aws

Guide de l’utilisateur

EventBridge Planificateur

EventBridge Planificateur: Guide de l’utilisateur

Table of Contents

Qu'est-ce qu'Amazon EventBridge Scheduler ?

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 centralisé. Très évolutif, le EventBridge planificateur vous permet de planifier des millions de tâches pouvant appeler plus de 270 AWS services et plus de 6 000 API opérations. Sans avoir à provisionner et à gérer l'infrastructure, ou à intégrer plusieurs services, EventBridge Scheduler vous permet de mettre en place des plannings à grande échelle et de réduire les coûts de maintenance.

EventBridge Le planificateur exécute vos tâches de manière fiable, grâce à des mécanismes intégrés qui ajustent vos plannings 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 les modèles récurrents, ou configurer des appels ponctuels. Vous pouvez configurer des fenêtres temporelles 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 du EventBridge planificateur

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

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

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

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

Accès au EventBridge planificateur

Vous pouvez utiliser le EventBridge planificateur via la EventBridge console, le EventBridge planificateurSDK, le ou en utilisant directement le AWS CLI planificateur. EventBridge API

Configuration d'Amazon EventBridge Scheduler

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

Rubriques

Inscrivez-vous pour AWS

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

Pour vous inscrire à un Compte AWS

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

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

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des AWS services et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l'utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

Création d'un utilisateur IAM

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

Choisissez un moyen de gérer votre administrateur	Pour	Par	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 meilleures pratiques, consultez la section Bonnes pratiques en matière de sécurité IAM dans le guide de IAM l'utilisateur.	Suivre les instructions de la section Mise en route dans le AWS IAM Identity Center Guide de l'utilisateur.	Configurez l'accès par programmation en configurant le AWS CLI à utiliser AWS IAM Identity Center dans le guide de l'AWS Command Line Interface utilisateur.
Dans IAM (Non recommandé)	Utiliser des identifiants à long terme pour accéder à AWS.	Suivez les instructions de la section Création de votre premier utilisateur IAM administrateur et de votre premier groupe d'utilisateurs dans le guide de IAM l'utilisateur.	Configurez l'accès par programmation en gérant les clés d'accès pour IAM les utilisateurs dans le guide de IAM l'utilisateur.

Utiliser des politiques gérées

À l'étape précédente, vous avez configuré un IAM utilisateur 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 du. API
- the section called "`AmazonEventBridgeSchedulerReadOnlyAccess`"— Accorde un accès en lecture seule au planificateur. EventBridge

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

Configurer le rôle d'exécution

Un rôle d'exécution est un IAM rôle que le EventBridge planificateur assume afin d'interagir avec d'autres personnes en votre AWS services 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 JSON politique d'acceptation des rôles 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 réussite, 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 JSON d'autorisation et enregistrez-la localement sous forme de `.json` fichier.

   Amazon SQS – SendMessage

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

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

   Amazon SNS – Publish

   Ce qui suit permet au EventBridge Scheduler de lancer l'`sns:Publish`action sur tous les SNS sujets Amazon 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. Prenez note de la politiqueARN. Vous l'ARNutiliserez 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 ARN celui 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 SQS file d'attente Amazon standard avec AWS CloudFormation.

Pour créer une nouvelle SQS file d'attente Amazon

1. Copiez le JSON AWS CloudFormation modèle suivant et enregistrez-le localement sous le nom`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 du AWS 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 réussite, 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 SQS file d'attente Amazon 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 AWS SDKs pour créer un calendrier avec un modèle de cible AmazonSQS. 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 IAM les utilisateurs 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 le AWS 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 Interface utilisateur 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 une planification à l'aide de la console

1. Connectez-vous au AWS Management Console, puis cliquez sur le lien suivant pour ouvrir la section EventBridge Planificateur de la EventBridge console : home ? https://us-west-2.console.aws.amazon.com/scheduler/ 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 Planification basée sur le taux et entrez un nombre positif pour Valeur, puis choisissez une unité dans les options déroulantes.

   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. 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 cibleAPI. Pour cet exemple, nous allons choisir la cible SQS `SendMessage` modélisée par Amazon.

   b. SendMessageDans la section « SQSfile d'attente », choisissez une SQS file d'attente Amazon existante, `arn:aws:sqs:`*`us-west-2`*`:`*`123456789012`*`:`*`TestQueue`* par ARN

exemple dans la liste déroulante. Pour créer une nouvelle file d'attente, choisissez Create new SQS queue pour accéder à la SQS console Amazon. Après avoir créé une file d'attente, revenez à la console du EventBridge planificateur et actualisez le menu déroulant. Votre nouvelle file d'attente ARN apparaît et peut être sélectionnée.

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 DELETEsi 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 NONEou ne choisissez pas une valeur si vous ne souhaitez pas que le EventBridge planificateur prenne des mesures une fois le planning terminé.

c. Dans la section Politique de réessai et file d'attente de lettres mortes (DLQ), pour la politique de réessai, activez Réessayer pour configurer une politique de nouvelle tentative 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 Dead-letter queue (DLQ), choisissez l'une des options suivantes :

- Aucun — Choisissez cette option si vous ne souhaitez pas configurer unDLQ.
- Sélectionnez une SQS file d'attente Amazon dans mon AWS compte sous la forme DLQ : choisissez cette option, puis sélectionnez une file d'attente ARN dans la liste déroulante, configurez DLQ la même Compte AWS que celle dans laquelle vous créez le calendrier.
- Spécifiez une SQS file d'attente Amazon dans un autre AWS compte comme DLQ suit : choisissez cette option, puis entrez la configuration ARN de la file d'attente comme suitDLQ, si la file d'attente se trouve dans un autre compte Compte AWS. Vous devez saisir le nom exact ARN 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 KMS clé gérée par le client afin de chiffrer votre entrée cible. Si vous choisissez cette option, entrez une KMS clé existante ARN ou choisissez Créer une AWS KMS clé 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 IAM la console 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 planning pour terminer la création de votre nouveau planning. 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 l'SQSobjectif Amazon, ouvrez la SQS console Amazon et procédez comme suit :

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

    b. Choisissez Envoyer et recevoir des messages.

    c. Sur la page Envoyer et recevoir des messages, sous Recevoir des messages, choisissez Solling for 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 `create-schedule`pour créer un calendrier EventBridge Scheduler avec un modèle de cible AmazonSQS. Remplacez les valeurs d'espace réservé pour les paramètres suivants par vos informations :

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

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

Example Python SDK

```
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 Java SDK

```
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 EventBridge planificateurSDK, consultez. AWS CLIGérer un planning
- Pour plus d'informations sur la configuration de cibles modélisées et sur l'utilisation du paramètre de cible universel, consultezGérer les cibles.
- Pour plus d'informations sur les types de données et les API opérations du EventBridge planificateur, consultez la référence du EventBridge planificateur API.

Types d'horaires dans 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 calendrier pour qu'il fonctionne à`1:00`, il invoquera la cible API entre `1:00:00` et`1:00:59`, en supposant qu'aucune fenêtre horaire flexible n'est définie.

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 SQS file d'attente Amazon, en utilisant le type de `SqsParameters` cible modélisé.

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. PSTle premier lundi de chaque mois. 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 SUN - SAT	, - * ? L #
Année	1970-2199	, - * /

Caractères génériques

- Le caractère générique , (virgule) inclut des valeurs supplémentaires. Dans le champ Mois, JANFEB, MAR inclut les mois de janvier, février et mars.
- 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 SQS file d'attente Amazon, en utilisant le type de cible modéliséSqsParameters.

```
$ 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 qu'il a atteint son objectif. 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 entre 13 h et UTC 8 h le 20 novembre 2022 et envoie un message à une SQS file d'attente Amazon, en utilisant le type de cible modéliséSqsParameters.

```
$ 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 le AWS 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 le cron qui invoque un modèle de SQS `SendMessage` cible Amazon à America/New_York tous les 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 programmes 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.

Gérer un planning dans le EventBridge planificateur

Un planning 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 API opération que le EventBridge planificateur appelle en votre nom à chaque fois que votre planning est exécuté. EventBridge Le planificateur prend en charge deux types de cibles : les cibles modélisées appellent API des opérations communes à un groupe principal 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, consultezGérer les cibles.

Vous configurez la façon 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. A DLQ est un outil standard utilisé par Amazon SQS Queue EventBridge Scheduler pour transmettre les événements ayant échoué, une fois que la politique de nouvelle tentative a été épuisée. Vous pouvez utiliser a DLQ pour résoudre les problèmes liés à votre calendrier ou à son objectif en aval. Pour plus d'informations sur, voirthe section called “Configuration d'un DLQ”.

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

Rubriques

- Modification de l'état du planning dans le EventBridge planificateur
- Configuration de fenêtres horaires flexibles dans le EventBridge planificateur
- Configuration de la file d'attente des lettres mortes d'un planning dans le planificateur EventBridge
- Supprimer un calendrier dans le EventBridge planificateur

- Quelle est la prochaine étape ?

Modification de l'état du planning dans le EventBridge planificateur

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

Example Python SDK

```
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 dans le EventBridge planificateur

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 SDK exemples suivants AWS CLI, ainsi que ceux du EventBridge planificateur, `UpdateSchedule` permettent de définir une fenêtre horaire flexible de 15 minutes pour un programme exécuté une fois par heure.

> **Note**
>
> Vous devez indiquer si vous souhaitez définir une fenêtre 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 Python SDK

```
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 de la file d'attente des lettres mortes d'un planning dans le planificateur EventBridge

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

La rubrique suivante appelle cela JSON un événement lettre morte. Un événement avec lettre morte vous permet de résoudre les problèmes liés à votre calendrier ou à vos objectifs. Si vous configurez une politique de nouvelles tentatives pour votre calendrier, le EventBridge planificateur envoie l'événement lettre morte correspondant au nombre maximal de tentatives que vous avez défini.

Les rubriques suivantes décrivent comment configurer une SQS file d'attente Amazon en fonction de votre calendrier, configurer les autorisations dont le EventBridge planificateur a besoin DLQ pour envoyer des messages à Amazon SQS et recevoir des événements de lettre morte de la part du. DLQ

Rubriques

Création d'une SQS file d'attente Amazon

Avant de configurer un DLQ pour votre planning, vous devez créer une file d'SQSattente Amazon standard. Pour obtenir des instructions sur la création d'une file d'attente à l'aide de la SQS console Amazon, consultez la section Création d'une SQS file d'attente Amazon dans le manuel Amazon Simple Queue Service Developer Guide.

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

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

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

En cas de succès, vous le verrez `QueueURL` dans le résultat.

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

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

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

En cas de succès, vous verrez la file d'attente ARN 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 sans réponse à Amazon. SQS

Configurer les autorisations des rôles d'exécution

Pour permettre à EventBridge Scheduler de transmettre des événements sans date limite à AmazonSQS, votre rôle d'exécution du calendrier doit respecter la politique d'autorisation suivante. Pour plus d'informations sur l'attachement d'une nouvelle politique d'autorisation à votre rôle d'exécution de planification, voir Configuration du rôle d'exécution.

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

> **Note**
>
> Votre rôle d'exécution de planification dispose peut-être déjà des autorisations requises si vous utilisez EventBridge Scheduler pour appeler une cible Amazon SQSAPI.

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

Spécifier une file d'attente de lettres mortes

Pour spécifier unDLQ, utilisez la console du EventBridge planificateur ou AWS CLI pour mettre à jour un calendrier existant ou en créer un nouveau.

Console

Pour spécifier un à DLQ l'aide de la console

1. Connectez-vous au AWS Management Console, puis cliquez sur le lien suivant pour ouvrir la section EventBridge Planificateur de la EventBridge console : home https://console.aws.amazon.com/scheduler/
2. Sur la console du EventBridge planificateur, créez un nouveau planning ou choisissez un planning existant dans votre liste de plannings à modifier.
3. Sur la page Paramètres, pour Dead-letter queue (DLQ), effectuez l'une des opérations suivantes :
   - Choisissez Sélectionnez une SQS file d'attente Amazon dans mon AWS compte en tant que DLQ, puis choisissez la file d'attente qui vous ARN DLQ convient dans la liste déroulante.
   - Choisissez Spécifier une SQS file d'attente Amazon dans d'autres AWS comptes en tant que DLQ, puis entrez la file d'attente ARN pour votreDLQ. Si vous choisissez une file d'attente dans un autre AWS compte, la console du EventBridge planificateur ne pourra pas afficher la file d'attente ARNs dans une liste déroulante.
4. Passez en revue vos sélections, puis choisissez Créer un calendrier ou Enregistrer le calendrier pour terminer la configuration d'unDLQ.
5. (Facultatif) Pour consulter les DLQ détails d'un planning, choisissez le nom du planning dans la liste, puis cliquez sur l'onglet File d'attente des lettres mortes sur la page détaillée du planning.

AWS CLI

Pour mettre à jour un calendrier existant à l'aide du AWS CLI

- Utilisez la `update-schedule`commande pour mettre à jour votre planning. Spécifiez la SQS file d'attente Amazon que vous avez créée précédemment en tant queDLQ. Spécifiez le IAM

rôle ARN auquel vous avez attaché les SQS autorisations Amazon 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 à l'DLQaide du AWS 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 le AWS CLI pour recevoir un événement lettre morte de la part du. DLQ

Récupérez l'événement « lettre morte »

Utilisez la `receive-message`commande, comme indiqué ci-dessous, pour récupérer un événement contenant une 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
```

En cas de succès, vous obtiendrez un résultat similaire 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 de lettre morte pour vous aider à identifier et à résoudre les problèmes pouvant expliquer l'échec de l'appel cible.

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

Dans l'exemple précédent, nous pouvons déterminer, en fonction 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 calendrier dans le EventBridge planificateur

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 programmes ponctuels, cela se produit une fois que le calendrier 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 Paramètres.
4. Dans la section Action une fois le planning terminé, DELETEsélectionnez 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 JSON fichier. 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. Vous devez donc spécifier 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 Python SDK

```
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. Gérer les cibles
- Pour plus d'informations sur les types de données et les API opérations du EventBridge planificateur, consultez la référence du EventBridge planificateur API.

Gestion d'un groupe de planification dans le EventBridge planificateur

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 votre Compte 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 à l'aide de la balise suivante : `environment:`*`production`*

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

Un groupe de planification a deux états possibles : ACTIVEet 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 dans le EventBridge planificateur

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 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, consultezPremiers pas.
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 SQS cible Amazon modélisé pour appeler l'`SendMessage`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 le EventBridge planificateur

Dans ce qui suit, vous découvrirez comment supprimer un groupe de planification à l'aide du AWS Management Console et du AWS 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 actuel Région AWS, recherchez le groupe que vous souhaitez supprimer. Si le groupe que vous recherchez ne s'affiche pas, choisissez-en un autre Région 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. Sélectionnez 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 Reference API.
- DeleteScheduleGroupopération dans le EventBridge Scheduler Reference API.

Gestion des cibles dans le EventBridge planificateur

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

Les cibles modélisées sont un ensemble d'APIopérations communes à un groupe de AWS services essentiels tels qu'AmazonSQS, Lambda et Step Functions. Par exemple, vous pouvez cibler l'APIopération Invoke de Lambda en fournissant la fonctionARN, ou l'`SendMessage`opération SQS d'Amazon avec la file d'attente ARN de la cible.

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

Pour configurer des cibles modélisées ou universelles, votre calendrier doit être autorisé à appeler l'APIopération que vous configurez comme cible. Pour ce faire, vous devez associer les autorisations requises au rôle d'exécution de votre planning. Par exemple, pour cibler SQS l'`SendMessage`opération d'Amazon, le rôle d'exécution doit être autorisé à effectuer l'`sqs:SendMessage`action. Dans la plupart des cas, vous pouvez ajouter les autorisations nécessaires en utilisant les politiques AWS gérées prises en charge par le service cible. Toutefois, vous pouvez également créer vos propres politiques gérées par le client ou ajouter des autorisations intégrées 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 plus d'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 dans EventBridge le planificateur

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

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

- 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 différents modèles de cibles et les IAM autorisations 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 Python SDK

```
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 Java SDK

```
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 Python SDK

```
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 Java SDK

```
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 Python SDK

```
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 Java SDK

```
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");
    }
}
```

Utilisation de cibles universelles dans le EventBridge planificateur

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

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

- RoleArn— Le ARN rôle d'exécution que vous souhaitez utiliser pour la cible. Le rôle d'exécution que vous spécifiez doit disposer des autorisations nécessaires pour appeler l'APIopération que vous souhaitez cibler dans votre planning.
- Arn — Le service completARN, y compris l'APIopération que vous souhaitez cibler, au format suivant :`arn:aws:scheduler:::aws-sdk:`*`service`*`:`*`apiAction`*.

  Par exemple, pour AmazonSQS, le nom du service que vous spécifiez est`arn:aws:scheduler:::aws-sdk:`**`sqs:sendMessage`**.
- Entrée — Une entrée bien formée JSON que vous spécifiez avec les paramètres de demande que le EventBridge planificateur envoie à la cible. API Les paramètres et la forme des paramètres JSON que vous définissez `Input` sont déterminés par le service invoqué par API votre calendrier. Pour trouver ces informations, consultez la API référence du service que vous souhaitez cibler.

Actions non prises en charge

EventBridge Le planificateur ne prend pas en charge les API actions 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
invokeModel
```

Par exemple, le service ARN pour l'`GetQueueUrl`APIaction serait le suivant :`arn:aws:scheduler:::aws-sdk:sqs:`**`getQueueURL`**. Comme l'APIaction 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 le service que API vous souhaitez invoquer. Par exemple, pour cibler Lambda `Invoke`, vous pouvez définir les paramètres répertoriés dans AWS Lambda API Reference. Cela inclut la JSON charge utile optionnelle que vous pouvez transmettre à une fonction Lambda.

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

Les exemples suivants montrent comment utiliser la cible universelle pour appeler des API opérations courantes avec LambdaSQS, Amazon 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 dans le EventBridge planificateur

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>**— Celui 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 la création d'un calendrier qui se déclenche toutes les cinq minutes et invoque l'SQS`SendMessage`opération Amazon 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 Python SDK

```
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 API opérations du EventBridge planificateur, consultez la section Référence du EventBridge planificateur API.

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 conformitéAWS .
- 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 AWS service qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. IAMles administrateurs contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources du EventBridge Scheduler. IAMest un AWS service 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 envoyer des demandes à votre IAM administrateur pour modifier les autorisations des utilisateurs de votre service. Consultez les informations de cette page pour comprendre les concepts de base deIAM. Pour en savoir plus sur

la façon dont votre entreprise peut utiliser IAM le EventBridge planificateur, consultez. Comment fonctionne EventBridge Scheduler avec IAM

IAMadministrateur — Si vous êtes IAM administrateur, 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, consultez. IAM Utilisation de politiques basées sur l'identité dans le planificateur EventBridge

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 que Utilisateur racine d'un compte AWS, en tant qu'IAMutilisateur ou en assumant un IAM rôle.

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 (IAMIdentity 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 en tant qu'identité fédérée, votre administrateur a préalablement configuré la fédération d'identité à l'aide de IAM rôles. 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 AWS API demandes dans le guide de IAM l'utilisateur.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez Authentification multifactorielle dans le guide de AWS IAM Identity Center l'utilisateur et Utilisation de l'authentification multifactorielle (MFA) AWS dans le guide de l'IAMutilisateur.

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 AWS services les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui nécessitent que vous vous connectiez en tant qu'utilisateur root, consultez la section Tâches nécessitant des informations d'identification utilisateur root dans le guide de IAM l'utilisateur.

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 AWS services 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 AWS services 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 plus d'informations sur IAM Identity Center, consultez Qu'est-ce qu'IAMIdentity Center ? dans le guide de AWS IAM Identity Center l'utilisateur.

Utilisateurs et groupes IAM

Un IAMutilisateur 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 IAM utilisateurs dotés d'informations d'identification à long terme, telles que des mots de passe et des clés d'accès. Toutefois, si vous avez des cas d'utilisation spécifiques qui nécessitent des informations d'identification à long terme auprès des IAM utilisateurs, nous vous recommandons

de faire pivoter les clés d'accès. Pour plus d'informations, voir Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification à long terme dans le Guide de IAM l'utilisateur.

Un IAMgroupe est une identité qui définit un ensemble d'IAMutilisateurs. 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 nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer IAM des ressources.

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, voir Quand créer un IAM utilisateur (au lieu d'un rôle) dans le Guide de IAM l'utilisateur.

IAMrôles

Un IAMrôle est une identité au sein de Compte AWS vous dotée d'autorisations spécifiques. Il est similaire à un IAM utilisateur, mais n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un IAM rôle dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une AWS API opération AWS CLI or ou en utilisant une option personnaliséeURL. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez la section Utilisation IAM des rôles dans le Guide de IAM l'utilisateur.

IAMles rôles dotés d'informations d'identification temporaires sont utiles dans les situations suivantes :

- 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 plus d'informations sur les rôles pour la fédération, voir Création d'un rôle pour un fournisseur d'identité tiers dans le guide de IAM l'utilisateur. Si vous utilisez IAM Identity Center, vous configurez un ensemble d'autorisations. Pour contrôler les accès auxquels vos identités peuvent accéder après leur authentification, IAM Identity Center met en corrélation l'ensemble d'autorisations avec un rôle dans. IAM Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations IAM utilisateur temporaires : un IAM utilisateur ou un rôle peut assumer un IAM rôle afin d'obtenir temporairement différentes autorisations pour une tâche spécifique.

- Accès entre comptes : vous pouvez utiliser un IAM rôle pour autoriser une personne (un mandant fiable) d'un autre compte à accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains AWS services cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, voir Accès aux ressources entre comptes IAM dans le guide de l'IAMutilisateur.
- Accès multiservices — Certains AWS services utilisent des fonctionnalités dans d'autres AWS services. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès transmises (FAS) — Lorsque vous utilisez un IAM utilisateur ou un rôle pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FASutilise les autorisations du principal appelant an AWS service, combinées à la demande AWS service pour adresser des demandes aux services en aval. FASles demandes ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes AWS services 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 les politiques relatives FAS aux demandes, consultez la section Transférer les sessions d'accès.
  - Rôle de service — Un rôle de service est un IAMrôle qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieurIAM. Pour plus d'informations, consultez la section Création d'un rôle auquel déléguer des autorisations AWS service dans le Guide de IAM l'utilisateur.
  - Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. AWS service 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 IAM administrateur peut consulter, mais pas modifier les autorisations pour les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un IAM rôle pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui AWS CLI soumettent des AWS API demandes. Cela est préférable au stockage des clés d'accès dans l'EC2instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour 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 exécutés sur l'EC2instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez la section Utilisation

d'un IAM rôle pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le Guide de IAM l'utilisateur.

Pour savoir s'il faut utiliser IAM des rôles ou des IAM utilisateurs, voir Quand créer un IAM rôle (au lieu d'un utilisateur) dans le guide de IAM l'utilisateur.

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 JSON documents. Pour plus d'informations sur la structure et le contenu des documents de JSON politique, voir Présentation des JSON politiques dans le guide de IAM l'utilisateur.

Les administrateurs peuvent utiliser AWS JSON des politiques 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 autoriser les utilisateurs à effectuer des actions sur les ressources dont ils ont besoin, un IAM administrateur peut créer des IAM politiques. L'administrateur peut ensuite ajouter les IAM politiques aux rôles, et les utilisateurs peuvent assumer les rôles.

IAMles politiques définissent les autorisations pour une action, quelle que soit la méthode que vous utilisez pour effectuer l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur doté de cette politique peut obtenir des informations sur le rôle auprès du AWS Management Console AWS CLI, ou du AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, consultez la section Création de IAM politiques dans le Guide de l'IAMutilisateur.

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 savoir comment choisir entre une politique gérée ou une politique intégrée, voir Choisir entre des politiques gérées et des politiques intégrées dans le Guide de l'IAMutilisateur.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents JSON de stratégie que vous attachez à une ressource. Les politiques de confiance dans les IAM rôles et les politiques relatives aux compartiments Amazon S3 sont des exemples de politiques basées sur les ressources. 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. AWS services

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser de politiques AWS gérées depuis une IAM stratégie basée sur les ressources.

Listes de contrôle d'accès (ACLs)

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLssont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format du document JSON de stratégie.

Amazon S3 et Amazon VPC sont des exemples de services compatiblesACLs. AWS WAF Pour en savoir plusACLs, consultez la présentation de la liste 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.

- Limites d'autorisations — Une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une IAM entité (IAMutilisateur ou rôle). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez la section Limites d'autorisations pour les IAM entités dans le Guide de IAM l'utilisateur.
- Politiques de contrôle des services (SCPs) : SCPs JSON politiques 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 des politiques de contrôle des services (SCPs) à l'un ou à l'ensemble de vos comptes. Les SCP limites d'autorisations pour les entités présentes dans les comptes des membres, y compris chacune d'entre elles Utilisateur racine d'un compte AWS. Pour plus d'informations sur les Organizations et consultez SCPs les politiques de contrôle des services dans le Guide de AWS Organizations l'utilisateur.
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez la section Politiques de session dans le guide de IAM l'utilisateur.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de IAM l'utilisateur.

Comment fonctionne EventBridge Scheduler avec IAM

Avant de commencer IAM à gérer l'accès au EventBridge Scheduler, découvrez quelles IAM fonctionnalités sont disponibles avec EventBridge Scheduler.

IAMfonctionnalités que vous pouvez utiliser avec Amazon EventBridge Scheduler

IAMfonctionnalité	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
ACLs	Non
ABAC(balises dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Rôles de service	Oui
Rôles liés à un service	Non

Pour obtenir une vue d'ensemble de la façon dont EventBridge Scheduler et les autres AWS services fonctionnent avec la plupart des IAM fonctionnalités, consultez la section AWS Services compatibles IAM dans le Guide de l'IAMutilisateur.

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 JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, consultez la section Création de IAM politiques dans le Guide de l'IAMutilisateur.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier les actions et les 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 une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour en savoir plus sur tous les éléments que vous pouvez utiliser dans une JSON politique, consultez la référence aux éléments de IAM JSON politique dans le Guide de IAM l'utilisateur.

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 dans le planificateur EventBridge

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 JSON de stratégie que vous attachez à une ressource. Les politiques de confiance dans les IAM rôles et les politiques relatives aux compartiments Amazon S3 sont des exemples de politiques basées sur les ressources. 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. AWS services

Pour activer l'accès entre comptes, vous pouvez spécifier un compte entier ou IAM des entités d'un autre compte comme 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 IAM administrateur du compte de confiance 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 une identité à l'entité. Toutefois, si une politique basée sur des 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 la section Accès aux ressources entre comptes IAM dans le Guide de IAM l'utilisateur.

Actions politiques pour EventBridge Scheduler

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser AWS JSON des politiques 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'`Action`élément d'une JSON politique décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès dans une politique. Les actions de stratégie portent généralement le même nom que l' AWS APIopération associée. Il existe certaines exceptions, telles que les actions avec autorisation uniquement qui n'ont pas d'opération correspondante. API 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 AWS JSON des politiques 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 `Resource` JSON de stratégie indique le ou les objets auxquels s'applique l'action. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de spécifier une ressource en utilisant 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 caractéristiquesARNs, consultez la section Ressources définies par Amazon EventBridge Scheduler dans le Service Authorization Reference. Pour savoir avec quelles actions vous pouvez spécifier pour chaque ressource, consultez ARN 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 dans le planificateur EventBridge

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 AWS JSON des politiques 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 autoriser un IAM utilisateur à accéder à une ressource uniquement si celle-ci est étiquetée avec son nom IAM d'utilisateur. Pour plus d'informations, consultez IAMla section Éléments de politique : variables et balises dans le Guide de IAM l'utilisateur.

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 contextuelles de condition AWS globales dans le guide de IAM l'utilisateur.

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 dans le planificateur EventBridge

ACLsdans EventBridge Scheduler

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLssont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format du document JSON de stratégie.

ABACavec EventBridge Scheduler

Supports ABAC (balises dans les politiques) : Partiel

Le contrôle d'accès basé sur les attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises à IAM des entités (utilisateurs ou rôles) et à de nombreuses AWS ressources. Le balisage des entités et des ressources est la première étape deABAC. Vous concevez ensuite des ABAC politiques pour autoriser les opérations lorsque le tag du principal correspond à celui de la ressource à laquelle il essaie d'accéder.

ABACest utile dans les environnements qui se développent rapidement et aide dans les situations 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'informationsABAC, voir Qu'est-ce que c'est ABAC ? dans le guide de IAM l'utilisateur. Pour consulter un didacticiel présentant les étapes de configurationABAC, voir Utiliser le contrôle d'accès basé sur les attributs (ABAC) dans le guide de l'IAMutilisateur.

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

Prend en charge les informations d'identification temporaires : oui

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

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 la section Passage à un rôle (console) dans le guide de IAM l'utilisateur.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide du AWS CLI ou AWS API. 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 la section Informations d'identification de sécurité temporaires dans IAM.

Autorisations principales interservices pour Scheduler EventBridge

Prend en charge les sessions d'accès transféré (FAS) : Oui

Lorsque vous utilisez un IAM utilisateur ou un rôle pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FASutilise les autorisations du principal appelant an AWS service, combinées à la demande AWS service pour adresser des demandes aux services en aval. FASles demandes ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes AWS services 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 les politiques relatives FAS aux demandes, consultez la section Transférer les sessions d'accès.

Rôles de service pour EventBridge Scheduler

Prend en charge les rôles de service : oui

Un rôle de service est un IAMrôle qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieurIAM. Pour plus d'informations, consultez la section Création d'un rôle auquel déléguer des autorisations AWS service dans le Guide de IAM l'utilisateur.

> **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. AWS service 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 IAM administrateur peut consulter, mais pas modifier les autorisations pour les rôles liés à un service.

Pour plus de détails sur la création ou la gestion des rôles liés à un service, consultez la section AWS Services compatibles 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 dans le planificateur EventBridge

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 en utilisant le AWS Management Console, AWS Command Line Interface (AWS CLI) ou AWS API. Pour autoriser les utilisateurs à effectuer des actions sur les ressources dont ils ont besoin, un IAM administrateur peut créer des IAM politiques. L'administrateur peut ensuite ajouter les IAM politiques aux rôles, et les utilisateurs peuvent assumer les rôles.

Pour savoir comment créer une politique IAM basée sur l'identité à l'aide de ces exemples de documents de JSON stratégie, consultez la section Création de IAM politiques dans le guide de l'IAMutilisateur.

Pour plus de détails sur les actions et les types de ressources définis par le EventBridge planificateur, y compris le format de chaque type de ressource, consultez la section Actions, ressources et clés de condition ARNs pour Amazon EventBridge Scheduler dans la référence d'autorisation de service.

Rubriques

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 les politiques AWS gérées ou les politiques AWS gérées pour les fonctions professionnelles dans le Guide de IAM l'utilisateur.

- Appliquer les autorisations du moindre privilège : lorsque vous définissez des autorisations à IAM l'aide de politiques, accordez uniquement les autorisations nécessaires à l'exécution d'une 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 IAM pour appliquer des autorisations, consultez la section Politiques et autorisations IAM dans le guide de IAM l'utilisateur.
- Utilisez des conditions dans IAM les politiques pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques pour limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez rédiger une condition de politique pour spécifier que toutes les demandes doivent être envoyées en utilisantSSL. 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 AWS service, tel que AWS CloudFormation. Pour plus d'informations, voir Éléments IAM JSON de politique : Condition dans le guide de IAM l'utilisateur.
- Utilisez IAM Access Analyzer pour valider vos IAM politiques afin de garantir des autorisations sécurisées et fonctionnelles. IAM Access Analyzer valide les politiques nouvelles et existantes afin qu'elles soient conformes au langage des IAM politiques (JSON) et IAM aux meilleures pratiques. IAMAccess Analyzer fournit plus de 100 vérifications des politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez la section Validation des politiques d'IAMAccess Analyzer dans le guide de IAM l'utilisateur.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des IAM utilisateurs ou un utilisateur root Compte AWS, activez-le MFA pour une sécurité supplémentaire. Pour exiger le MFA moment où les API opérations sont appelées, ajoutez MFA des conditions à vos politiques. Pour plus d'informations, consultez la section Configuration de l'APIaccès MFA protégé dans le Guide de l'IAMutilisateur.

Pour plus d'informations sur les meilleures pratiques en matière de sécuritéIAM, consultez la section Bonnes pratiques en matière de sécurité IAM dans le Guide de IAM l'utilisateur.

EventBridge Autorisations du planificateur

Pour qu'un IAM principal (utilisateur, groupe ou rôle) puisse créer des horaires dans le EventBridge planificateur et accéder aux ressources du EventBridge planificateur via la console ou leAPI, le principal doit disposer d'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 lancer l'`CreateSchedule`APIopération. 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 IAM politiques 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 les politiques AWS gérées dans

le Guide de IAM l'utilisateur. 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 du. 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 KMS clé 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 des adjoints confuse dans EventBridge Scheduler

Le problème de député confus est un problème de sécurité dans lequel une entité qui n'est pas autorisée à effectuer une action peut contraindre une entité plus privilégiée à le faire. En AWS, l'usurpation d'identité interservices peut entraîner un problème de confusion chez les adjoints. L'usurpation d'identité entre services peut se produire lorsqu'un service (le service appelant) appelle un autre service (le service appelé). Le service appelant peut être manipulé 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 prémunir contre le problème de confusion des adjoints consiste à utiliser la clé de contexte de la condition `aws:SourceArn` globale avec l'intégralité ARN 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'intégralité ARN de la ressource ou si vous spécifiez plusieurs ressources, utilisez la clé de condition contextuelle `aws:SourceArn` globale avec des caractères génériques (*) pour les parties inconnues duARN. olpPar exemple : `arn:aws:scheduler:*:123456789012:schedule-group/*`.

La valeur de `aws:SourceArn` doit être le groupe de planification du EventBridge planificateur ARN 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. Le groupe ARN que vous spécifiez doit être un groupe de planification.

L'exemple suivant montre comment vous pouvez utiliser les clés contextuelles `aws:SourceArn` et les clés de contexte de condition `aws:SourceAccount` globale dans votre politique de confiance en matière de 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 lorsque vous utilisez EventBridge Scheduler et. IAM

Rubriques

- Je ne suis pas autorisé à effectuer une action dans le EventBridge planificateur
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder aux ressources de mon EventBridge planificateur

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 lorsque l'`mateojackson`IAMutilisateur essaie d'utiliser la console pour afficher les détails d'une *`my-example-widget`* ressource fictive mais ne dispose pas des `scheduler:`*`GetWidget`* autorisations 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 AWS services 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 IAM utilisateur 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 un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

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

Je souhaite 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 (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder 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 donner accès à vos ressources sur un site Comptes AWS qui vous appartient, consultez la section Fournir l'accès à un IAM utilisateur dans un autre site Compte AWS que vous possédez dans le Guide de IAM l'utilisateur.
- 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 IAM l'utilisateur.

- Pour savoir comment fournir un accès via la fédération d'identité, consultez la section Fournir un accès aux utilisateurs authentifiés de manière externe (fédération d'identité) dans le guide de l'IAMutilisateur.
- Pour connaître la différence entre l'utilisation de rôles et l'utilisation de politiques basées sur les ressources pour l'accès entre comptes, voir Accès aux ressources entre comptes IAM dans le guide de l'IAMutilisateur.

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 AWS services que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez la section Confidentialité des données FAQ. Pour plus d'informations sur la protection des données en Europe, consultez le modèle de responsabilitéAWS partagée et le billet de GDPR blog sur le blog sur la AWS sécurité.

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) pour chaque compte.
- UtilisezSSL/TLSpour communiquer avec les AWS ressources. Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Configuration API et 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 AWS services.
- 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 FIPS 140 à 3 modules cryptographiques validés pour accéder AWS via une interface de ligne de commande ou unAPI, utilisez un point de terminaison. FIPS Pour plus d'informations sur les FIPS points de terminaison disponibles, voir Federal Information Processing Standard (FIPS) 140-3.

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 EventBridge Scheduler ou autre à AWS services l'aide de la console, API AWS CLI, ou. AWS SDKs Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez un URL à un serveur externe, nous vous recommandons vivement de ne pas inclure d'informations d'identification dans le URL afin de valider votre demande auprès de ce serveur.

Chiffrement au repos dans le EventBridge planificateur

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 KMS clés : Clés détenues par AWSet les clés gérées par le client.

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

Clés détenues par AWSsont KMS des clés 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 KMS clés 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 fait également partie de 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 KMS clés
- 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 KMS clé 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, désactivation) du planning.	Pris en charge	Non pris en charge
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	Pris en charge	Non pris en charge

Type de données	Description	Clé détenue par AWS	clé gérée par le client
	que la date de début, la date de fin et le fuseau horaire du planning.		
Configuration cible	Le nom de la ressource Amazon de la cible (ARN) et d'autres détails de configuration relatifs 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 tentative s du calendrier et détails de la file d'attente en cas d'échec des livraison s.	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 KMS clés" section suivante pour savoir comment vous devez gérer vos IAM ressources et vos politiques clés afin d'utiliser une clé gérée par le client avec EventBridge Scheduler.

Gestion des KMS clés

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 les tarifs, consultez la section sur AWS Key Management Service les tarifs

EventBridge Le planificateur utilise IAM les autorisations 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 le EventBridge planificateurAPI. 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 le 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 IAM autorisations requises pour utiliser une clé gérée par le client sur EventBridge Scheduler.

Rubriques

- Ajouter des IAM autorisations
- Gérer la politique clé

Ajouter des IAM autorisations

Pour utiliser une clé gérée par le client, vous devez ajouter les autorisations suivantes au IAM principal basé sur l'identité qui crée un calendrier, ainsi que le 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 le EventBridge planificateur API 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 vérifier que la clé que vous fournissez est une KMS clé 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 de l'appeler 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 API liés aux appels. Cela inclut API les appels chaque fois que le EventBridge planificateur utilise la 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 dans le EventBridge planificateur

EventBridge Le planificateur chiffre vos données en transit lorsqu'elles circulent sur le réseau. Transport Layer Security (TLS) chiffre vos données lorsque vous appelez une API opération du EventBridge planificateur, ainsi que lorsque le EventBridge planificateur appelle une cible APIs lorsqu'il invoque votre calendrier. Par défaut, EventBridge Scheduler utilise la version 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 TLS version lorsque vous utilisez le EventBridge planificateur.

Utilisation du EventBridge planificateur API : lorsque vous effectuez une API opération, par exemple, le EventBridge planificateur chiffre l'intégralité de la HTTP demande`CreateSchedule`, y compris le corps et les en-têtes de la demande. EventBridge Le planificateur chiffre également l'intégralité de l'objet de réponse que vous recevez de notre part. APIs

Utilisation de la cible APIs : lorsque le EventBridge planificateur appelle votre calendrier, il appelle la cible API 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 AWS services de conformité AWS service s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez AWS services 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 AWS services 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 HIPAA sécurité et la conformité sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent AWS créer HIPAA des applications éligibles.

> **Note**
>
> Tous ne AWS services sont pas HIPAA éligibles. Pour plus d'informations, consultez la référence des services HIPAA éligibles.

- 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 AWS services et reprennent les directives relatives aux contrôles de sécurité dans de nombreux 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 AWS service 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.
- Amazon GuardDuty — Cela AWS service détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité PCIDSS, par exemple en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous AWS service 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 les API appels AWS publiés pour accéder au EventBridge planificateur via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Sécurité de la couche de transport (TLS). Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Des suites de chiffrement parfaitement confidentielles (PFS) telles que (Ephemeral Diffie-Hellman) ou DHE 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 identifiant de clé d'accès et d'une clé d'accès secrète associés à un IAM principal. 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 joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances d'Amazon EventBridge Scheduler et de vos autres AWS solutions. AWS fournit les outils de surveillance suivants pour surveiller le EventBridge planificateur, signaler un problème et prendre des mesures automatiques le cas échéant :

- Amazon CloudWatch surveille vos AWS ressources et les applications que vous utilisez AWS en temps réel. 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 plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.
- AWS CloudTrailcapture API les appels et les événements connexes effectués par ou pour le compte de votre AWS compte et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. Pour plus d'informations, consultez le AWS CloudTrail Guide de l'utilisateur .

Rubriques

Surveillance d'Amazon EventBridge Scheduler avec Amazon CloudWatch

Vous pouvez surveiller Amazon EventBridge Scheduler à l'aide d'Amazon Scheduler CloudWatch, qui collecte les données brutes et les traite en métriques lisibles en temps quasi réel. EventBridge Le planificateur émet un ensemble de mesures pour tous les plannings, et un ensemble supplémentaire de métriques pour les plannings associés à une file d'attente de lettres mortes (). DLQ Si vous configurez un DLQ pour votre calendrier, le EventBridge planificateur publie des mesures supplémentaires lorsque votre calendrier a épuisé sa politique de nouvelles tentatives.

Ces statistiques sont conservées pendant 15 mois, afin que vous puissiez accéder aux informations historiques, avoir une meilleure idée des raisons pour lesquelles un calendrier échoue et résoudre les problèmes sous-jacents. Vous pouvez également définir des alarmes qui surveillent certains seuils et envoient des notifications ou prennent des mesures lorsque ces seuils sont atteints. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.

Rubriques

Conditions

Espace de noms

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

CloudWatch métriques

Une CloudWatch métrique représente un ensemble chronologique de points de données spécifiques à 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 le nombre.

Dimensions

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

Dimension	Description
ScheduleGroup	Le groupe de plannings pour lequel vous souhaitez consulter les métriques à l'aide de CloudWatch. Si vous n'avez pas encore créé de groupe, EventBridge Scheduler associe vos plannings au `default` groupe.

Accès aux métriques

Cette section décrit comment accéder aux mesures de performance CloudWatch pour un planning de EventBridge planificateur spécifique.

Pour consulter les indicateurs de performance d'une dimension

1. Ouvrez la page Metrics sur la CloudWatch console.
2. Utilisez le sélecteur de AWS région pour choisir la région correspondant à votre emploi du temps
3. Choisissez l'espace de noms du planificateur.
4. Dans l'onglet Toutes les mesures, choisissez une dimension, par exemple Schedule Group Metrics. Pour voir les statistiques de tous les plannings que vous avez créés dans la région que vous avez sélectionnée, choisissez Account Metrics.
5. Choisissez une CloudWatch métrique pour une dimension. Par exemple InvocationDroppedCount, InvocationAttemptCountou choisissez ensuite Recherche graphique.
6. Choisissez l'onglet Graphed metrics pour afficher les statistiques de performance des metrics EventBridge Scheduler.

Liste des 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

Indicateurs pour tous les plannings

Espace de noms	Mesure	Unité	Description
AWS/Scheduler	InvocationAttemptCount	Nombre	Émis à chaque tentative d'invocation. Utilisez cette métrique pour vérifier que EventBridge Scheduler essaie d'invoquer vos plannings et pour voir à quel moment les appels approchent les quotas de votre compte.
AWS/Scheduler	TargetErrorCount	Nombre	Émis lorsque la cible renvoie une exception après que le EventBridge Scheduler a appelé la cible. API Utilisez-le pour vérifier en cas d'échec de la livraison vers une cible.
AWS/Scheduler	TargetErrorThrottledCount	Nombre	Émis lorsque l'invocation de la cible échoue en raison d'APIun ralentissement par la cible. Utilisez-le pour diagnostiquer les échecs de livraison lorsque la raison sous-jacente est la cible

Espace de noms	Mesure	Unité	Description
			des appels de API régulation effectués par le planificateur EventBridge
AWS/Scheduler	InvocationThrottleCount	Nombre	Émis lorsque le EventBridge planificateur limite un appel cible parce qu'il dépasse vos quotas de service définis par le planificateur. EventBridge Utilisez-le pour déterminer à quel moment vous avez dépassé votre quota maximal d'appels. Pour plus d'informations sur les quotas de service, consultezQuotas.

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

Indicateurs pour les plannings dotés d'un DLQ

Espace de noms	Mesure	Unité	Description
AWS/Scheduler	InvocationsSentToDeadLetterCount	Nombre	Émis pour chaque livraison réussie selon un calendrierDLQ. Utilisez-le pour déterminer à quel moment les événements sont envoyés

Espace de noms	Mesure	Unité	Description
			à unDLQ, puis vérifiez l'événement livré conformément au calendrier DLQ 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 peut pas envoyer d'événement au. DLQ Utilisez ces deux mesures pour déterminer la raison pour laquelle le EventBridge planificateur n'est pas en mesure d'envoyer un événement auDLQ, et modifiez votre DLQ configuration pour résoudre le problème. Voici un exemple de InvocationsFailedToBeSentToDeadLetterCount_<error_code
AWS/Scheduler	InvocationsFailedToBeSentToDeadLetterCount_<error_code>	Nombre	

Espace de noms	Mesure	Unité	Description
			> métrique lorsque la SQS file d'attente Amazon que vous spécifiez 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 le EventBridge planificateur tronque la charge utile que vous spécifiez dans l'attribut d'un planning. `Input`

EventBridge Mesures d'utilisation du planificateur

CloudWatch collecte des métriques qui permettent de suivre l'utilisation de certaines AWS ressources. Ces mesures correspondent aux quotas AWS de service. Le suivi de ces métriques peut vous aider à gérer de manière proactive vos quotas. Utilisez les mesures suivantes pour déterminer à quel moment vous avez dépassé les quotas de votre EventBridge planificateur. Pour plus d'informations sur les quotas de service, consultezQuotas.

Ces métriques sont contenues dans l'espace de `AWS/Usage` noms, plutôt que`AWS/Scheduler`, et sont collectées toutes les minutes.

Actuellement, le seul nom de métrique publié dans cet espace de noms CloudWatch est`CallCount`. Cette métrique est publiée avec les dimensions `Resource`, `Service` et `Type`. La `Resource` dimension indique le nom de l'APIopération suivie.

Par exemple, la `CallCount` métrique aux dimensions suivantes indique le nombre de fois que l' Planificateur EventBridge `CreateSchedule`APIopération a été appelée dans votre compte :

- « Service » : « Planificateur »
- « Tapez » : « API »
- « Ressource » : "CreateSchedule»

La métrique `CallCount` n'a pas d'unité spécifiée. La statistique la plus utile pour la métrique est `SUM`, qui représente le nombre total d'opérations pour une période d'1 minute.

Métriques

Métrique	Description		
`CallCount`	Nombre d'opérations spécifiées effectuées dans votre compte.		

Dimensions

Dimension	Description		
`Service`	Nom du AWS service contenant la ressource. Pour les métriques Planificateur EventBridge d'utilisation, la valeur de cette dimension est`Scheduler` .		
`Class`	Classe de ressource suivie. Planificateur EventBridge APIles métriques d'utilisation utilisent cette dimension avec une valeur de`None`.		
`Type`	Type de ressource suivi.		

Dimension	Description
	Actuellement, lorsque la dimension `Service` est `Scheduler` , la seule valeur valide pour `Type` est `API`.
`Resource`	Le nom de l'APIopération. Les valeurs valides sont notamment les suivantes : • `CreateSchedule` • `CreateScheduleGroup` • `DeleteSchedule` • `DeleteScheduleGroup` • `GetSchedule` • `GetScheduleGroup` • `ListScheduleGroups` • `ListSchedules` • `ListTagsForResource` • `TagResource` • `UntagResource` • `UpdateSchedule`

Journalisation des appels Amazon EventBridge Scheduler à l'aide API de AWS CloudTrail

Amazon EventBridge Scheduler est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans EventBridge Scheduler. CloudTrail capture tous les API appels au EventBridge Scheduler sous forme d'événements. Les appels capturés incluent des appels provenant de la console du EventBridge planificateur et des appels de code vers les opérations du EventBridge planificateurAPI. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour EventBridge Scheduler. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans

la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite au EventBridge Scheduler, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

EventBridge Informations sur le planificateur dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans le EventBridge planificateur, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre navigateur Compte AWS, y compris des événements pour EventBridge Scheduler, créez un parcours. Un suivi permet CloudTrail de fournir des fichiers journaux à 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 enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

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

Toutes les API actions du EventBridge planificateur sont enregistrées CloudTrail et documentées dans le manuel Amazon EventBridge API Scheduler Reference. Par exemple, les appels au `CreateSchedule` `UpdateSchedule` et les `DeleteSchedule` 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 faite avec les informations d'identification de l'utilisateur root 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 demande a été faite par un autre AWS service.

Pour plus d'informations, consultez l'CloudTrail userIdentityélément.

Comprendre les EventBridge entrées du fichier journal du planificateur

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des API appels publics, ils n'apparaissent donc pas dans un ordre spécifique.

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 la plupart des quotas, mais certains 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.

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

Nom	Par défaut	Ajusta	Description
CreateSchedule taux de demandes	ca-central-1 : 250 eu-central-1 : 1 000 Chacune des autres régions prises 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 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
DeleteSchedule taux de demandes	ca-central-1 : 250 eu-central-1 : 1 000 Chacune des autres régions prises 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.
GetSchedule taux de demandes	ca-central-1 : 250 eu-central-1 : 1 000 Chacune des autres régions prises 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.

Nom	Par défaut	Ajusta	Description
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	eu-central-1 : 1 000 Chacune des autres régions prises 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.
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.

Nom	Par défaut	Ajusta	Description
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.
Nombre de plannings	ca-central-1 : 10 000 000 eu-central-1 : 10 000 000 Chacune des autres régions prises en charge : 1 000 000	Oui	Le nombre maximum de programmes par région. Ce quota inclut les programmes ponctuels dont l'exécution est terminée. Nous vous recommandons de configurer vos plannings de manière à ce qu'ils soient automatiquement supprimés une fois ActionAfterComplet ion cette fonctionnalité terminée.

Nom	Par défaut	Ajusta	Description
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	ca-central-1 : 250 eu-central-1 : 1 000 Chacune des autres régions prises 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

Résolution des problèmes liés aux quotas dans le EventBridge planificateur

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer concernant les quotas du EventBridge planificateur.

ServiceQuotaExceededException

Je reçois des erreurs de régulation concernant`CreateSchedule`,`DeleteSchedule`, ou le taux de `UpdateSchedule` demandes`GetSchedule`, même si je suis inférieur à la limite de débit par défaut.

Cause commune

Le 7 septembre 2023, EventBridge Scheduler a commencé à prendre en charge le (ScheduleGroup ARNAmazon Resource Name) plutôt que le Schedule ARN dans les politiques de confiance des rôles d'exécution. Les clients autorisés à continuer à utiliser Schedule ARNs dans leur politique de confiance peuvent avoir une limite de 50TPS, au lieu des limites par défaut de 250 à 1 000 TPS (selon la région).

Résolution

Contactez le support pour demander une limite maximale plus élevée.

Prévention

Modifiez vos politiques de confiance existantes de l'une des manières suivantes :

- Suppression de toute la portée du rôle.
- Définir la portée du rôle afin qu'il puisse être assumé à l'aide du calendrier ARN ou du ScheduleGroup ARN.

  Supposons, par exemple, que vous disposiez de la politique de confiance suivante :

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "scheduler.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
        "StringEquals": {
            "aws:SourceArn":
 "arn:aws:scheduler:region:account:schedule/schedule_group/schedule"
        }
    }
}
```

  Vous pouvez mettre à jour la politique de confiance comme suit :

```
{
    "Effect": "Allow",
    "Principal": {
```

```
        "Service": "scheduler.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:SourceArn": [
                "arn:aws:scheduler:region:account:schedule/schedule_group/schedule",
                "arn:aws:scheduler:region:account:schedule-group/schedule_group"
            ]
        }
    }
}
```

Historique du document pour le guide de l' EventBridge utilisateur du planificateur

Le tableau suivant décrit les versions de documentation pour EventBridge Scheduler.

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 “Préventi on de l’adjoint confus”	7 septembre 2023
Suppression automatique des plannings une fois terminés	EventBridge Le planificateur prend en charge la suppressi on automatique. Lorsque vous configurez la suppression automatique, le EventBridge planificateur supprime votre calendrier après son dernier appel planifié. • the section called “Suppress ion une fois le planning terminé”	02/08/2023
Rubrique mise à jour sur l'utilisation de cibles universel les	Mise à jour de la liste des services pris en charge que EventBridge Scheduler peut	17 mars 2023

	cibler et auxquels il peut s'intégrer. Cette mise à jour inclut également une liste des `GET` API opérations non prises en charge 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"	
Informations mises à jour sur les programmes basés sur les tarifs qui n'ont pas de date de début	Ajout d'informations sur la façon dont le EventBrid ge 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 Scheduler. Utilisez ce chapitre pour apprendre à créer un groupe, à ajouter des plannings au groupe, à appliquer des balises pour gérer et surveiller plus facilement les ressources de votre EventBridge planificateur, et enfin à supprimer un groupe. • Gestion d'un groupe de planning	17 mars 2023
Nouveaux sujets sur l'heure d'été et les fuseaux horaires	De nouvelles sections ont été ajoutées qui décrivent comment EventBridge Scheduler gère l'heure d'été et comment 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 métriques sur lesquelles EventBridge Scheduler publie. CloudWatch Vous pouvez utiliser ces indicateurs pour surveiller les échecs d'invocation et comprendre comment résoudre les problèmes liés à vos plannings. • the section called "Surveillance avec CloudWatch"	15 novembre 2022
Première version	Première publication du guide de l'utilisateur du EventBridge 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.