, consultez Quotas.

Espace de noms	Mesure	Unité	Description
AWS/Scheduler	InvocationDroppedCount	Nombre	Émis lorsque le EventBridge planificateur arrête de tenter d'appeler la cible une fois que la politique de nouvelle tentative d'un calendrier a été épuisée. Pour plus d'informations sur les politiques relatives aux nouvelles tentatives, consultez RetryPolicyla référence de l'APIEventBridge Scheduler.

Métriques pour les plannings dotés d'un DLQ

Espace de noms	Mesure	Unité	Description
AWS/Scheduler	InvocationsSentToDeadLetterCount	Nombre	Émis pour chaque livraison

Espace de noms	Mesure	Unité	Description
			réussie au DLQ d'un calendrier. Utilisez-le pour déterminer à quel moment les événements sont envoyés à un DLQ, puis vérifiez l'événement envoyé au DLQ du calendrier pour obtenir des informations supplémentaires qui vous aideront à déterminer la cause de l'échec.

Espace de noms	Mesure	Unité	Description
AWS/Scheduler	InvocationsFailedToBeSentToDeadLetterCount	Nombre	Émis lorsque le EventBridge planificateur ne parvient pas à transmettre un événement au DLQ. Utilisez ces deux mesures pour déterminer la raison pour laquelle EventBridge Scheduler n'est pas en mesure d'envoyer un événement au DLQ et modifiez la configuration de votre DLQ pour résoudre le problème. Voici un exemple deInvocationsFailedToBeSentToDeadLette
AWS/Scheduler	InvocationsFailedToBeSentToDeadLetterCount_<error_code>	Nombre	

Espace de noms	Mesure	Unité	Description
			rCount_<error_code> métrique lorsque la file d'attente Amazon SQS que vous spécifiez en tant que DLQ n'existe pas :InvocationsFailedToBeSentToDeadLetterCount_ **AWS.SimpleQueueService.NonExistentQueue**

Espace de noms	Mesure	Unité	Description
AWS/Scheduler	InvocationsSentToDeadLetterCount_Truncated_MessageSizeExceeded	Nombre	Émis lorsque la charge utile de l'événement envoyé au DLQ dépasse la taille maximale autorisée par Amazon SQS, et que EventBridge Scheduler tronque la charge utile que vous spécifiez dans l'Inputattribut d'un calendrier.

Journalisation des appels d'API Amazon EventBridge Scheduler à l'aide deAWS CloudTrail

Amazon EventBridge Scheduler est intégré avecAWS CloudTrail, un service qui enregistre les actions effectuées par un utilisateur, un rôle ou unAWS service dans EventBridge Scheduler. CloudTrail capture les appels d'API pour EventBridge Scheduler en tant qu'événements. Les appels capturés incluent des appels de la console EventBridge Scheduler et les appels de code adressés aux opérations d'API EventBridge Scheduler. Si vous créez un journal de suivi, vous pouvez activer l'envoi en continu d' CloudTrail événements à un compartiment Amazon S3, notamment d'événements pour EventBridge Scheduler. Si vous ne configurez pas de journal d'activité, vous pouvez toujours afficher 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 envoyée à EventBridge Scheduler, l'adresse IP à partir de laquelle la demande a été effectuée, l'auteur de la demande, la date de la demande, ainsi que d'autres informations.

Pour en savoir plus CloudTrail, consultez le Guide deAWS CloudTrail l'utilisateur.

EventBridge Informations sur le planificateur dans CloudTrail

CloudTrail est activé dans votreCompte AWS lors de la création de ce dernier. Lorsqu'une activité a lieu dans le EventBridge Planificateur, cette activité est enregistrée dans un CloudTrail événement avec d'autres événementsAWS de service dans Historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre Compte AWS. Pour de plus amples informations, veuillez consulter Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements dans votreCompte AWS, y compris les événements pour EventBridge Scheduler, créez un journal de suivi. Un journal CloudTrail de suivi permet de livrer des fichiers journaux dans un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal d'activité consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Simple Storage Service (Amazon S3) de votre choix. En outre, vous pouvez configurer d'autresAWS services pour analyser plus en profondeur les données d'événements collectées dans les CloudTrail journaux et agir sur celles-ci. Pour en savoir plus, consultez les ressources suivantes :

- Présentation de la création d'un journal d'activité
- CloudTrail services et intégrations pris en charge
- Configuration de notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail CloudTrail journaux de plusieurs comptes

Toutes les actions EventBridge du planificateur sont enregistrées CloudTrail et documentées dans la référence de l'API Amazon EventBridge Scheduler. Par exemple, les appels à`UpdateSchedule` et les`CreateScheduleDeleteSchedule` actions génèrent des entrées dans les fichiers CloudTrail journaux.

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 effectuée avec les informations d'identification utilisateur racine ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre service AWS.

Pour de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

EventBridge Présentation de fichiers journaux

Un journal de suivi est une configuration qui permet la remise d'événements sous forme de fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux peuvent contenir une ou plusieurs entrées de journaux. Un événement représente une demande individuelle émise à partir d'une source quelconque et comprend des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail Les fichiers journaux ne constituent pas une pile ordonnée retraçant les appels d'API publics.

Quotas pour Amazon EventBridge Scheduler

Votre AWS compte dispose de quotas par défaut, anciennement appelés limites, pour chaque AWS service. Sauf indication contraire, chaque quota est spécifique à la région. Vous pouvez demander des augmentations pour certains quotas, mais d'autres ne peuvent pas être augmentés.

Pour consulter les quotas du EventBridge Scheduler, ouvrez la console Service Quotas. Dans le volet de navigation, choisissez AWS services, puis sélectionnez EventBridge Planificateur.

Pour demander une augmentation de quota, consultez Demande d'augmentation de quota dans le Guide de l'utilisateur Service Quotas. Si le quota n'est pas encore disponible dans Service Quotas, utilisez le Formulaire d'augmentation de limite de service.

> **Note**
>
> Les quotas de `CreateScheduleUpdateSchedule`,`GetSchedule`, et de `DeleteSchedule` transactions par seconde (TPS) pour EventBridge Scheduler sont ajustables jusqu'à des milliers de TPS. Le quota d'appels est ajustable jusqu'à des dizaines de milliers de TPS.

Votre AWS compte possède les quotas suivants liés au EventBridge planificateur.

Nom	Par défaut	Ajusta	Description
CreateSchedule taux de demandes	Chaque Région prise en charge : 50	Oui	Nombre maximum CreateSchedule de demandes par seconde. Lorsque vous atteignez ce quota, le EventBrid ge planificateur rejette les demandes pour cette opération pour le reste de l'intervalle.
CreateScheduleGroup taux de demandes	Par région prise en charge : 10	Oui	Nombre maximum CreateScheduleGroup de

Nom	Par défaut	Ajusta	Description
			demandes par seconde. Lorsque vous atteignez ce quota, le EventBrid ge planificateur rejette les demandes pour cette opération pour le reste de l'intervalle.
DeleteSchedule taux de demandes	Chaque Région prise en charge : 50	Oui	Nombre maximum DeleteSchedule de demandes par seconde. Lorsque vous atteignez ce quota, le EventBrid ge planificateur rejette les demandes pour cette opération pour le reste de l'intervalle.
DeleteScheduleGroup taux de demandes	Par région prise en charge : 10	Oui	Nombre maximum DeleteScheduleGroup de demandes par seconde. Lorsque vous atteignez ce quota, le EventBrid ge planificateur rejette les demandes pour cette opération pour le reste de l'intervalle.

Nom	Par défaut	Ajusta	Description
GetSchedule taux de demandes	Chaque Région prise en charge : 50	Oui	Nombre maximum GetSchedule de demandes par seconde. Lorsque vous atteignez ce quota, le EventBrid ge planificateur rejette les demandes pour cette opération pour le reste de l'intervalle.
GetScheduleGroup taux de demandes	Par région prise en charge : 10	Oui	Nombre maximum GetScheduleGroup de demandes par seconde. Lorsque vous atteignez ce quota, le EventBrid ge planificateur rejette les demandes pour cette opération pour le reste de l'intervalle.
Limite d'invocations dans les transacti ons par seconde	Chaque région prise en charge : 500	Oui	Un appel est une charge utile planifiée envoyée à la cible définie. Une fois la limite atteinte, les invocations sont limitées, c'est-à-dire qu'elles se produisent encore, mais sont retardées.

Nom	Par défaut	Ajusta	Description
ListScheduleGroups taux de demandes	Par région prise en charge : 10	Oui	Nombre maximum ListScheduleGroups de demandes par seconde. Lorsque vous atteignez ce quota, le EventBrid ge planificateur rejette les demandes pour cette opération pour le reste de l'intervalle.
ListSchedules taux de demandes	Chaque Région prise en charge : 50	Oui	Nombre maximum ListSchedules de demandes par seconde. Lorsque vous atteignez ce quota, le EventBrid ge planificateur rejette les demandes pour cette opération pour le reste de l'intervalle.
ListTagsForResource taux de demandes	Par région prise en charge : 10	Oui	Répertorie les balises associées à la ressource Scheduler.
Nombre de groupes d'horaires	Chaque région prise en charge : 500	Oui	Nombre maximum de groupes d'horaires par région.

Nom	Par défaut	Ajusta	Description
Nombre de plannings	Chaque région prise en charge : 1 000 000	Oui	Le nombre maximum de programmes par région. Ce quota inclut les programmes ponctuels dont l'exécuti on est terminée. Nous vous recommand ons de supprimer vos programmes ponctuels une fois qu'ils ont terminé leur exécution et qu'ils ont invoqué un objectif.
TagResource taux de demandes	Par région prise en charge : 1	Oui	Affecte une ou plusieurs balises (paires clé-valeur) à la ressource Scheduler spécifiée.
UntagResource taux de demandes	Par région prise en charge : 1	Oui	Supprime une ou plusieurs balises de la ressource Scheduler spécifiée.
UpdateSchedule taux de demandes	Chaque Région prise en charge : 50	Oui	Nombre maximum UpdateSchedule de demandes par seconde. Lorsque vous atteignez ce quota, le EventBrid ge planificateur rejette les demandes pour cette opération pour le reste de l'intervalle.

Pour plus d'informations sur les quotas et les points de terminaison de service pour le EventBridge Scheduler, consultez la section Points de terminaison et quotas Amazon EventBridge Scheduler dans le guide de référence général. AWS

Historique des documents pour EventBridge Guide d'utilisation du planificateur

Le tableau suivant décrit les versions de votre envoi d'une documentation pour EventBridge Planificateur.

Modification	Description	Date
Changements apportés au rôle d'exécution et confusion en matière de prévention des adjoints	Cette mise à jour décrit les modifications apportées à la manière dont le rôle d'exécution est appliqué à une ressource de groupe de planification lorsque vous implémentez la prévention de la confusion dans les adjoints dans la politique d'autorisation du rôle. • the section called “Prévention de l'adjoint confus”	7 septembre 2023
Suppression automatique des plannings une fois terminés	EventBridge Le planificateur prend en charge la suppression automatique. Lorsque vous configurez la suppression automatique, EventBridge Le planificateur supprime votre calendrier après sa dernière invocation planifiée. • the section called “Suppression une fois le planning terminé”	02/08/2023

Rubrique mise à jour sur l'utilisation de cibles universelles	Mise à jour de la liste des services pris en charge qui EventBridge Le planificateur peut cibler et intégrer. Cette mise à jour inclut également une liste des métriques non prises en charge`GET`Opérations d'API, et inclut des améliorations apportées aux exemples de cibles universelles, ainsi que d'autres améliorations mineures apportées à l'ensemble du guide. • the section called “Utiliser des cibles universelles”	17 mars 2023
Informations mises à jour sur les programmes basés sur les tarifs qui n'ont pas de date de début	Informations supplémentaires sur la façon dont EventBridge Le planificateur gère les plannings basés sur les taux si vous ne spécifiez pas de`StartDate`. • the section called “Horaires basés sur les tarifs”	17 mars 2023

Nouveau sujet sur la gestion des groupes de planificateurs	Ajout d'un nouveau chapitre sur la création de groupes de planificateurs avec EventBridge Planificateur. Utilisez ce chapitre pour apprendre à créer un groupe, à ajouter des horaires au groupe, à appliquer des balises pour gérer et surveiller plus facilement votre EventBridge Planifier les ressources, et enfin supprimer un groupe. • Gestion d'un groupe de planning	17 mars 2023
Nouveaux sujets sur l'heure d'été et les fuseaux horaires	Ajout de nouvelles sections qui décrivent comment EventBridge Le planificateur gère l'heure d'été et la façon dont vous pouvez créer des horaires dans différents fuseaux horaires. • the section called "Heure d'été" • the section called "Fuseaux horaires"	17 novembre 2022

Nouveau sujet sur les métriques	Ajout d'une nouvelle rubrique qui décrit les mesures qui EventBridge Le planificateur publie sur CloudWatch. Vous pouvez utiliser ces métriques pour surveiller les échecs de votre envoi d'appels. Vous pouvez utiliser ces métriques pour surveiller les métriques. • the section called "Surveillance avec CloudWatch"	15 novembre 2022
Première version	Publication initiale du EventBridge Guide d'utilisation du planificateur.	10 novembre 2022

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.